appviewx



CERT+ Guides

Version: 2023.1.0 FP2.1

CERT+ Guides

AppViewX's CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CERT+, security teams can manage the certificate lifecycle from an intuitive single-pane management Interface. It enables the Certificate Lifecycle Management and Automation solution which helps enterprise IT manage and automate the entire lifecycle of their internal and external PKI. The key stages of the certificate lifecycle can be broken into the following stages:



What is Certificate Lifecycle Management (CLM)?

There is a growing need for organizations to allow and control only specific individuals, devices, machines to gain access to the network. The need for digital certificates to authenticate, identify and control who can access and operate on an organization's network. Managing digital certificates across complex networks to ensure protection and prevent failures is a must for all businesses. CLM ensures continuous monitoring of digital certificates, with the ability to audit and keep track of expirations and renewals to avoid any service disruption. The digital certificate is a mechanism by which machines and individuals are identified and authenticated.

What is x.509 Digital Certificate?

The digital certificate is a mechanism by which machines and individuals are identified and authenticated. Digital certificates (x.509 certificates) are essential to establish trust and authenticate the identity of machines, people, and so on.

It helps to verify the identity between users in operation, servers, and other entities in a network. Also, identifies servers from whom the encrypted data is received, the signer of information, and helps

to establish authenticity and integrity. The x.509 digital certificate protects information belonging to enterprises and their customers.

A digital certificate contains:

- Name of the certificate holder.
- Serial Number that is used to uniquely identify the service, individual, or entity identified by the certificate.
- Expiry date.
- Copy of the certificate holder's public key (used for decrypting messages and digital signatures).
- Digital Signature of the certificate-issuing authority.

Certificate Authority

A Certificate Authority (CA) is also known as a certification authority or certificate issuer and is an establishment that validates the identities of certificate requesters and associates them to a cryptographic key through the issuance of electronic documents known as digital certificates.

Core Capabilities of CERT+

- Integrate with multiple Certificate Authorities (CAs) for certificate provisioning.
- Integrate with and manage services across native cloud services like Amazon Web Services, Microsoft Azure, and Google Cloud Platform.
- Discover, monitor, analyze, orchestrate and fully automate certificate lifecycle management and key management solutions.
- Manage certificates as a service with pre-built integrations and extensible APIs that plugin to your enterprise applications, web servers, micro services, and multi-cloud environments.
- Analyze certificates for crypto standards like key size, cipher strength, and allowed protocol versions.
- Setup policies for enforcing high crypto standards.
- Update certificates as per new policies.
- Provision certificates for devices and applications.
- Monitor certificate status in real-time.
- Setup alerts on certificates to prevent security breaches.

Copyright AppViewX, Inc.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Trademarks

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

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

CERT+ Guides....ii

What is Certificate Lifecycle Management (CLM)?....ii

What is x.509 Digital Certificate?....ii

Certificate Authority....iii

Core Capabilities of CERT+....iii

Preface....26

Revision History....26

About this Guide....26

Audience....26

Text Conventions....26

Chapter 1. CERT+ User Guide....27

Getting Started....27

About AppViewX....27

Getting Started with CERT+....30

What's In It for you?....32

Web Browser Prerequisites....33

Accessing CERT+....34

Onboard Certificates....34

Prerequisites for Onboarding Certificates....34

Certificate Discovery....34

Discovery Status....98

Excluded from Discovery....103

Syncing Certificates with Network Devices or Servers....108

Manage Devices....110

Inventory Actions....110

Device Prerequisite....116

ADC Prerequisite....117

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Firewall and Web Application Firewall (WAF) Prerequisite..... 121
Server Prerequisite..... 123
Certificate Actions..... 128
Enrolling Certificates..... 129
Renewing Certificates..... 170
Pushing Certificates to Devices..... 177
Reissuing Certificates..... 327
Revoking Certificates..... 331
Regenerating Certificates..... 338
Reinstating Certificates..... 343
Running Revocation Check-OCSP..... 346
Generating Certificate Signing Request (CSR)..... 349
Migrating CAs (CA Switch)..... 354
Running the SSL Checker for a Certificate..... 358
Managing the Certificate Inventory..... 359
Managing the Server Certificate Inventory..... 360
Managing the Client Certificate Inventory..... 369
Managing the Code Signing Certificate Inventory..... 378
Managing the Device Certificate Inventory..... 386
Managing the Intermediate Certificate Inventory..... 394
Managing the Root Certificate Inventory..... 395
Uploading a Certificate..... 396
Downloading Certificates..... 396
Certificate Reporting and Monitoring..... 404
Accessing the Dashboard..... 404
Creating a Dashboard..... 405
Exporting Dashboard Information..... 406
Importing a Dashboard..... 407
Understanding Certificate Reports on the Dashboard..... 407

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Searching for Dashboard, Object, or Widget..... 488
Deleting a Dashboard..... 489
Alerts and Logs..... 489
Overview..... 489
Certificate Alerts..... 490
Configuring Expiry Alerts..... 491
Configuring a Certificate Expiry Alert 512
Configuring a Certificate Sync Alert 513
Configuring a Certificate Validation Alert 515
Configuring a Connection Failure Alert 516
Certificate Logs 518
Export Certificates Logs 519
Standard Practices..... 520
PKI Standard Practices..... 520
CLM - Best Practices..... 523
Standard Practices followed in the Certificate Inventory Management 524
Securing CERT+..... 526
Chapter 2. CERT+ Admin Guide..... 527
Getting Started..... 527
About AppViewX..... 527
CERT+ Overview..... 527
What is Certificate Lifecycle Management (CLM)?..... 528
What is x.509 Digital Certificate?..... 529
Certificate Authority..... 529
CERT Administration..... 529
Prerequisites..... 530
Accessing the CERT+..... 530
CERT+ Home Page..... 530
RBAC Configuration..... 531

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CERT+ Setup....532
Configuring CA Settings....533
CA Policy....632
Certificate Group....723
Configuring Certificates....731
Managing Devices....741
Certificate Reports....903
Auto Enrollment Protocols....923
Chapter 3. CERT+ API Guide....1065
Login to AppViewX....1066
Request Structure....1066
Response Structure....1066
Status Codes....1067
Sample Request/Response....1067
Create a Certificate in Async mode....1068
Before you begin....1068
Request Structure....1068
Response Structure....1075
Status Codes....1076
Related Information....1076
CA Specific Information....1077
Common Payload Objects....1202
Create a Certificate in Sync mode....1203
Request Structure....1203
Response Structure....1210
Sample Request/Response....1211
Related Information....1213
Renew a Certificate in Async mode....1214
Before you begin....1214

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Structure....1214
Response Structure....1216
Status Codes....1217
Sample Request/Response....1218
Related Information....1219
Renew a Certificate in Sync mode....1219
Request Structure....1219
Response Structure....1222
Status Codes....1223
Sample Request/Response....1223
Related Information....1224
Revoke a Certificate in Async mode....1224
Before you begin....1224
Request Structure....1224
Response Structure....1226
Status codes....1227
Sample Request/Response....1228
Related Information....1229
Revoke a Certificate in Sync mode....1229
Request Structure....1229
Response Structure....1232
Status Codes....1232
Sample Request/Response....1233
Related Information....1233
Reissue a Certificate in Async mode....1233
Before you begin....1233
Request Structure....1234
Response Structure....1236
Status codes....1236

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response..... 1238
Related Information.....1238
Reissue a Certificate in Sync mode..... 1238
Request Structure..... 1238
Response Structure..... 1242
Status Codes..... 1242
Sample Request/Response..... 1242
Related Information.....1243
Regenerate a Certificate in Async mode.....1244
Before you begin.....1244
Request Structure..... 1244
Response Structure..... 1246
Status codes..... 1247
Sample Request/Response..... 1248
Regenerate a Certificate in Sync mode.....1249
Request Structure..... 1249
Response Structure..... 1252
Status Codes..... 1252
Sample Request/Response..... 1252
Suspend a Certificate.....1253
Before you begin.....1253
Request Structure..... 1254
Response Structure..... 1256
Status Codes..... 1256
Sample Request/Response..... 1258
Reinstate a Certificate.....1258
Before you begin.....1259
Request Structure..... 1259
Response Structure..... 1261

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes..... 1262
Sample Request/Response..... 1263
Search/ Get Certificate Inventory.....1264
Request Structure..... 1264
Response Structure..... 1269
Status Codes..... 1271
Sample Request/Response..... 1271
Add Certificate Attributes..... 1274
Request Structure..... 1275
Response Structure..... 1277
Status Codes..... 1277
Sample Request/Response..... 1278
Related Information.....1280
Update Certificate Attributes..... 1280
Request Structure..... 1280
Response Structure..... 1282
Status Codes..... 1283
Sample Request/Response..... 1283
Related Information.....1285
Get Certificate Attributes.....1285
Request Structure..... 1285
Response Structure..... 1286
Status Codes..... 1287
Sample Request/Response..... 1287
Related Information.....1288
Delete Certificate Attributes..... 1288
Request Structure..... 1288
Response Structure..... 1289
Status Codes..... 1290

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response ... 1290
Download a Certificate ... 1291
Request Structure ... 1291
Response Structure ... 1292
Status Codes ... 1293
Sample Response ... 1294
Download a Certificate by Format ... 1294
Request Structure ... 1294
Response Structure ... 1297
Status Codes ... 1297
Sample Request/Response ... 1298
Common Response Objects ... 1299
Push and Bind Certificate to a Firewall Profile ... 1300
Before you Begin ... 1300
Request Structure ... 1300
Response Structure ... 1305
Status Codes ... 1306
Sample Request/Response ... 1307
Rollback certificate to firewall profile ... 1308
Before you begin ... 1308
Request Structure ... 1308
Response Structure ... 1310
Status Codes ... 1311
Sample Request/Response ... 1312
Get Available Server Profiles ... 1312
Before you begin ... 1312
Request Structure ... 1312
Response Structure ... 1314
Status Codes ... 1315

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response..... 1316
Push and Bind Certificate to a server profile.....1316
Before you Begin..... 1316
Request Structure..... 1317
Response Structure..... 1333
Status Codes..... 1334
Sample Request/Response..... 1335
Sample Request/Response for Apache Server.....1336
Sample Request/Response for IPlanet Server.....1337
Sample Request/Response for Tomcat Server.....1338
Sample Request/Response for Weblogic Server..... 1339
Sample Request/Response for Websphere Server.....1340
Rollback Certificate to server profile.....1343
Before you begin.....1343
Request Structure..... 1343
Response Structure..... 1345
Status Codes..... 1346
Sample Request/Response..... 1347
After you are done.....1347
Approve a Request.....1348
Implement Request.....1355
Download Private Key of a Certificate.....1362
Request Structure.....1362
Response Structure..... 1364
Status Codes..... 1364
Sample Request/Response..... 1365
Delete Certificate using UUID.....1366
Request Structure.....1366
Response Structure..... 1368

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes..... 1368
Sample Request/Response..... 1369
CERT+ ADC API.....1369
Push and Bind Certificate to a ADC Profile..... 1369
Push and Bind Certificate to ADC Devices..... 1391
Rollback to ADC profile..... 1417
Discover Certificates from Firewall..... 1421
Before you begin.....1421
Request Structure..... 1422
Response Structure..... 1424
Status Codes..... 1424
Sample Request/Response..... 1426
Discover Certificates from Server..... 1427
Before you begin.....1427
Request Structure..... 1427
Response Structure..... 1429
Status Codes..... 1430
Sample Request/Response..... 1431
HP iLO Vendor Integration via REST Interface..... 1432
Chapter 4. MultiCloud Configuration User Guide.....1433
Supported Vendors..... 1433
Prerequisites.....1433
Limitation..... 1435
Prerequisites.....1435
Limitation..... 1436
Viewing the Cloud Device Inventory.....1436
Amazon Web Services (AWS).....1440
Prerequisites for Migrating AWS Standalone Accounts from Older Versions.....1440
Onboarding a Standalone Account in AWS..... 1443

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Onboarding a Cross Account in AppViewX....1461
AWS Cross/Federated Account Onboarding....1500
Azure....1509
Azure Services Supported by AppViewX....1510
Permissions Required for Onboarding Azure....1511
Onboarding Azure Settings in AppViewX....1513
Google Cloud Platform (GCP)....1516
GCP Services Supported by AppViewX....1516
Onboarding GCP Projects in AppViewX....1517
Limitations....1532
Apache SSM integration specification....1532
Device Addition....1533
Credential management....1533
Functional Specification....1534
Basic information specifications....1534
Account name....1534
Description....1535
Account number....1535
Proxy required....1535
Credentials Specifications....1535
Credential input type....1535
Access key....1536
Secret key....1536
Key information specifications....1537
Data Center....1537
Region....1537
Service....1538
Additional Attributes Specifications....1539
Generic Linux SSM Integration Specification....1540

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Device Addition....1540
Credential management....1541
Instances Discovery Specification....1542
Specifications....1542
Chapter 5. MultiCloud API Guide....1543
Push Certificates to ACM....1543
Before You Begin....1543
Request Structure....1543
Response Structure....1548
Status Codes....1549
Sample Request/Response....1550
Push Certificates to IAM....1551
Before You Begin....1552
Request Structure....1552
Response Structure....1556
Status Codes....1557
Sample Request/Response....1558
Push Certificates to ELB via ACM....1560
Before You Begin....1560
Request Structure....1560
Response Structure....1565
Status Codes....1566
Sample Request/Response....1567
Push Certificates to ELB via IAM....1568
Before You Begin....1568
Request Structure....1569
Response Structure....1573
Status Codes....1574
Sample Request/Response....1575

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Push Certificates to Cloudfront via ACM....1577
Before You Begin....1577
Request Structure....1577
Response Structure....1582
Status Codes....1583
Sample Request/Response....1584
Push Certificates to Cloudfront via IAM....1585
Before You Begin....1585
Request Structure....1586
Response Structure....1590
Status Codes....1591
Sample Request/Response....1592
Chapter 6. CERT+ Troubleshooting Guide....1595
Troubleshooting for CAs....1595
Troubleshooting for Amazon CA....1596
Troubleshooting Custom CA....1602
Troubleshooting DigiCert CA....1607
Troubleshooting EJBCA CA....1613
Troubleshooting Entrust MPKI....1624
Troubleshooting GlobalSign CA....1628
Troubleshooting GoDaddy CA....1634
Troubleshooting Google Private CA....1644
Troubleshooting InCommon CA....1654
Troubleshooting LetsEncrypt CA....1665
Troubleshooting Microsoft Enterprise CA....1669
Troubleshooting Microsoft Standalone CA....1699
Troubleshooting Sectigo CA....1724
Troubleshooting Symantec CA....1737
Troubleshooting Trustwave CA....1742

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Windows Agent Setup..... 1749
Troubleshooting General.....1763
Overview..... 1764
Troubleshooting Certificate Group.....1764
Troubleshooting Certificate Policy..... 1766
Troubleshooting Certificate Reports Configuration.....1768
Troubleshooting Configuration of Workflow.....1770
Troubleshooting Protocols.....1770
Overview..... 1770
Troubleshooting Auto-Enrolment ACME.....1771
Troubleshooting Auto-Enrolment EST..... 1776
Troubleshooting Auto-enrolment of MsIntune SCEP.....1783
Troubleshooting Auto-enrolment of SCEP.....1786
Troubleshooting AWS, CLOUD..... 1790
Overview..... 1790
Troubleshooting of AWS - CLOUD (ACM and IAM).....1791
Troubleshooting AWS CLOUD CloudFront..... 1799
Troubleshooting AWS CLOUD ELB..... 1803
Troubleshooting Azure CLOUD..... 1808
Troubleshooting CLOUD - Common Functionality..... 1824
Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors 1835
Overview..... 1836
Troubleshooting Apache Linux..... 1836
Troubleshooting Barracuda WAF..... 1848
Troubleshooting Cisco ASA Firewall..... 1852
Troubleshooting Cisco CallManager.....1856
Troubleshooting Common Functionality of Servers.....1862
Troubleshooting Data Power Server..... 1867
Troubleshooting F5 WAF.....1874

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Fortigate Firewall....1880
Troubleshooting HP ILO....1885
Troubleshooting IBMClient Linux....1890
Troubleshooting IBMClient Windows....1897
Troubleshooting Imperva WAF....1905
Troubleshooting Linux JBoss Server....1910
Troubleshooting Microsoft Enterprise CA....1926
Troubleshooting Microsoft Tomcat....1955
Troubleshooting MQServer Linux....1967
Troubleshooting MQServer Windows....1975
Troubleshooting MS SQL Windows....1981
Troubleshooting Nginx Server....1986
Troubleshooting NginxPlus ADC....1992
Troubleshooting Paloalto Firewall....1997
Troubleshooting Panorama Firewall....2002
Troubleshooting RabbitMQ Server....2006
Troubleshooting Rapid SB Server Inventory....2019
Troubleshooting Rapid SB Linux Server....2026
Troubleshooting Tomcat Linux....2045
Troubleshooting Weblogic Linux....2055
Troubleshooting Websphere Linux....2066
Troubleshooting Websphere Windows....2079
Troubleshooting Windows Apache Server....2086
Troubleshooting Windows JBoss Server....2092
Troubleshooting Windows Weblogic Server....2106
Chapter 7. CERT+ Automation Workflows User Guide....2114
Getting Started....2114
Prerequisites....2114
Role-Based Access Control....2115

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Accessing CERT+ Automation Workflows....2115
Accessing CERT Automation Workflow Tasks 2116
Certificate Expiry Workflows....2117
Overview....2118
Certificate Expiry Notification based on Certificate Attributes....2119
Certificate Expiry Notification - Cert Group Hierarchy....2121
Certificate Expiry Notification - Days....2123
Certificate Expiry Notification - Devices | Servers....2125
Certificate Expiry Notification....2128
Update Certificate Attributes....2129
Certificate Expiry Notification with JIRA....2131
Certificate Expiry Notification with ServiceNow....2133
Orphan Certificates Report....2135
Certificate Enrollment Workflows....2136
Overview....2137
Enroll Certificate and Download....2137
Certificate Provisioning with Notification....2143
Enroll Certificate Based on Policy | CSR Details | CSR Upload....2149
Create LTM SSL Profile and Enroll Certificate....2161
Enroll Certificate with Certificate Group and CSR Upload....2174
Enroll Certificate With ServiceNow....2176
Enroll Certificate and Push with ServiceNow....2183
Easy Certificate Provisioning....2190
Enroll Certificate with CAA Validation....2193
Enroll Certificate and Push 2199
Renew Certificate Workflows....2217
Overview....2218
Renew Certificate....2218
Regenerate Certificate with New CSR....2223

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Renew Certificate and Push.....2231
Renew Certificate with ServiceNow.....2238
Renew Certificate and Push with ServiceNow.....2243
Automation Workflow Tasks.....2248
Overview.....2249
Expiry Task.....2249
Enrollment Tasks.....2256
Renew Tasks.....2263
Push Tasks.....2278
Designing a Custom Workflow using OOB Tasks.....2285
Scheduling an OOB workflow.....2292
Customizing an OOB Workflow.....2292
Chapter 8. CERT+ Automation Workflows API Guide.....2294
Getting Started.....2294
Before you Begin.....2294
Login to retrieve active SessionId.....2295
Enroll Certificate and Download 2297
Overview.....2298
Request Structure.....2298
Payload.....2299
Response Structure.....2303
Status Codes.....2304
Sample Request/Response.....2304
Easy Certificate Provisioning 2307
Overview.....2307
Request Structure.....2307
Payload.....2308
Response Structure.....2309
Response.....2310

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes..... 2310
Sample Request/Response..... 2311
Enroll Certificate and Push 2313
Overview..... 2313
Request Structure..... 2313
Payload..... 2314
Response Structure..... 2321
Response..... 2321
Status Codes..... 2322
Sample Request/Response..... 2322
Enroll Certificate with ServiceNow 2325
Overview..... 2326
Request Structure..... 2326
Payload..... 2326
Response Structure..... 2331
Response..... 2332
Status Codes..... 2332
Sample Request/Response..... 2333
Enroll Certificate and Push with ServiceNow Integration..... 2335
Overview..... 2336
Request Structure..... 2336
Payload..... 2336
Response Structure..... 2341
Response..... 2342
Status Codes..... 2342
Sample Request Response..... 2343
Renew Certificate and Push 2345
Overview..... 2346
Request Structure..... 2346

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload ... 2347
Response Structure ... 2352
Response ... 2352
Status Codes ... 2353
Sample Request/Response ... 2353
Renew Certificate with ServiceNow Integration ... 2356
Overview ... 2356
Request Structure ... 2356
Payload ... 2357
Response Structure ... 2360
Response ... 2360
Status Codes ... 2361
Sample Request/Response ... 2361
Renew Certificate and Push With ServiceNow Integration ... 2364
Overview ... 2364
Request Structure ... 2364
Payload ... 2365
Response Structure ... 2369
Response ... 2369
Status Codes ... 2370
Sample Request/Response ... 2371
Regenerate Certificate - With New CSR ... 2373
Overview ... 2373
Request Structure ... 2373
Payload ... 2374
Response Structure ... 2379
Response ... 2379
Status Codes ... 2380
Sample Request/Response ... 2380

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Get Request Summary/Log..... 2383
Overview..... 2384
Request Structure..... 2384
Response Structure..... 2384
Status Codes..... 2385
Sample Request/Response..... 2385
Chapter 9. CERT+ Solution Guides.....2388
EST Client Configuration Guide - Linux and Windows.....2388
Overview..... 2388
Installation Steps.....2389
Downloading and Extracting the EST Client in Linux Machine..... 2390
Downloading and Extracting the EST Client in Windows Machine..... 2392
Configuring the AppViewX EST Client for Redistribution to End-Users (Linux and Windows).2394
Generator And Installer For EST Client in Linux Machine..... 2401
Generator and Installer for EST Client in Windows Machine.....2407
Available Commands and Features in EST Client.....2412
Keystore..... 2415
Troubleshooting Steps and Common Errors [Linux and Windows].....2418
Best Practices for Client.....2424
EST Server Configuration Guide.....2424
Getting Started.....2424
EST Configuration.....2431
Gateway - EST Logs..... 2435
Verification of the EST Server.....2436
Testing EST Enrollment by using CURL.....2436
SCEP Configuration Guide.....2438
Getting Started.....2438
SCEP Service Flow 2441
EST Enrollment.....2445

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX Server URL Details 2446
ACME Configuration Guide..... 2447
EST Client Authentication in Cloud Connector..... 2448
Certbot Configuration Guide..... 2448
Winacme Configuration Guide..... 2485
Posh-ACME Configuration Guide..... 2504
MSIntune Integration Guide..... 2533
Overview..... 2533
Simple Certificate Enrollment Protocol (SCEP)..... 2534
MS Intune AppViewX Connector..... 2534
Prerequisites..... 2535
Configuring the AppViewX SCEP MS Intune Agent..... 2542
Testing on the Windows v10.0 Device..... 2544
References..... 2552
Chapter 10. Glossary..... 2553

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Preface

Revision History

Revision	Description	Date
4.0	Updated draft of document for release 2023.1.0 FP2.1	March 2024
3.0	Updated draft of document for release 2023.1.0 FP2	February 2024
2.0	Updated draft of document for release 2023.1.0 FP1	November 2023
1.0	Initial draft of document for release 2023.1.0	September 2023

About this Guide

Welcome to the complete guide to perform Certificate Lifecycle Management (Discovery, Monitor, Enroll, Renew, Push, Regenerate, Reissue, Revoke, and Inventorize certificate) and manage organization PKI posture. CERT+ helps you to enroll and manage public and private certificates.

Audience

This guide is intended for CISO, PKI Security, and Application Teams.

Text Conventions

The following text conventions are used in this document:

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 1: CERT+ User Guide

AppViewX's CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CERT+, security teams can manage the certificate lifecycle from an intuitive single-pane management Interface. It enables the Certificate Lifecycle Management and Automation solution which helps enterprise IT manage and automate the entire lifecycle of their internal and external PKI. The key stages of the certificate lifecycle can be broken into the following stages:

• Getting Started
• Onboard Certificates
• Manage Devices
• Certificate Actions
• Managing the Certificate Inventory
• Certificate Reporting and Monitoring
• Alerts and Logs
• Standard Practices

Getting Started

• About AppViewX
• Getting Started with CERT+
• What's In It for you?
• Web Browser Prerequisites
• Accessing CERT+

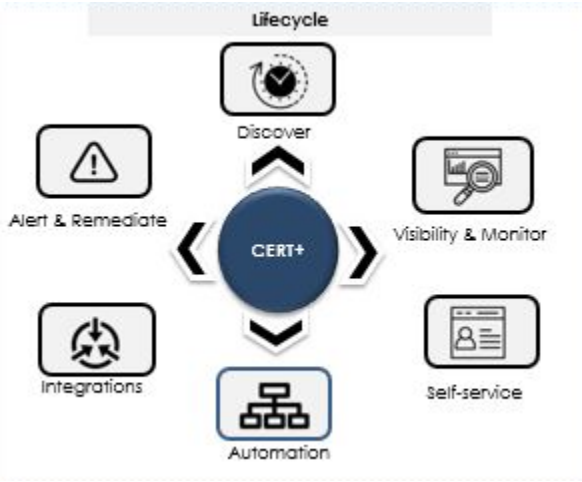
About AppViewX

AppViewX is an advanced cybersecurity and network management, automation, and orchestration platform for Enterprise IT. AppViewX Lifecycle Management Solution for Certificates on ADC or Load Balancers, Servers, Firewall, Cloud, Web Application Firewall (WAF), and enterprise mobility solution aims to avoid network outages due to unplanned certificate expiration and improve organization security posture. This remote monitoring and management platform helps network operations move faster, enforce compliance, eliminate errors, and reduce costs in the organization.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CERT+ Overview

AppViewX's CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CERT+, security teams can manage the certificate lifecycle from an intuitive single-pane management Interface. It enables the Certificate Lifecycle Management and Automation solution which helps enterprise IT manage and automate the entire lifecycle of their internal and external PKI. The key stages of the certificate lifecycle can be broken into the following stages:



- **Certificate Discovery & Inventory Management**: Allows users to discover certificates across the network and manage inventory of all certificates in one place.
- **Visibility and Monitoring**: Enables the user to monitor certificate expiry and usage. The monitored data is represented as a detailed report on the web portal along with options to trigger email alerts. Allows users to gain insights into certificates; monitor and take remedial action.
- **Certificate Enrollment**: Allows users to request certificates from a certificate authority (CA) which confirms their identity and generates a certificate.
- **Certificate Renewal**: Allows users to either manually or automatically renew a certificate before the expiry date by retaining the old private key.
- **Certificate Regeneration**: Allows users to enroll new certificates with similar parameters to an old certificate. When a user generates a new private key, the user can modify the parameters if required.
- **Certificate Reissuance**: Allows users to enroll new certificates with similar parameters to an old certificate. But the newly issued certificate comes with the same validity as the older certificate and can modify the parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Certificate Revocation**: Allows users to revoke a certificate in the event of certificate loss, compromise, or any other reason when the certificate is no more necessary for business.
- **Certificate Audit**: Track and audit the usage, creation, expiration, and revocation of certificates. Track user interaction with the platform.

What is Certificate Lifecycle Management (CLM)?

There is a growing need for organizations to allow and control only specific individuals, devices, machines to gain access to the network. The need for digital certificates to authenticate, identify and control who can access and operate on an organization’s network. Managing digital certificates across complex networks to ensure protection and prevent failures is a must for all businesses. CLM ensures continuous monitoring of digital certificates, with the ability to audit and keep track of expirations and renewals to avoid any service disruption. The digital certificate is a mechanism by which machines and individuals are identified and authenticated.

What is x.509 Digital Certificate?

The digital certificate is a mechanism by which machines and individuals are identified and authenticated. Digital certificates (x.509 certificates) are essential to establish trust and authenticate the identity of machines, people, and so on.

It helps to verify the identity between users in operation, servers, and other entities in a network. Also, identifies servers from whom the encrypted data is received, the signer of information, and helps to establish authenticity and integrity. The x.509 digital certificate protects information belonging to enterprises and their customers.

A digital certificate contains:

- Name of the certificate holder.
- Serial Number that is used to uniquely identify the service, individual, or entity identified by the certificate.
- Expiry date.
- Copy of the certificate holder's public key (used for decrypting messages and digital signatures).
- Digital Signature of the certificate-issuing authority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Authority

A Certificate Authority (CA) is also known as a certification authority or certificate issuer and is an establishment that validates the identities of certificate requestors and associates them to a cryptographic key through the issuance of electronic documents known as digital certificates.

Getting Started with CERT+

AppViewX CERT+

AppViewX's CERT+ provides extensive visibility into the certificate and encryption key infrastructure. It helps to protect the enterprise from security threats and outages due to the unavailability of service and expired certificates. The PKI and Application teams can self-service through automation, which delivers compliance and true business agility.

Key Features of the CERT+:

- Certificate Discovery
- Inventory and Management
- Dashboard for Visibility and Monitoring
- Certificate Actions for Enrollment and Provisioning
- Alerts & Logs
- Groups & Policies
- Administration

Certificate Discovery

An administrator can leverage CERT+ capabilities to identify certificates through various modes of discovery such as scanning a network to fetch certificates from AppViewX managed servers, devices, or certificates.

Inventory and Management

AppViewX Certificate Inventory is a repository of all the certificates discovered, uploaded, or enrolled via AppViewX. An administrator of the platform can configure role-based access control to an inventory of certificates through Certificate Groups.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Dashboard for Visibility and Monitoring

The dashboard is AppViewX's way of representing all the information about the certificates and certificate Hosting infrastructure. Users can leverage it to gain visibility into the PKI infrastructure and monitor for expiring certificates or compromises to the security posture of the organization. Users are capable of configuring custom widgets providing business-specific views into the Certificate infrastructure.

Certificate Actions for Enrollment and Provisioning

Certification Enrollment allows users to generate CSR, get a CSR signed by a CA, renew or regenerate a certificate, reissue certificate while Certificate Provisioning pushes a certificate to the device, and bind it to the application configurations.

Additional management actions to revoke a certificate, migrate certificates from one CA to another through CA switch, check for revocation status of a certificate using OCSP and SSL checker to validate the deployment of a certificate can also be leveraged by a user.

Alerts & Logs

CERT+ platform alerts you about the certificate expiring within a user-configured time and stores the information about events that have occurred or performed by a user for the certificate lifecycle management. The platform offers additional Alerts which monitor changes to the availability of a certificate on an endpoint. It avoids the unexpected expiration of certificates with alerts and notifications to save time and secure the enterprise network.

Groups & Policies

The certificates generated/discovered in the CERT+ platform can be logically grouped together for ease of management. All the certificate actions on a specific group can be restricted via role-based access control (RBAC). The platform comes prebuilt with a Default group to which all the certificates identified from Managed devices are associated. Groups are similar to a folder that stores the number of certificates with similar components.

The policy is a set of rules that can be enforced on a Certificate Group. A defined set of certificate parameters can be created as policies. This helps in enforcing security compliance over certificate creation across the organization. All the certificates discovered and inventoried are compared against the policy to identify non-compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Administration

This feature helps in administrative activities such as saving a certificate Keystore password into password vault, configuring auto-enrollment, certificate authority, device management, certificate profile, programmable certificate authority, programmable application endpoint, job scheduler, certificate attributes, email settings, and actions on an expired certificate and history of the certificate.

CLM Automation

Certificate automation enables you to automate the certificate lifecycle process across your enterprise through a configurable workflow engine. The platform allows to automate and orchestrate not just CLM actions above but also configure change and process automation defined by the organization processes.

What’s In It for you?

Overview

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

Discovery and Visibility

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

CLM Automation

- Access to a catalog of advanced automation workflows for certificate management.
- Build custom, event-driven automation using pre-built workflow tasks.
- Self-service automation workflows for easier policy-based certificate enrollment.
- Integrate with ITSM, ChatOps tools for holistic Incident and Change management, and notifications.
- Enforce custom expiration dates or enable auto-rotation of keys.

Cloud and DevOps

- Discover, manage and automate certificates across multi-cloud and container environments.
- Generate internal certificates for test applications before migrating to external certificates.
- Request any certificate and provision it to cloud key stores using a single interface.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Manage certificate enrollment and availability on Vault Keystores for containerized environments.
- ACME for easier certificate enrollment.

Secure Key Management

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

Certificate and Key Compliance

- Standardize certificate provisioning using self-service.
- Enforce organization standards through policies for complaince.
- Define granular role-based access control and enforce business-specific policies.
- Create audit trails for each user and certificate or key-related activity.
- Get the certificate and key logs on SIEM dashboards.

IoT and Enterprise Mobility Certificate Management

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

SSH Key Lifecycle Automation

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

Web Browser Prerequisites

Browsers	Version
Firefox	v74.0.1 (64-bit) or later
Google Chrome	v85.0.4183.83 (64-bit) or later

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Accessing CERT+

1. Login to AppViewX and from the upper left corner of the screen, click  (**Menu**).

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

2. From the menu displayed, select **CERT+**.
   The CERT+ home page is displayed. The menu is replaced with the menu for CERT+.

Onboard Certificates

- Prerequisites for Onboarding Certificates
- Certificate Discovery
- Discovery Status
- Excluded from Discovery
- Syncing Certificates with Network Devices or Servers

Prerequisites for Onboarding Certificates

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

Certificate Discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

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

- Network Scan
- Managed Devices Scan
- Transparency Log Scan
- Certificate Authority Scan
- Cloud Scan
- Scanning Uploaded Certificates
- On-demand Discovery
- Scheduled Discovery

Network Scan

A network scan is used to discover

- **digital certificates** within a network or infrastructure

  These certificates can include SSL/TLS certificates used for secure website communication, code signing certificates, client authentication certificates, and other types of digital certificates.

  For the certificates discovered, AppViewX also records details related to the issuing certificate authority and the discovery source.

- **network devices** (for example, servers, load balancers) from which the certificates were discovered

  These devices use the SSL/TLS certificates for secure communications.

  For the devices discovered, AppViewX records details like their IP address, operating system running on the device, device vendor name, and so on.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

• Initiating a Network Discovery Scan

Initiating a Network Discovery Scan

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

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

   Discovery run type options

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

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

   Field descriptions for on-demand discovery

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

   OR

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Field descriptions for scheduled discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

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

Field descriptions for discovering certificates from a IP range

Field	Description
***Start IP**	Enter the IPv4 address from which the network scan should start.
***End IP**	Enter the IPv4 address till which the network scan should run. **Note:** Ensure that the **End IP** value is greater than the **Start IP** value,
***IPs per Batch of Discovery**	Enter the number of IP addresses that should be scanned in one batch. **Note:** • A batch can include a maximum of 256 IP addresses. • Batching IP addresses for scanning in one go can be useful for throttling scan traffic.
***Scan Ports**	From the dropdown list, from the following options, select which ports have to be scanned: • **All Ports** • **Standard Ports**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	To get a list of the standard ports, click **Download here** from below the dropdown menu. • **Custom Ports**
Add More Ports	**Note:** This field is displayed only when **Scan Ports** = **Standard Ports**. To scan ports other than the standard ports, enter a comma-separated list of port numbers in this field. You can enter a hyphenated range of ports, as well as a comma-separated list of port ranges.
***Add Ports**	**Note:** This field is displayed only when **Scan Ports** = **Custom Ports**. Enter a comma-separated list of port numbers to be scanned from between 0 to 65535. You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges. For example: **444-666**, **888-999**.
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
SNI Hostname(s)	To discover certificates from SNI protected websites that share the same IP and port

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	number with another web application, enter the hostname in this field. You can also enter a comma-separated list of hostnames.
***TLS version(s)**	From the dropdown list, select the required TLS version.
Exclusion List	Select the list of entries to be excluded from the discovery operation. **Note:** • Only exclusion lists disabled here will be populated in this dropdown list. • Once you add the exclusion list a pop-up message appears as Discovery batches are re-adjusted since some of the entries are excluded from discovery based on the exclusion(s) selected to view the entries excluded. You can click **View** to view the excluded list.
Add	Click **Add** to add the network details entered. The entered details are displayed in the table shown after the **Select a File** field.
Exclusion List	Same as above
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Device discovery**	From the dropdown list, from the following options, select your device discovery requirement: • **Do not discover devices** Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed. • **Discover devices along with their operating system** AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed. **Note:** To discover the operating system version, AppViewX requires sudo access.
**: Mandatory fields*	

- **Subnet**

Field descriptions for discovering certificates from a subnet

Field	Description
***Network**	Enter the subnet/mask in the field. For example: **192.168.1.1/24**.
***Subnets per Batch of Discovery**	Based on the value entered, the provided subnet will be split into multiple batches for the discovery process.
***Scan Ports**	From the dropdown list, from the following options, select which ports have to be scanned: • **All Ports** • **Standard Ports**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	To get a list of the standard ports, click **Download here** from below the dropdown menu. • **Custom Ports**
Add More Ports	**Note:** This field is displayed only when **Scan Ports** = **Standard Ports**. To scan ports other than the standard ports, enter a comma-separated list of port numbers in this field. You can enter a hyphenated range of ports, as well as a comma-separated list of port ranges.
***Add Ports**	**Note:** This field is displayed only when **Scan Ports** = **Custom Ports**. Enter a comma-separated list of port numbers to be scanned from between 0 to 65535. You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges. For example: **444-666**, **888-999**
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
SNI Hostname(s)	To discover certificates from SNI protected websites that share the same IP and port

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	number with another web application, enter the hostname in this field. You can also enter a comma-separated list of hostnames.
***TLS version(s)**	From the dropdown list, select the required TLS version.
Exclusion List	Select the list of entries to be excluded from the discovery operation. **Note:** Once you add the exclusion list a pop-up message appears as Discovery batches are re-adjusted since some of the entries are excluded from discovery based on the exclusion(s) selected to view the entries excluded. You can click on the View hyperlink to view the excluded list.
Add	Click **Add** to add the network details entered. The entered details are displayed in the table shown after the **Select a File** field.
Exclusion List	Same as above
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Device discovery**	From the dropdown list, from the following options, select your device discovery requirement: • **Do not discover devices** Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed. • **Discover devices along with their operating system** AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed. **Note:** To discover the operating system version, AppViewX requires sudo access.
**: Mandatory fields*	

- **URL**

Field descriptions for discovering certificates from a URL

Field	Description
***URL**	Enter the HTTPS URL for discovering the associated certificate.
***Ports to Scan**	**Note:** This field is disabled if the **Scan All Ports** field is selected. Enter a comma-separated list of port numbers in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges.
Scan All Ports	**Note:** Enabling this field will disable the **Ports to Scan** field is enabled. Select the **Scan All Ports** checkbox to scan all the HTTPS-enabled ports. This is particularly useful if the number of HTTPS-enabled ports is significantly large or is unknown.
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
Add	Click **Add** to add the network details entered. The entered details are displayed in the table shown after the **Select a File** field.
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

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

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

Managed Devices Scan

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

A managed devices certificate scan is the process of scanning and managing digital certificates that are on the devices under the control of an organization. The purpose is for organizations to ensure the integrity of their security infrastructure and the prevention of security incidents.

AppViewX's managed devices certificate scan feature is built to handle the complete lifecycle of certificates deployed on managed devices (like ADC load balancers, servers, firewalls, WAFs, and so on) starting from discovery to renewal, revocation, and removal. This section outlines the steps for discovering certificates deployed on managed devices. AppViewX discovers certificates from managed devices and uses the SSL profile and virtual server to gather and retain details of the discovered certificates.

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

• Initiating a Managed Devices Scan

Initiating a Managed Devices Scan

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

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

   Discovery run type options

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

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

OR

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

Field descriptions for scheduled discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

3. In the **Discover By** section, from the **Discovery From** dropdown list, select the source for the certificate discovery.
   • **Managed ADCs**

Instruction for discovering certificates from Managed ADCs

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.
**: Mandatory fields*	

- **Managed Servers**

Instruction for discovering certificates from Managed Servers

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.
**: Mandatory fields*	

- **Managed MDMs**

Instruction for discovering certificates from Managed MDMs

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.
**: Mandatory fields*	

- **Managed Firewalls**

Instruction for discovering certificates from Managed Firewalls

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.
**: Mandatory fields*	

- **Managed WAFs**

Instruction for discovering certificates from Managed WAFs

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.

- **Internal**

Instruction for discovering certificates from internal devices

Field	Description
***Discovery From**	From the dropdown list, from the following options, select the source of the discovery: • **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**
Devices window	A list of all the managed devices is displayed in the devices window. Select devices to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Directories to Scan**	**Note:** This field is displayed only when **Discovery From** = **Managed Servers/Internal** From the following options, select one: • **Default**: Select this to discover certificates from the default configuration directory. • **Custom**: Select this to discover certificates from a custom configuration directory defined by the user.
Directory Name	If **Directories to Scan** = **Custom**, enter the name of the custom configuration directory in this field and click **Add**.
**: Mandatory fields*	

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

Field descriptions for the After Discover section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Transparency Log Scan

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for discovery details

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Field descriptions for the Discover By section

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

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

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

Certificate Authority Scan

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger a certificate authority scan:

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

Field descriptions for the Discover Details section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

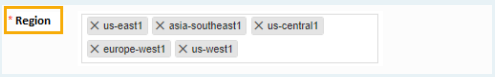
Field	Description
	• **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select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

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

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select the source for certificate discovery.
***Select CA**	From the dropdown list, select a CA to view its managed accounts in AppViewX for certificate discovery.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting version 2021.1.0, on selecting the ACM Private CA, the regions configured corresponding to the selected account are listed in the Region field. 
CA window	All managed CAs will be listed in this CA window. Select the CAs you want to discover certificates from. The CA window has the following option: • **Add as Favorites**: You can mark your frequently used CAs as favorites. • **All**: Select this to see the complete list of CAs (unfiltered). • **Selected**: Select this to list only the selected CAs. • **Unselected**: Select this to list only the unselected CAs. • **Delete**: Delete the required CA(s) from the favorites list.
Scan Type	**Note:** This field is displayed **Select CA** = **Microsoft Enterprise**. • **Aggressive**: To discover all certificates from the selected CA account, select **Aggressive**. • **Optimized**: To filter and discover certificates based on a specific discovery paramater, select **Optimized**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Discovery Parameters	For **Select CA** = **Entrust**: • For Entrust CA, AppViewX lets you set the following parameters for certificate discovery: certificate status and certificate type. • To filter the outcome of the certificate authority discovery for Entrust CA, from the **Discovery Parameters** dropdown list, select the parameter(s) . **Important:** The discovery parameters specified in the subsequent fields will take precedence over the **Associate Rule** specified in the **Discovery Rules** section. **Important:** If the certificates discovered basis the discovery parameters have associated root and/or intermediate certificates, those certificates will also be included in the results, irrespective of their type and status. For **Select CA** = **Microsoft Enterprise**: a. From the dropdown list, from the following options, select the discovery parameter on which you want to filter the certificates: • **RequesterName** • **Certificate Template** • **Common Name** • **Certificate Effective Date** • **Certificate Expiration Date** A corresponding text field/dropdown list, to enter/select the value for the selected discovery parameter, is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.

5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Cloud Scan

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

- Initiating a Cloud Discovery Scan for Azure
- Initiating a Cloud Discovery Scan for AWS
- Initiating a Cloud Discovery Scan for GCP

Initiating a Cloud Discovery Scan for Azure

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

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

Discovery run type options

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Field descriptions for on-demand discovery

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

OR

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

Field descriptions for scheduled discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click  . **OR**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Field descriptions for the After Discover section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Initiating a Cloud Discovery Scan for AWS

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

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

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

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

Field descriptions for on-demand discovery

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

OR

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

Field descriptions for scheduled discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

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

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

Initiating a Cloud Discovery Scan for GCP

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

   Discovery run type options

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

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

   Field descriptions for on-demand discovery

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

   OR

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

   Field descriptions for scheduled discovery

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Discover By section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Scanning Uploaded Certificates

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

To scan the uploaded certificate:

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

Field descriptions for the Discover Details section

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

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

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select the source of the discovery.
***Choose File**	You can upload a certificate file in one of the following formats: **.zip**, **.tar**, **tar.gz**, **.crt**, **.cer**, **.der**, **.p7b**, **.p7c**, **.pem**, **.pfs**, **.jks**, **.p12**. To upload a certificate file: a. Click **Upload** and navigate to the location of the required certificate file. b. Select the file and click **Open**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***File Password**	If the certificate file uploaded in **Choose File** is password-protected, in this field, enter the password for accessing the file.
Comments	Enter any additional remarksor details related to the process.
**: Mandatory fields*	

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

Field descriptions for the After Discover section

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Group**	From rthe dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

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

On-demand Discovery

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

There are two ways you can trigger a on-demand discovery:

- On-demand Discovery: Method 1
- On-demand Discovery: Method 2

On-demand Discovery: Method 1

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

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

On-demand Discovery: Method 2

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

To trigger a on-demand discovery:

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

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

   OR

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

   Field descriptions for the Discover Details section

Field	Description
***Discovery Run Type**	Select **On-demand**.
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** Character limit: **2000 characters**
**: Mandatory fields*	

4. In the **Discover By** section, from the **Discovery From** dropdown list, select the source of the discovery.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Based on your selection in this field, the rest of the fields will be displayed. For instructions on specifying the rest of the details:

Field descriptions for the Discover By section

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

Scheduled Discovery

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

There are two ways you can schedule a discovery process:

- Scheduled Discovery: Method 1
- Scheduled Discovery: Method 2

Scheduled Discovery: Method 1

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

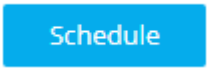
Click a scan type from the list above for instructions on how you can select on demand discovery for that type.

Scheduled Discovery: Method 2

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

To trigger a scheduled discovery:

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

   If this is the first scheduled discovery instance, click 

from the center of the page.

   OR

   Click 

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

Field descriptions for the Discover Details section

Field	Description
***Discovery Run Type**	Select **Scheduled**.
Discovery Instance Name	Enter the name of the discovery instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Discover By section

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

Discovery Status

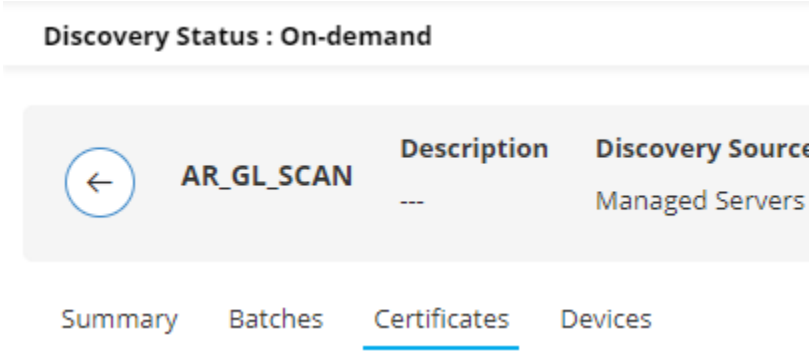
The discovery status section gives a summary of the on-demand and scheduled discoveries triggered. In addition to this, the discovered certificates can be filtered for their status, exclusion in the discovery list, and so on.

- Excluding Unmanaged Certificate
- Updating Discovered Certificates Status
- Exporting Details of Discovered Certificates
- Aborting Certificate Discovery
- Delta Discovery

Excluding Unmanaged Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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



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



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

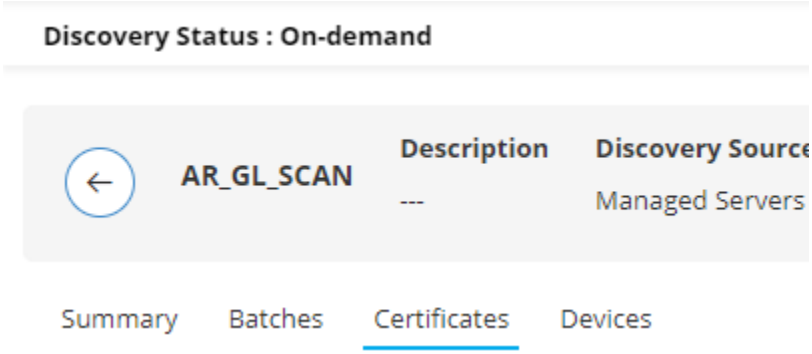
> **Note:** Excluded certificates will be removed from the current discovery instance and will be added to the **Excluded from discovery** inventory.

Updating Discovered Certificates Status

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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



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

Bulk Updating Discovered Certificates Status

To bulk update the status of the discovered certificates:

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Ignore**
- **Exclude**

5. To view details of the bulk certificate status update operation, go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Certificate Logs**.

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

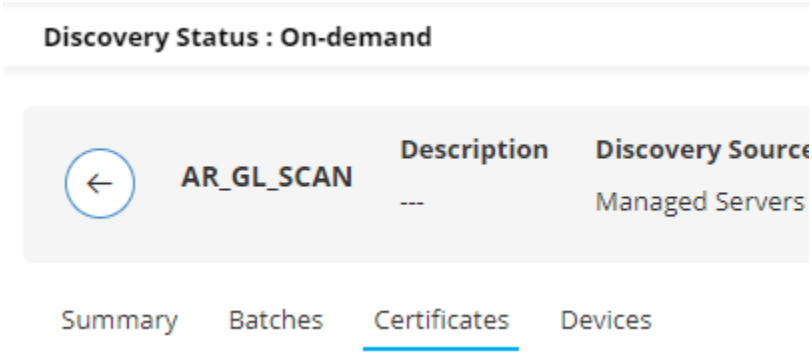
The tooltip text for the corresponding entry of this operation in the certificate log includes the complete details of the operation.

Exporting Details of Discovered Certificates

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

To export the details of discovered certificates:

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



4. From **Name**, select the checkbox for the certificate of which you want to export the details.
5. Click **Export**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Export** dialog box is displayed.

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

Aborting Certificate Discovery

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

Delta Discovery

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

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Excluded from Discovery

- Certificate
- Network

Certificate

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

To exclude certificates:

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

Network

For a network scan, AppViewX lets you create and manage exclusion lists. Exclusion lists are a list of IP addresses and/or subnets that have to be excluded from a network discovery scan. Exclusion lists are different from rules because, while rules let you exclude IP addresses after a discovery operation is completed, an exclusion list will do the same thing even before the discovery operation is triggered. AppViewX lets you:

- Creating an Execution List
- Disabling an Execution List
- Enabling an Execution List
- Deleting an Execution List

Creating an Execution List

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Excluded from Discovery** > **Networks**.
   The **Excluded from Network Scan** page is displayed.
2. Click **Create Exclusion List**.
   The **Excluded from Network Scan : Add** page is displayed.
3. Enter/Select the following details:

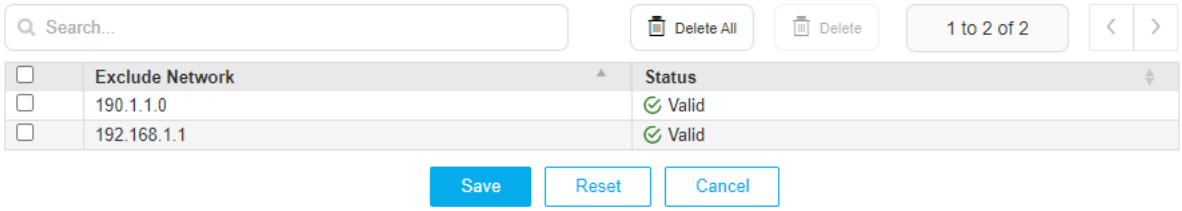
Field	Description
***Exclude List Name**	Enter a name for the exclusion list. **Important:** This field does not support special characters.
***Exclusion By**	Fom the dropdown list, select the source of the exclusion list from the following options: • **Custom**: Lets you enter a list of the required IP addresses and/or subnets to be excluded from the network scan • **Upload**: Lets you upload a file that has the IP addresses and/or subnets to be excluded from the network scan **Note:** To view a sample template for the **Upload** option: a. From this dropdown down, select **Upload**. The **Upload File** field is displayed. b. From below the **Upload File**field, click **Download Sample Template**. The sample template will be downloaded to your system.
***Exclude List**	**Note:** This field is displayed if **Exclusion By** = **Custom**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter a valid IP, subnet, IP range, or any combination of them. Listed below are examples of the acceptable formats: • Sample value for IP address: **192.168.1.1** • Sample value for subnet: **192.168.1.1/24** • Sample value for a range of IP addresses: **192.168.1.1 – 192.168.1.10**
***Upload File**	**Note:** This field is displayed if **Exclusion By** = **Upload**. **Note:** To view a sample template for the **Upload** option: a. From this dropdown down, select **Upload**. The **Upload File** field is displayed. b. From below the **Upload File**field, click **Download Sample Template**. The sample template will be downloaded to your system. To a upload a **.xlsx/.xls/.csv** file that has the exclusion list: a. Click **Upload**. b. Navigate to the location of the file and click **Open**.
**: Mandatory fields*	

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Click **Save.**
   If an excluded IP address/Subnet was previously discovered and is already part of the inventory, the current discovery operation cannot change that. The user will need to manually delete the certificates related to that entry from the inventory.

Disabling an Execution List

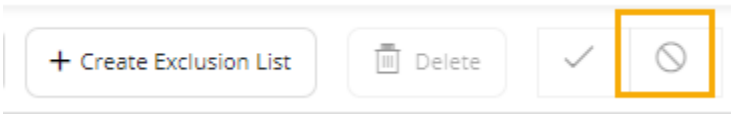
By default, exclusion lists are enabled as soon as they are created. Which means that when a network discovery operation is triggered, the results will exclude the IP addresses, subnets, and/or IP address ranges that are a part of the exclusion lists. To be able to select whether or not an exclusion list will be considered during a discovery operation, you need to disable an execution list here. Once you've disabled an execution list, at the time of configuring a network scan, it will be listed in the **Exclusion List** dropdown field, and you can choose if this list should be used during the scan.

To disable an execution list:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Excluded from Discovery** > **Networks**.
   The **Excluded from Network Scan** page is displayed.
2. Under **Exclude Network**, select the checkbox corresponding to the exclusion list you want to disable.

> **Note:** You can select more than one list at a time.

3. Click



.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. On the confirmation dialog box, click **Yes**.
   The **Status** for the selected exclusion list is updated to **Disabled**.

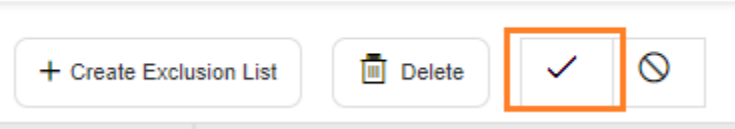
Enabling an Execution List

To enable an exclusion list after it has been disabled:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Excluded from Discovery** > **Networks**.
   The **Excluded from Network Scan** page is displayed.
2. Under **Exclude Network**, select the checkbox corresponding to the exclusion list you want to enable.

> **Note:** You can select more than one lists at a time.

3. Click .



4. On the confirmation dialog box, click **Yes**.
   The **Status** for the selected exclusion list is updated to **Enabled**.

Deleting an Execution List

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Excluded from Discovery** > **Networks**.
   The **Excluded from Network Scan** page is displayed.
2. Under **Exclude Network**, select the checkbox corresponding to the exclusion list you want to delete.

> **Note:** You can select more than one list at a time.

3. Click Delete .

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



4. On the confirmation dialog box, click **Yes**.
   The selected exclusion list(s) is deleted.

Syncing Certificates with Network Devices or Servers

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

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

Note: The device must be managed in AppViewX.

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

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

Viewing the Device and Certificate Synchronization Cron Job

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

Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Job Scheduler**.
The **Job Scheduler** page is displayed. The **Device and Certificate synchronization** cron job is listed on this page, along with its details.

Modifying the Device and Certificate Synchronization Cron Job

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Field descriptions for the details

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day(s) of the week on which you want the cron job to be triggered.
Summary	Displays a summary of the selections made for scheduling the cron job
**: Mandatory fields*	

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

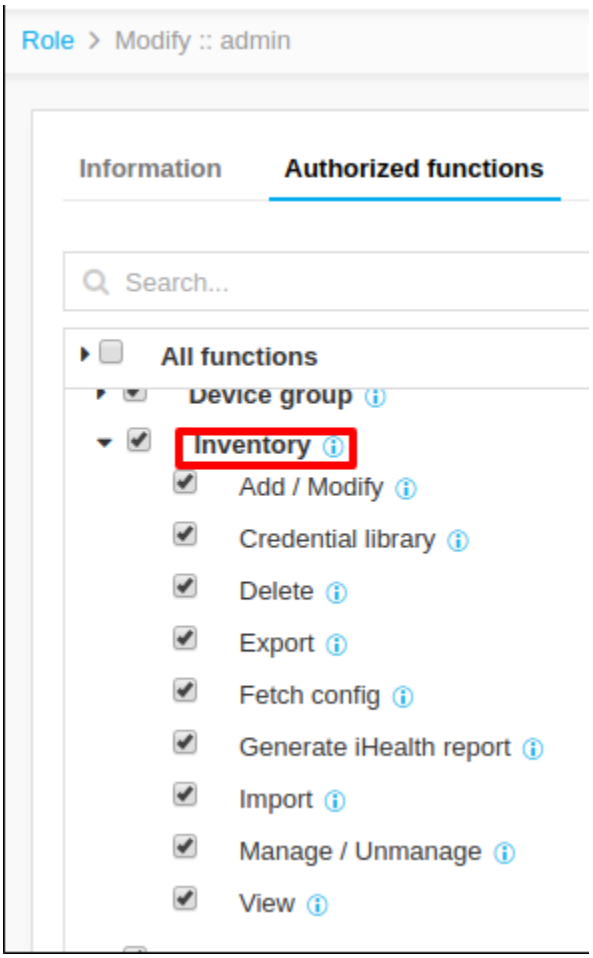
Manage Devices

- Inventory Actions
- Device Prerequisite
- ADC Prerequisite
- Firewall and Web Application Firewall (WAF) Prerequisite
- Server Prerequisite

Inventory Actions

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



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

Manually Fetch the Configuration for a Device

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To manually get the configuration for a device,

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

Delete Device

To delete the device from the inventory,

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

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

Export Device Details

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

To export the details of one or more devices,

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Import Devices

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

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

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Customizing Columns

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

To customize columns,

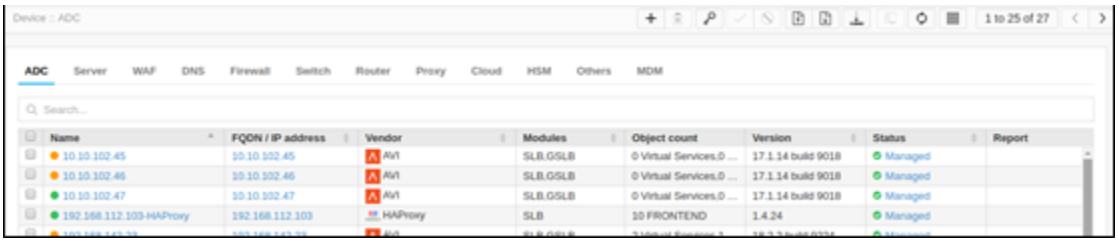
1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. Click the **Columns** icon in the Command bar.
   The **Columns** pop-up opens.
4. In the Columns pop-up, you can modify the columns by doing any of the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

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

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

Validating the Column selection

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



Manage Device

To manage devices,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

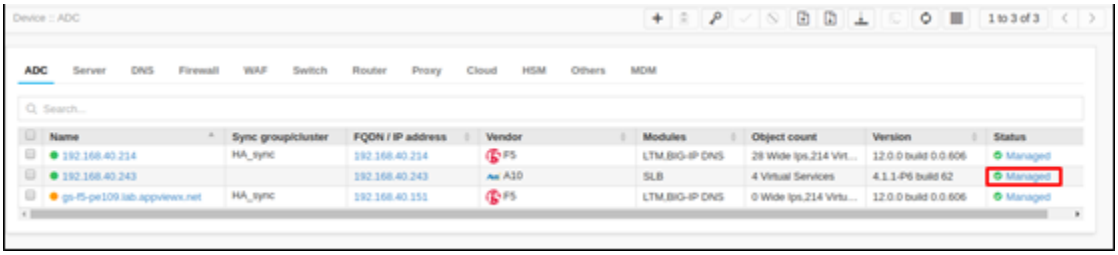
1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.

   By default, the **ADC** tab opens.
3. If the device you want to manage is not listed on the screen, run a search to locate it.

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

Validating the Manage Action

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

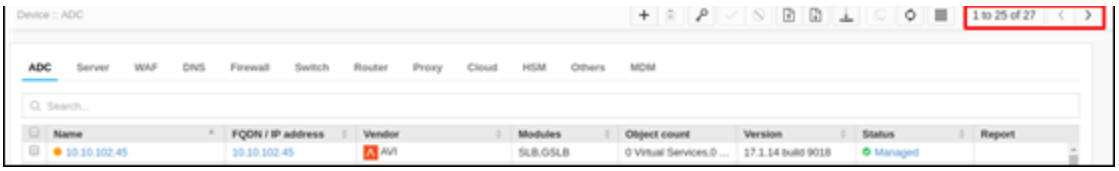


Pagination

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

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

   By default, the **ADC** tab opens.
3. Select the number of records to be displayed on the device inventory page.



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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Unmanage Device

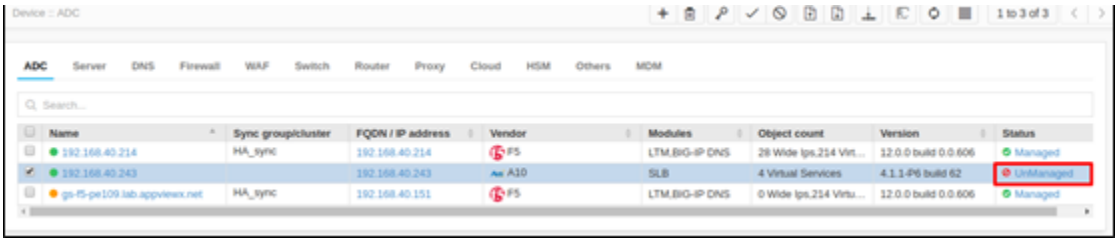
This action is being used to move the device to the unmanaged status from the managed status in the AppViewX application. If the devices are in ‘Unmanaged’ status, the midnight config fetches, and other features like Syslog, Statistics, Write actions will be disabled for those devices.

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

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

Validating the Unmanaged Action

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



Device Prerequisite

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

ADC Prerequisite

Supported Vendors	A10	AVI	Akamai	Amazon ELB	BigIQ	Cisco
IP Address/ FQDN	IP Address/ FQDN	IP Address/ FQDN Note: Device must not be added with Cluster IP.	Not Applicable	Not Applicable	IP Address	IP Address
User Privilege	• CLI/ WEB/ xAPI access • Read/ write access	• Super-user access • System admin role for all the tenants.	• Client token • Client Secret • Access Token • Host URL	• Access Key • Secret Key • Region	• Username/ Password • Credential List • AppViewX/ CyberArk	• Username/ Password
Enable Password	Required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	Not Applicable
Services and Prot for AppViewX communication	Port number: 22, 88, and 443	Port number: 22, 443, and 5514 (to receive Syslog on	Port number: 443 (Outbound from AppViewX to Manage Device and	Port number: 443 (Outbound Internet access is required to	Port number: 22 (SSH)	• Outbound Access from AppViewX

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	A10	AVI	Akamai	Amazon ELB	BigIQ	Cisco
		AppViewX from AVI)	Perform Akamai Actions.)	manage the ELB in AWS.)		for SSH service • HTTPS service
Internet Access/Proxy if required	Not Required	Not Required	Required	Required	Not Required	Required, if needs to be accessed with a Public IP address.
Location from which the certificates are discovered if Certificate Managed	No specific location	No specific location(use API's to get certificate details)	Not Applicable	Not Applicable (Certificates that are assigned to the listeners will be discovered by AppViewX)	CERT+ Discovery is not supported	CERT+ Discovery is not supported

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Citrix	F5	HAProxy	NginxPlux	Infoblox LBDN
IP Address/ FQDN	IP Address/ FQDN	IP Address/ FQDN	IP Address	IP Address/FQDN	IP Address/ FQDN
User Privilege	• Super-user access. • Username/ Password • Credential List • AppViewX/ CyberArk	• Admin access • TMSH access • Username / Password • Credential List AppViewx/ CyberArk	• Username / Password • Credential List AppViewx/ CyberArc	Access to Nginx Installed configuration locations and access to check the syntax of Nginx. conf and restart the Nginx service to apply changes.	• Super-user access or • Access to LBDN objects that need to be managed from AppViewX
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Yes	Yes	Yes	Not Applicable
Services and Prot for AppViewX communication	• Outbound Access from AppViewX for SSH & HTTPS service (Default/ Custom Port Information is required) • Outbound access to	Port number: 22 and 443	Port number: 22 (SSH)	Port number: 22 and any custom port for stats	Port number: 443 or custom port to access API calls

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Citrix	F5	HAProxy	NginxPlux	Infoblox LBDN
	port 5514 is required for Citrix Device to forward the Syslog to AppViewX				
Internet Access/Proxy if required	Required, if needs to be accessed with Public IP address.	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed	Certs are parsed only from /flash/ nsconfig/ssl/ directory	/config/ filestore/ files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/ pki/tls/certs/ V10 /config/ssl/ ssl.crt/ /etc/ httpd/conf/ ssl.crt/ /etc/ pki/tls/certs/	CERT+ Discovery is not supported	/etc/nginx/conf.d/ or any custom location	Not Applicable

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Firewall and Web Application Firewall (WAF) Prerequisite

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required
Services and Prot for AppViewX communication	Port number: 22 (SSH)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH, till R77) and 443 (API, from R80)
Internet Access/ Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH.	Not supported	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are /web/ conf/server.crt

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
					/web/conf/ server.key
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Not Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required
Services and Prot for AppViewX communication	Port number: 22 (SSH, till R77) and 443 (API, from R80)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH) and 443 (API)
Internet Access/Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are /web/conf/ server.crt /web/conf/ server.key	Certificates are fetched by issuing a direct command to device through SSH.	Not supported	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10 /config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10 /config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Server Prerequisite

Supported Vendors	APACHE	APACHE Tomcat	Microsoft IIS	Microsoft PC	Microsoft Server	Oracle Weblogic
Operating System	All Linux Flavour	All Linux Flavour	Windows	Windows	Windows	All Linux Flavour

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	APACHE	APACHE Tomcat	Microsoft IIS	Microsoft PC	Microsoft Server	Oracle Weblogic
IP Address/ FQDN	IP Address	IP Address	FQDN	FQDN	FQDN	IP Address
User Privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Local admin or Domain Admin	• Username / Password • Local admin or Domain Admin	• Username / Password • Local admin or Domain Admin	• Username / Password • Admin or sudo user privilege
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Services and Port for AppViewX Communication	Port number: 22 (SSH)	Port number: 22 (SSH) and Reset Port	Port number: 5985 (Powershell), 135 (Native API/WMI) , 445 (network drive), and 8999 (Appviewx agent port)	Port number: 5985 (Powershell), 135 (Native API/WMI) , 445 (network drive), and 8999 (Appviewx agent port)	Port number: 22 (SSH)	Port number: 22 (SSH)
Internet Access / Proxy If Required	Not Applicable	Not Applicable	Need access to Agent installed in Client env	Need access to Agent installed in Client env	Need access to Agent installed in Client env	Not Applicable
Enter Path/ Location	Customized	Customized	Not Applicable	Not Applicable	Customized JKS	Yes, Weblogic Dir path

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	APACHE	APACHE Tomcat	Microsoft IIS	Microsoft PC	Microsoft Server	Oracle Weblogic
Location from which Certificates are discovered If Certificate managed	Certificates defined under Virtualhost of <httpd.conf> File location	Certificates defined under Connector tag of <server.xml> File location	Windows Store	Windows Store	JKS File location	Keystore/ truststore entry defined in <config.xml> File location
Supported SNI feature	Yes	No	No	Not Applicable	Not Applicable	No
Multiple Instance Support	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	Yes
Supported Cert Format	<.pem>, <.crt>, and <.cer>	<.pem>, <.crt>, <.cer>, <.jks>, <.keystore>, and <.truststore>	<.pfx>	<.pfx>	<.jks>	<.jks>

Supported Vendors	Oracle IPlanet	IBM Websphere	IBM Data Power	Linux	Domino
Operating System	All Linux Flavour	All Linux Flavour	All Linux/ Windows flavour	All Linux Flavour	Windows

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Oracle IPlanet	IBM Websphere	IBM Data Power	Linux	Domino
Supported Cert Format	<.jks>	<.jks>	All format of certificates(except <jks> and <kdb>)	All format of certificates	All format of certificates

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Certificate Actions

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

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

- Enrolling Certificates
- Renewing Certificates
- Pushing Certificates to Devices
- Reissuing Certificates
- Revoking Certificates
- Regenerating Certificates
- Reinstating Certificates
- Running Revocation Check-OCSP
- Generating Certificate Signing Request (CSR)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

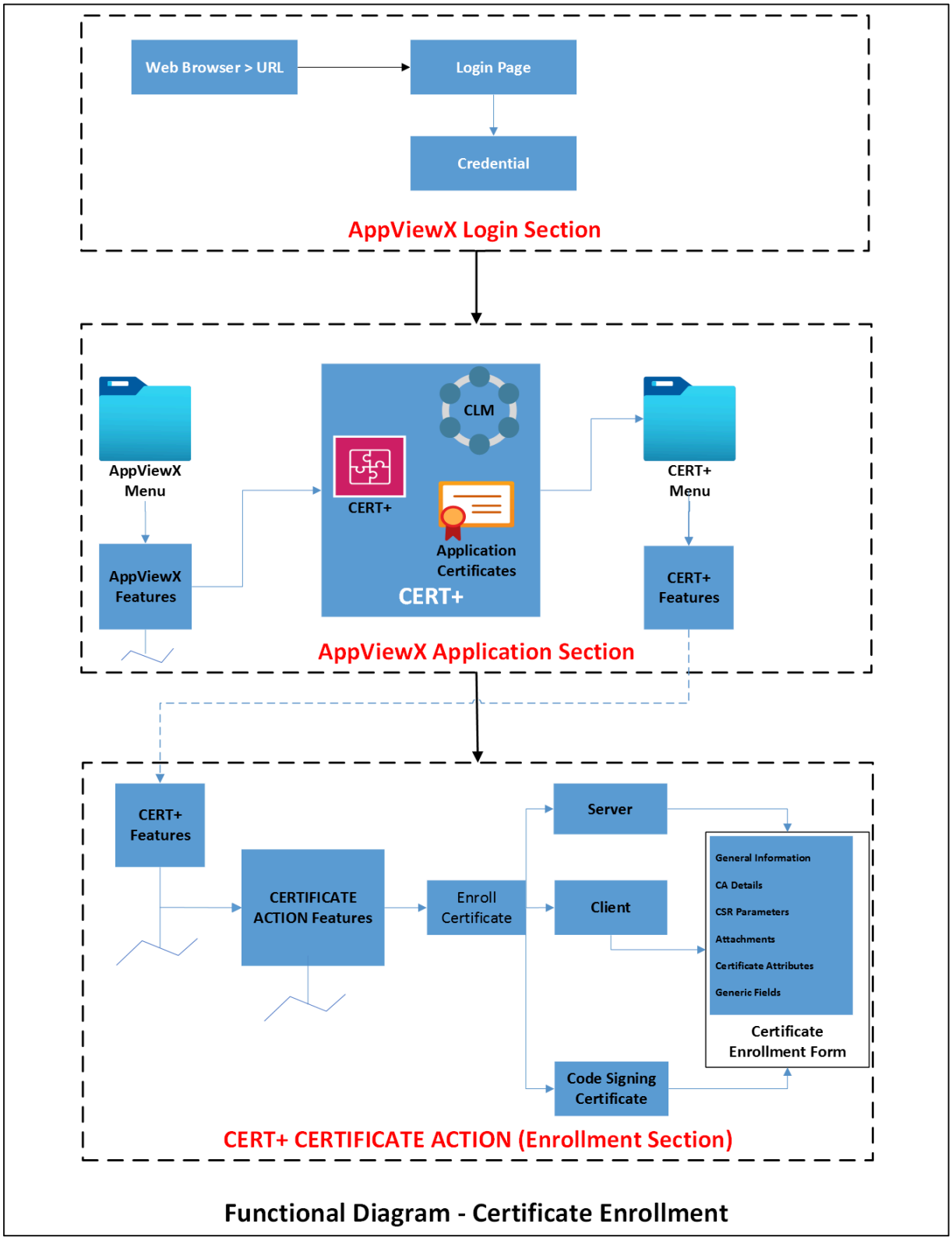
- Migrating CAs (CA Switch)
- Running the SSL Checker for a Certificate

Enrolling Certificates

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Functional Diagram - Certificate Enrollment

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Enrolling a Server Certificate

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

To enroll a server certificate:

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

Field descriptions for the CA Details section

Options	
***Certificate Authority**	From the dropdown list, select IDnomic. **Note:** For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Cer
***Renew Automatically**	**Note:** Changing the group inherited renew period overwrites the renewal period for this certifica Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submi
Certificate Type	From the dropdown list, select the required certificate type.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate willl be enrolled.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this fi From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a CA+RA setting is se From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Connector Name**	Enter the friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to po a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. • **HSM**: **Note:** This option is disabled when **Certificate Authority** = **Google**. To generate the private key and the CSR, based on the CSR parameters given, in an HSM device: a. Under **CSR Generation**, select **HSM**. b. Fields for gathering your HSM-related inputs are displayed. **To generate the private key and the CSR, enter/select the following details:**

Field
***Device Type**
***Vendors**
***Devices**
***Key Handler Name**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	

Field
***Key Reference Name**

- **End Point**:



Note: This option is disabled when **Certificate Authority** = **Google**.

To generate the private key and the CSR in the selected end point device, enter/select the foll

Field
Category
Vendor
***Devices**
Tenant

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Field
	CSR Location
	Partition
	***CSR File Name**
	***Key File Name**

**: Mandatory fields*

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
Procedures	**Note:** This field is applicable only when **Certificate Authority** = **Nexus CA**. From the dropdown list, select the required procedure. In addition to the default procedure, the dropdown list displayes only the procedures mapped to the server.
**: Mandatory fields*	

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

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter/From the dropdown list, select the Subject Alternative Name for the certificate being enrolled. You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Multiple values must be separated by a comma. • The cumulative count SANs is displayed in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	Enter a valid email address of the person responsible for maintaining the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group’s policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

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

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you've uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

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

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

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

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)
Certificate holder Email	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policiesconfigured for the requested workflow
First name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters for their operational purposes.
   - By default, the **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section).
   - The **Certificate ID** can be modified by the user.
   - If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**.
   - If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.
10. Click **Add**.

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

    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.

13. Click **Approve** to proceed.



The **Approve** dialog box is displayed.

14. Enter your comments in the text field.

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

15. Click **Yes**.

Once the approval process is complete, the **Implement** option is displayed in the holistic view.

16. Click **Implement**.



The **Implement** dialog box is displayed.

17. Enter your comments in the text field.

If the workflow request has to be implemented automatically in the future, click **Schedule later** .

18. Click **Yes**.

CSR Submission to CA is in progress.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

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

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

Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

Enrolling a Client Certificate

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

Note: These certificates cannot be hosted on clients.

To enroll a client certificate:

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Options	

***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed.
	
	From the dropdown list, select the required certificate authority (CA).
	
	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an erro
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details**
	
	Note: The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Cer

***Renew Automatically**	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certifica
***CA Account**	To which account the enrollment request to be submitted.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.  **Note:** This field will be shown only for Digicert CA.
Certificate Profile	 **Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this fi From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	 **Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a CA+RA setting is se From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown.  **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown.  **Note:** This is applicable only for Google CA.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the hol
Description	Enter the description in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	
	Note: Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **UploadCSR** - Uploaded CSR will be taken as a source to populate CSR parameters and submit to C • Click the **Browse** button, and then the file. • Click the **Upload** button to upload the selected file. • On uploading CSR successfully, CSR parameters are automatically filled in the CSR section. • **HSM** - Private key and CSR will be created in the selected HSM device based on CSR parameters g

Field	
*Device Type	Select the type of device as required. The possible options are: • HSM Devices • ADC Devices.
*Vendors	Select the desired vendors from the dropdown list. The possible vendors are when device selected as HSM Dev • Fortanix • PKCS11 The possible vendors are when device selected as ADC Dev • Safenet • Thales • Fortanix

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	

Field	
*Devices	Select the desired device from the dropdown list. **Note:** • By default, the **None Selected** option is enabled. • When Device Type = ADC - User chooses from th
*Key Handler Name	Enter the desired handler name in the field.
*Key Reference Name	Enter the Key Reference Name. **Note:** This field appears only when Device Type = AD

• End Point - Private key and CSR will be created in the selected End Point device based on CSR par

Field	
Category	Select the desired category from the dropdown list. The possible options • ADC • Server • Firewall.
Vendor	Select the desired vendor from the dropdown list. The possible options ar • AVI • Citrix • F5 • Ngnix Plus • HAProxy. **Note:** Vendor list is populated based on the category, select the de
***Devices**	Select the desired device from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	
	Field
	Note: By default, the None option is selected.
	Tenant
	Enter the tenant id in this field.
	Note: This field appears when you select category as ADC.
	***CSR file name**
	Enter the name of the CSR file in this field.
	Note: This field appears when you select category as Server.
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certifica
	***Partition**
	Enter the partition in this field.
	Note: This field appears when you select category as Firewall.
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certifica
	***Key File Name**
	Enter the name of the key file in this field.
	Note: For all CA types except Amazon, you have the option to generate the CSR. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters giv
**: Mandatory fields*	

4. Only for the EJBCA CA, enter/select the **Vendor Specific Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Vendor Specifc Details section.

Field	Description
End entity user name	Enter the name of the end entity.
*** End Entity Profile Name**	Select the profile name from the dropdown list.
*** User Common Name**	Select the common name from the dropdown list.
*** Certificate Profile Name**	Select the certificate profile name from the dropdown list.
**: Mandatory fields*	

Note: Enhancement for 22.1.0 FP1 - While enrolling for a Nexus CA policy, the vendor specific details section will have the Procedures dropdown displaying only those procedures mapped to server and the default procedure.

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

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. Select the subject alternative subject name from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

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

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

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

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)
Certificate holder Email	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policiesconfigured for the requested workflow
First name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters for their operational purposes.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

10. Click **Add**.

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

    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.

    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.



    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

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

15. Click **Yes**.

    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Implement** dialog box is displayed.

17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

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

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

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

Enrolling a Code Signing Certificate

Code Signing certificate enrollment refers to the process of creating a digital ID for a code or document. It starts with the generation of a key pair (private and public key) and CSR and then submitting the CSR to the desired CA to procure a certificate. CERT+ supports the generation of key pair on the device, HSM, and AppViewX. You can also upload the CSR for enrolling for a digital certificate.

Note: These certificates cannot be hosted on servers.

To enroll a code signing certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

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

Field descriptions for the CA Details section

Options	Description
***Certificate Authority**	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA de • Digicert MPKI • GlobalSign SSL • GlobalSign MSSL • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Any Other Programmable CA configured by the user.
***Renew Automatically**	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certifica
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	Select the Profile to which the Certificate must enroll. **Note:** This field is applicable only for AppViewX CA and Google CA.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the hol
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **UploadCSR** - Uploaded CSR will be taken as a source to populate CSR parameters and submit to C • Click the **Browse** button, and then the file. • Click the **Upload** button to upload the selected file. • On uploading CSR successfully, CSR parameters are automatically filled in the CSR section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>• HSM - Private key and CSR will be created in the selected HSM device based on CSR parameters g
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>Select the type of device as required.

The possible options are:
• HSM Devices
• ADC Devices.</td></tr>
<tr><td>*Vendors</td><td>Select the desired vendors from the dropdown list.

The possible vendors are when device selected as HSM Devices:
• Fortanix
• PKCS11

The possible vendors are when device selected as ADC Devices:
• Safenet
• Thales
• Fortanix</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.

Note:
• By default, the None Selected option is enabled.
• When Device Type = ADC - User chooses from the list based on</td></tr>
<tr><td>*Key Handler Name</td><td>Enter the desired handler name in the field.</td></tr>
<tr><td>*Key Reference Name</td><td>Enter the Key Reference Name.</td></tr>
</table></td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Description

Field	Description
	Note: This field appears only when Device Type = ADC Devices.

• End Point - Private key and CSR will be created in the selected End Point device based on CSR par

Field	Description
Category	Select the desired category from the dropdown list. The possible options are: • ADC • Server • Firewall.
Vendor	Select the desired vendor from the dropdown list. The possible options are: • AVI • Citrix • F5 • Ngnix Plus • HAProxy. **Note:** Vendor list is populated based on the category, select the desired ver
***Devices**	Select the desired device from the dropdown list. **Note:** By default, the None option is selected.
Tenant	Enter the tenant id in this field. **Note:** This field appears when you select category as ADC.
***CSR file name**	Enter the name of the CSR file in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Description
	Field / **Description** **Note:** This field appears when you select category as Server. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this fi *__Partition__ Enter the partition in this field. **Note:** This field appears when you select category as Firewall. *__Key File Name__ Enter the name of the key file in this field. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this fi **Note:** For all CA types except Amazon, you have the option to generate the CSR. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters giv
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: While enrolling certificates with policies using Google CA, the following points must be considered

Certificate Enrollment - Strict Policy

- The Common Name will not be pre-filled from the policy.
- The following validation will be seen based on strict policy guidelines.
  - If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.

Certificate Enrollment - Suggestive Policy

- The Common Name will not be pre-filled from the policy
- The following validation will be seen based on strict policy guidelines.
  - If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
  - If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.

4. Only for the EJBCA CA, enter/select the **Vendor Specific Details**.

Field descriptions for the Vendor Specifc Details section.

Field	Description
End entity user name	Enter the name of the end entity.
*** End Entity Profile Name**	Select the profile name from the dropdown list.
*** User Common Name**	Select the common name from the dropdown list.
*** Certificate Profile Name**	Select the certificate profile name from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

Note: Enhancement for 22.1.0 FP1 - While enrolling for a Nexus CA policy, the vendor specific details section will have the Procedures dropdown displaying only those procedures mapped to server and the default procedure.

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

Field descriptions for the CSR parameters

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

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

Field descriptions for the Attachments section

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

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)
Certificate holder Email	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policiesconfigured for the requested workflow
First name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters for their operational purposes.
   - By default, the **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section).
   - The **Certificate ID** can be modified by the user.
   - If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**.
   - If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.
10. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.

11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.



    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

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

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Implement** dialog box is displayed.

17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.

    Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

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

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

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

Renewing Certificates

Important: A IDnomic CA certificate can be renewed only if the certificate enrollment is done using a Registration Authority (RA) setting.

Digital certificates are issued with a limited validity period. Before the expiration of their validity, the certificates have to be renewed and placed on the server for service continuity. The renewal process is specific to CAs, depending on their operations. The result is be the issuance of the certificate with extended validity. CERT+ enables you to trigger certificate renewal in different ways. You can trigger renewal from the certificate inventory or the certificate details and its provisioned details can be verified and trigger the renewal from a holistic view. Group policy auto-renewal takes care of the certificate renewal automatically and it can be combined with auto-push for hassle-free automation.

Note: You can renew the certificates via the Certificate Inventory section also.

Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

- Renewing a Server Certificate
- Bulk Renewing Server Certificates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Renewing a Client Certificate
• Renewing Certificates via the Process Explorer

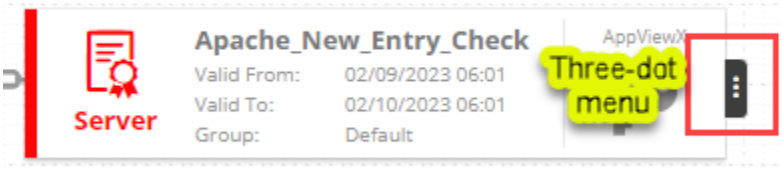
Renewing a Server Certificate

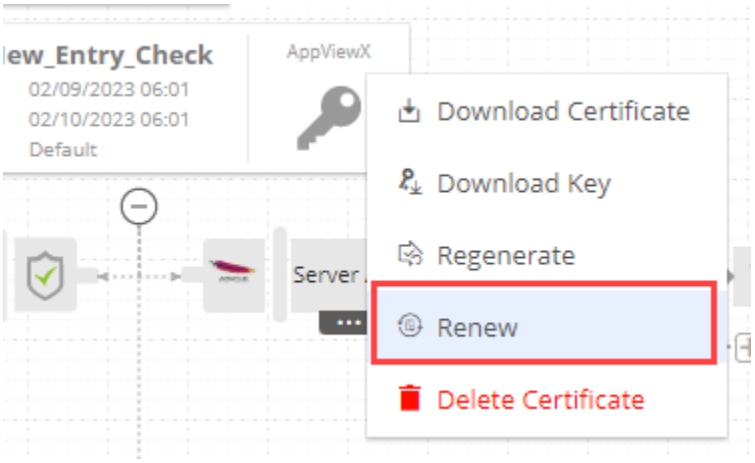
Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

If you are renewing a single certificate, you can trigger the renewal from the holistic view as they can verify all the details before initiating the renewal.

To renew a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To open the holistic view of a certificate, under **Common Name**, select the required certificate name.
3. From the three-dot menu for the certificate, click **Renew**.





   The **Server Certificate** > **Renew** page is displayed. The fields on this page are displayed depending on the type of certificate and the issuing cetificate authority.
4. On the **Server Certificate > Renew** page, update the renewal details if and as required.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Starting version 2023.1.0 FP2, for certificates issued by Entrust and Microsoft, you can upload a new CSR in the **CSR Generation** field.

- If you are uploading a new CSR, ensure that the new and existing **Common Name** in the **CSR Parameters** are the same.

5. Click **Renew**.

   The **Renew** dialog box is displayed.
6. Enter your comments in the text field and click **Yes**.

   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
7. Click **Approve** to proceed.



   The **Approve** dialog box is displayed.
8. Enter your comments in the text field.

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

9. Click **Yes**.

   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
10. Click **Implement**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Implement** dialog box is displayed.

11. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
12. Click **Yes**.
    The renewal process is triggered. After renewal is completed, the workflow status updates to **Completed**.

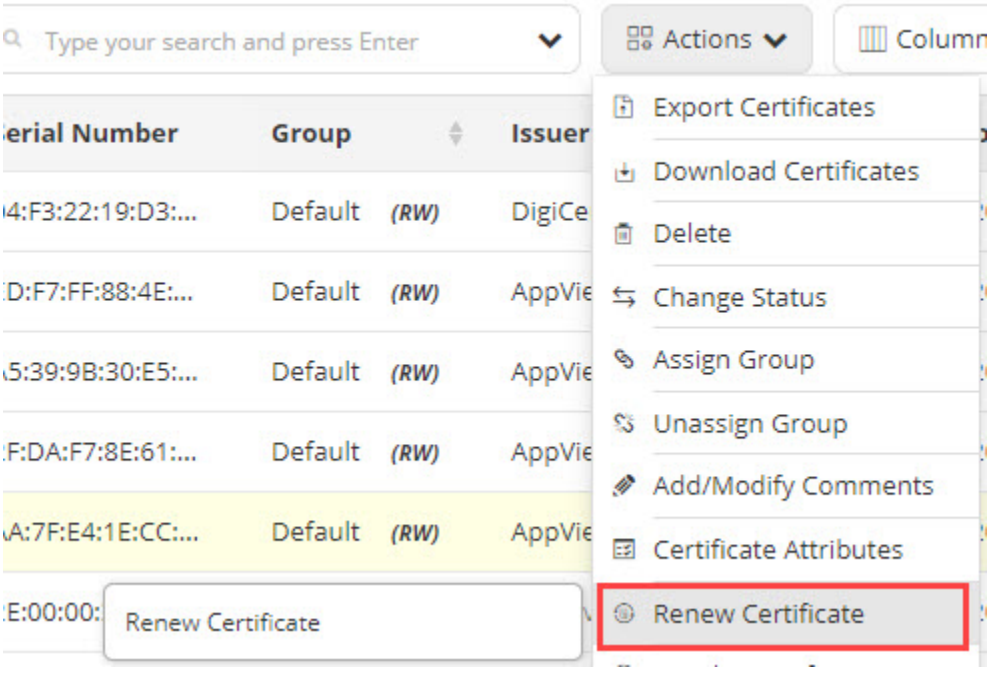
Bulk Renewing Server Certificates

Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

Bulk renewal of the certificates can be triggered from the inventory by selecting more than one certificate.

To renew server certificates in bulk:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. Under **Common Name**, select the checkboxes corresponding to all the certificates you want to renew.
3. From the **Actions** dropdown menu, click **Renew Certificate**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Renew Certificate** dialog box is displayed.

4. From the following options, select when do you want to **Renew Selected Certificate(s)**:
   a. To immediately renew the selected certificate(s), select **Now**.
      • Certificate renewal request, for the selected certificate(s), will be triggered immediately.

> **Note:**
> • Certificates with the work order status in progress or with read-only permission will be skipped.
> • In case of Digicert certificates, the certificates will be auto-reissued unless the Order validity is expired.

   OR
   b. To schedule an automatic renewal for a later time, select **Set auto-renew**.
   c. In the **Renew Certificates** _____ **Days before Expiry** field, to specify how many days before their expiry the selected certificate(s) should be renewed, enter a value between **1** and **120**.
      • Assuming that you have entered **120** in this text field, certificates with validity less than 120 days will be triggered for renewal within the next **6 hours**.

> **Note:**
> • Certificates with the work order status in progress or with read-only permission will be skipped.
> • In case of Digicert certificates, the certificates will be auto-reissued unless the Order validity is expired.

5. Click **Submit**.
   Depending on the selections made in the **Renew Certificate** dialog box, the certificate renewal process will be triggered.

> **Note:** The status of the renewal process is monitored using the process explorer.

Renewing a Client Certificate

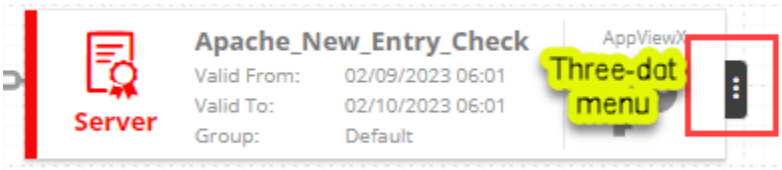
Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

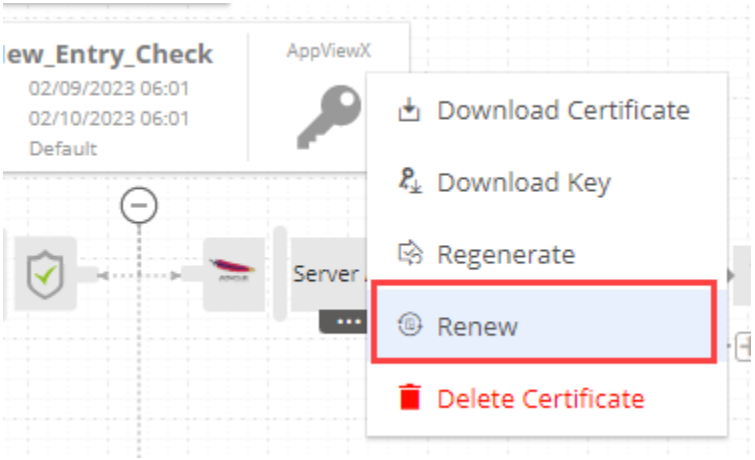
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

If you are renewing a single certificate, you can trigger the renewal from the holistic view as they can verify all the details before initiating the renewal.

To renew a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Client**.
   The **Client Certificate** page is displayed.
2. To open the holistic view of a certificate, under **Common Name**, select the required certificate name.
3. From the three-dot menu for the certificate, click **Renew**.





   The **Client Certificate** > **Renew** page is displayed. The fields on this page are displayed depending on the type of certificate and the issuing certificate authority.
4. On the **Client Certificate > Renew** page, update the renewal details if and as required.

> **Note:** Starting version 2023.1.0 FP2, for certificates issued by Entrust and Microsoft, you can upload a new CSR in the **CSR Generation** field.
> - If you are uploading a new CSR, ensure that the new and existing **Common Name** in the **CSR Parameters** are the same.

5. Click **Renew**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Renew** dialog box is displayed.

6. Enter your comments in the text field and click **Yes**.
   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
7. Click **Approve** to proceed.



The **Approve** dialog box is displayed.

8. Enter your comments in the text field.

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

9. Click **Yes**.
   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
10. Click **Implement**.



The **Implement** dialog box is displayed.

11. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
12. Click **Yes**.
    The renewal process is triggered. After renewal is completed, the workflow status updates to **Completed**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Renewing Certificates via the Process Explorer

The **Process Explorer** is a listing of all certificates that are scheduled for renewal on that day and the certificates that are awaiting approval. Once a certificate is renewed, it is removed from this listing. The **Process Explorer** is useful for monitoring the renewal status especially in the case of bulk renewals.

To access the process explorer:

Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Process Explorer**.
The **Renew Certificate** page is displayed.

Pushing Certificates to Devices

Pushing certificates refers to the automated distribution and deployment of digital certificates. You can enable certificates to be pushed at the time of adding an application connector.

Note: Users can push certificates to Akamai CPS only when the CSR is generated on the end point.

- Adding Application Connectors
- Pre - and Post - Push Script Usage Steps
- Pushing a Server Certificate to a Device
- Pushing a Client Certificate to a Device
- Pushing an Intermediate Certificate to a Device
- Pushing a Root Certificate to a Device

Adding Application Connectors

An application connector is a software application running on a server. To add the application connector the application should be managed under the AppViewX device inventory. All the supported devices in the AppViewX inventory can be provisioned with the certificate by adding the connector. The connector enables certificate provisioning for cloud-managed devices.

Note: Users can push certificates to Akamai CPS only when the CSR is generated on the end point.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The following sections will take you through the steps for creating application connectors for different device categories.

• Adding Application Connectors for ADC Devices
• Adding Application Connectors for Servers
• Adding Application Connectors for Cloud Devices
• Adding Application Connectors for Firewalls
• Adding Application Connectors for MDMs
• Adding Application Connectors for Cloud Connectors
• Adding Application Connectors for WAFs

Adding Application Connectors for ADC Devices

AppViewX supports creating an application connector for the following ADC device vendors:

• A10

• Array

• AVI

• Citrix

• F5

• HAProxy

• NginxPlus

• Radware

1. Enter the **General Information** for the ADC devices.

Field descriptions for the Certificate Details

Field	Description
***Category**	From the dropdown list, select **ADC**.
***Vendor**	From the dropdown list, select the ADC device vendor (for the device to which this certificate will be pushed).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **SSL Templates/Server selection/Virtual server selection/SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Note: The name of this section is populated based on the **Vendor** selected.

2. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Activate Certificate	To activate the certificate after it has been pushed, select this checkbox.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stod.
***Key Location**	The private key associated with a certificate is stored in a key file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

	In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Certificate key pair name**	Enter the key-pair name used to identify the certificate and its associated private key.
Enable SNI Push for Certificate	To enable SNI push in the virtual server, select this checkbox.
Enable SNI in Virtual Server	To enable SNI in the virtual server, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.
Service Restart	To restart the device service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here. **IMPORTANT**: R
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

5. Click **Save**.

   The connector is displayed on the certificate holistic view.

Adding Application Connectors for Servers

AppViewX supports creating an application connector for the following server vendors:

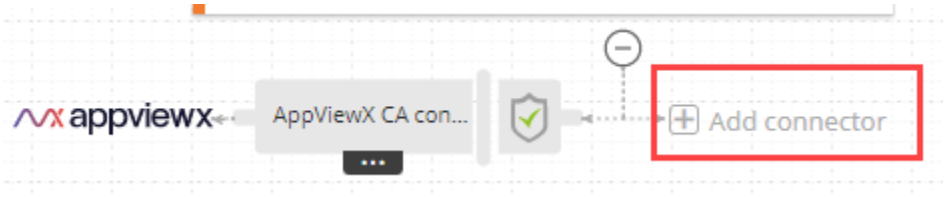
- ABAP
- ADFS Server
- Akamai CPS
- Arbor
- Apache (Linux)
- Apache (Windows)
- Cisco CallManager
- CiscoIOS
- CiscoISE
- CiscoUCS
- IBM Client (Linux)
- IBM Client (Windows)
- IBM Data Power
- IBM Domino
- IIS
- ILO
- iPlanet
- Java
- JBoss
- Linux Server
- Microsoft PC
- Microsoft Server
- MQServer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- MQClient (Windows)
- MQServer (Windows)
- MS SQL
- MySQL
- Nginx
- Rabbit MQServer
- VMWare
- Web Dispatcher
- Weblogic (Linux)
- Weblogic (Windows)
- Websphere (Linux)
- Websphere (Windows)
- Tomcat (Linux)
- Tomcat (Windows)

ABAP

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **ABAP**.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Service Restart	To restart the ABAP service immediately after the certificate is pushed, enable this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For ABAP, this field is enabled by default and is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

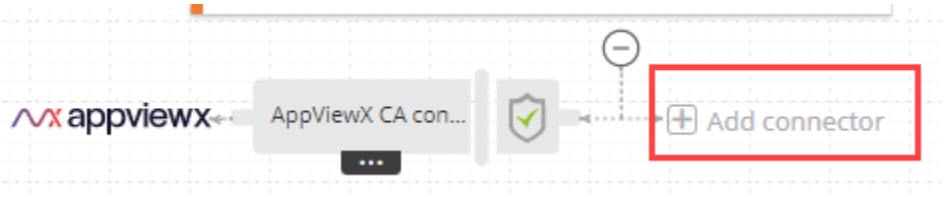
Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** ead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** ead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

ADFS Server

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **ADFS Server**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ADFS Server devices already onboarded in AppViewX.

3. Enter/Select the **Certificate Details**.

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the ADFS server, or a URL from where the ADFS server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Name**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Name** field, enter the name of the JKS keystore in which the certificate to be pushed is stored.
***KeyStore Password**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
User	Enter the details of the user that has the necessary permissions to push the certificate.
Group	Enter the details of the user group that has the necessary permissions to push the certificate.
Password Version	Enter the version of the algorithm that is used to encrypt the password for accessing the ADFS server.
Alias Name	This field is displayed when **Certificate Type** has one of the following values: • **PKCS#12 (*.pfx)** • **PKCS#12 (*.p12)***

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **PKCS#12 (_Cert)** • **CERTDB (*.db)** Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate File Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the intermediate certificate file.
***CA File Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the root certificate file.

Based on the information populated here, the **Server selection** section is populated with the list of available ADFS Server devices already onboarded in AppViewX.

4. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
5. Enter/Select the **Push Details**.

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. The script that automates the push operation is called a push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script Parameters	Enter the values that will be passed to the pre-push script.
***Push Script File Name**	Enter the name of the push script.
Push Script Parameters	Enter the values that will be passed to the push script.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post Push Script Parameters	Enter the values that will be passed to the post-push script.
Post Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Rollback Location	To recover from a conflict or failure during a push operation, copies of the certificate and configuration file are stored in a directory or storage location. In the **Rollback Location** field, enter the path to this location.
Rollback Parameters	Enter the rollback parameters (settings) used to initiate the rollback process.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Akamai CPS

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Akamai CPS**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Akamai CPS server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed. For Akamai CPS, by default, the **PEM (*.pem)** certificate is selected and the dropdown list is non-editable.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

	For Akamai CPS, this feature is enabled by default and the field is non-editable.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Akamai CPS, this feature is enabled by default and the field is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** ead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Arbor

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Arbor**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Arbor server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate File Name**	Enter the file name of the certificate (with the extension) to be pushed.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored.

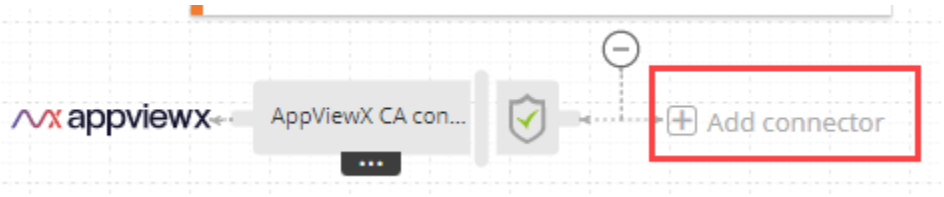
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Apache (Linux)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Apache**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Apache (Linux) server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
Intermediate Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the path to the location on your local system where the intermediate certificate file is stored.
Root Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the path to the location on your local system where the root certificate file is stored.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Apache (Windows)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows Apache**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stod.
***Key Location**	The private key associated with a certificate is stored in a key file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	Enter the path to the location on your local system where the intermediate certificate file is stored.
Root Location	Enter the path to the location on your local system where the root certificate file is stored.
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored.

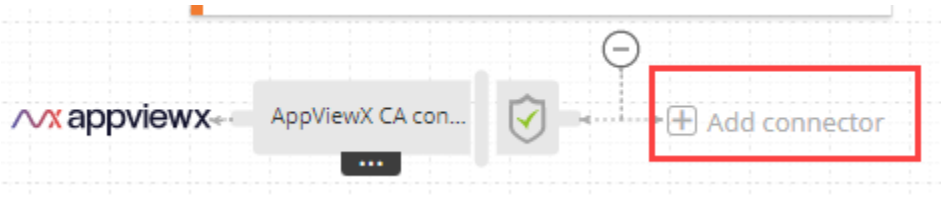
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Cisco CallManager

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Cisco CallManager**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Cisco Call Manager devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Restart Service(s)	To restart the Cisco CallManage service(s) immediately after the certificate is pushed, enable this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

CiscoIOS

1. On the certificate holistic view, click **Add Connector**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **CiscoIOS**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Profile Selection** section is populated with the list of available Cisco IOS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Profile Selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Trustpoint Name**	For Cisco IOS devices, a trustpoint configuration is an element that includes details related to a certificate such as the certificate file, the private key file, the CA certificate, and other settings related to the certificate. In the **Trustpoint Name** field, enter the name of the trustpoint configured on the Cisco IOS device(s) to which the certificate will be pushed.
Push Root Certificates	To push the root certificate, along with the end certificate, select this checkbox. **Note:** For Cisco IOS devices, the intermediate certificates are automatically included in the certificate chain.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.

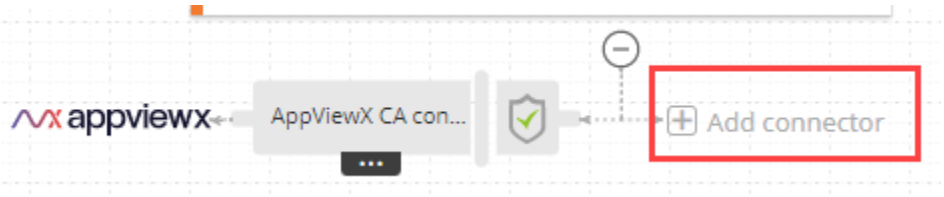
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

CiscoISE

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **CiscoISE**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **Server selection** section is populated with the list of available Cisco ISE devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing server configuration XML file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
Friendly Name	Enter the certificate friendly name assigned in the CSR generated for requesting/enrolling the certificate
Used By	From the dropdown list, select the purpose for which the certificate will be used.
Push Root and Intermediate Certificates	To push the root certificate, along with the end certificate, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

CiscoUCS

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **CiscoUCS**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Cisco UCS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Key ring**	A key ring configuration stores the keys and certificates used for encryption and authentication. Enter the name of the key ring configuration on the Cisco UCS server.
Trust point	A trustpoint configuration is used to manage certificates on a Cisco UCS server. In the **Trust point** field, enter the name of the trustpoint configured on the Cisco UCS server(s) to which the certificate will be pushed.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

IBM Client (Linux)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **IBMClient**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **SSL templates** section is populated with the list of available IBM Client (Linux) devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the IBM Client server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

IBM Client (Windows)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows IBMClient**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows IBM Client devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the Windows IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Windows IBM Client server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

IBM Data Power

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **IBMDataPower**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available IBM data Power devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Push Location	From the dropdown list, select the file type of the certificate to be pushed.
Certificate Location	Enter the path to the location on your local system where the certificate file to be pushed is stod.
Key Location	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.
Root Location	Enter the path to the location on your local system where the root certificate file (for the end certificate being pushed) is stored.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

IBM Domino

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **IBMDomino**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **SSL templates** section is populated with the list of available IBM Domino devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Push Location	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server from where the server can retrieve the certificate.
KYR Password	Enter the password to the key ring file (KYR file), which stores the keys and certificates used for encryption and authentication.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

IIS

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **IIS**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available IIS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select where the certificate to be pushed is located: • **Certificate Store**: A repository that stores certificates and their associated keys • **Centralized file system**: A file server that stores certificate files
Certificate Store	This option is displayed only when **Location Type** = **Certificate Store**. Within the certificate store, select the location where the certificates are stored from the following options: • **Personal store**: A location where user-specific certificates, such as those used for encryption and authentication, are stored • **Web hosting store**: A location where certificates used for web server configurations are stored
***Friendly name**	Enter the certificate friendly name assigned in the CSR generated for requesting/ enrolling the certificate
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Bind type**	To manage the SSL/TLS certificates for websites, select a bind type from the following options: • **Update Certificate Only**: Update the SSL/TLS certificate used by an existing site binding on the web server. It replaces the current certificate with a new one without modifying any other settings associated with the site binding (such as the hostname or port). • Update Site Binding: Update the SSL/TLS settings for an existing site binding on the web server. It allows you to update not only the certificate but also other settings associated with the site binding, such as the hostname, port, and SSL/TLS protocol settings. • **Create New Site Binding**: Create a new site binding on the web server for the specified hostname, port, and IP address (if applicable) and associates it with the specified SSL/TLS certificate. This is typically used when you want to add a new website or domain to the web server and configure SSL/TLS settings for it.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

ILO

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **ILO**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ILO devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

iPlanet

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **iPlanet**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **Server selection** section is populated with the list of available iPlanet devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***Database Path**	This field is displayed only when **Customize Push Location** is selected. Enter the path to the location on your local system where the certificate and key database files are stored.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

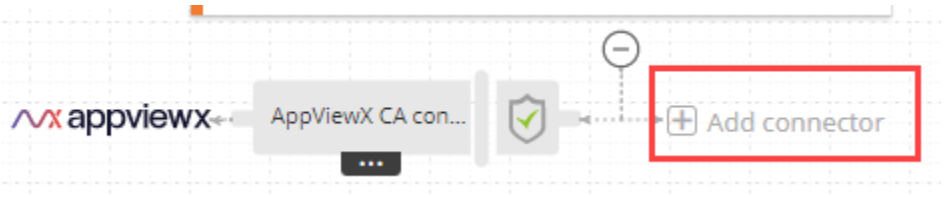
Field	Description
	Important: Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Java

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Java**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Java devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Name**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Name** field, enter the name of the JKS keystore in which the certificate to be pushed is stored.
***KeyStore Password**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
User	Enter the details of the user that has the necessary permissions to push the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Group	Enter the details of the user group that has the necessary permissions to push the certificate.
Password Version	Enter the version of the algorithm that is used to encrypt the password for accessing the ADFS server.
Alias Name	This field is displayed when **Certificate Type** has one of the following values: • **PKCS#12 (*.pfx)** • **PKCS#12 (*.p12)** • **PKCS#12 (_Cert)** • **CERTDB (*.db)** Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate File Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the intermediate certificate file.
***CA File Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the root certificate file.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. The script that automates the push operation is called a push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script Parameters	Enter the values that will be passed to the pre-push script.
***Push Script File Name**	Enter the name of the push script.
Push Script Parameters	Enter the values that will be passed to the push script.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post Push Script Parameters	Enter the values that will be passed to the post-push script.
Post Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Rollback Location	To recover from a conflict or failure during a push operation, copies of the certificate and configuration file are stored in a directory or storage location. In the **Rollback Location** field, enter the path to this location.
Rollback Parameters	Enter the rollback parameters (settings) used to initiate the rollback process.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

JBoss

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **JBoss**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available JBoss devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***KeyStore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Alias Name**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)** and **JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Linux Server

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **LinuxServer**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Custom Push	This field is displayed for all **PEM** and **DER** certificate types. From the following options, select the method of pushing certificates: • **Chain**: The full certificate chain, which includes the end, intermediate, and root certificates, will be pushed to the server. • **Issuer & Server**: The server's certificate and its issuer's certificates will be pushed to the server. • **Server Only**: Only the server's certificate will be pushed to the server.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Linux Server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Certificate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. Enter the path to the location on your local system where the certificate file to be pushed is stod.
Key Location	This field is displayed for all PEM, DER and PKCS#7 certificates. The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. This field is not displayed when **Custom Push** = **Server only**. Enter the path to the location on your local system where the intermediate certificate file is stored.
***KeyStore Location**	This field is displayed for the PKCS#12 and JKS certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed for the PKCS#12 and JKS certificates. Enter the password required to access the keystore file for the certificate to be pushed.
***Alias Name**	This field is displayed for the PKCS#12 and JKS certificates. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Truststore Location	This field is displayed for the JKS certificates. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
Truststore password	This field is displayed for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Microsoft PC

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Microsoft PC**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **Certificate Store Location** section is populated with the list of available Microsoft PC devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **Certificate Store Location**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate File Name**	Enter the file name of the certificate to be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

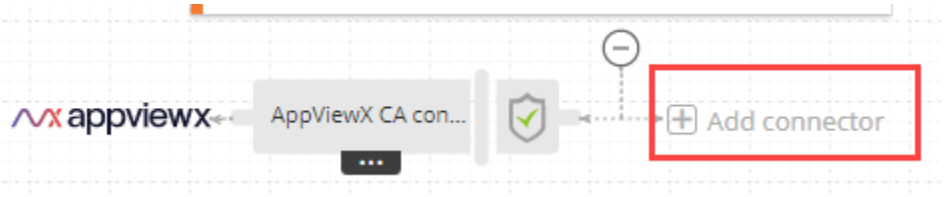
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Microsoft Server

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Microsoft Server**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Credential Type**	This field is displayed for the JKS certificates. From the dropdown list, select the source of the access credentials.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***PFX Password**	This field is displayed for the **PKCS#12** certificate types. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***Key File Name**	This field is displayed for the **PEM**, **DER**, and **PKCS#7** certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Password**	This field is displayed for JKS certificate types. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
Alias Name	This field is displayed for the PKCS#12 and CERTDB certificate types. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private key entry password	This field is displayed for the JKS certificates. Enter the password required to decrypt the private key associated with the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate Certificate Alias Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. This field is not displayed for the JKS certificate types. Enter the alias name of the intermediate certificate file.
***Root Certificate Alias Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the alias name of the root certificate file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.

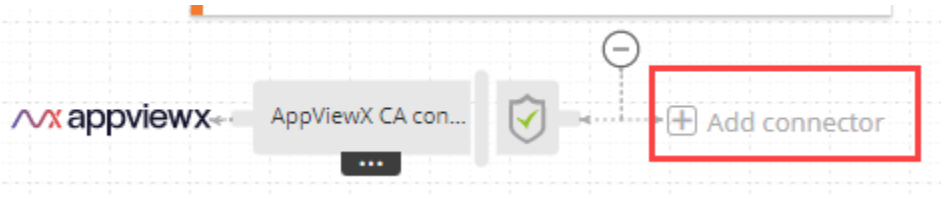
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

MQServer

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **MQServer**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. Under **SSL templates**:

   a. Based on the functionality required, select the **Profile**.

   b. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click ».
   The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	This field is displayed only for the **Create KDB** profile. Enter the name of the KDB certificate file that will be pushed to the server.
***KDB password**	This field is displayed only for the **Create KDB** profile. Enter the password required to access the KDB certificate file.
QManager Name	This field is displayed only for the **Create KDB** profile. From the dropdown list, select the name of the MQServer's queue manager.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Server Certificate Label	This field is displayed only for the **Create KDB** and **Override** profiles. This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the MQServer, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	This field is displayed for the **Create Label** profile. If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

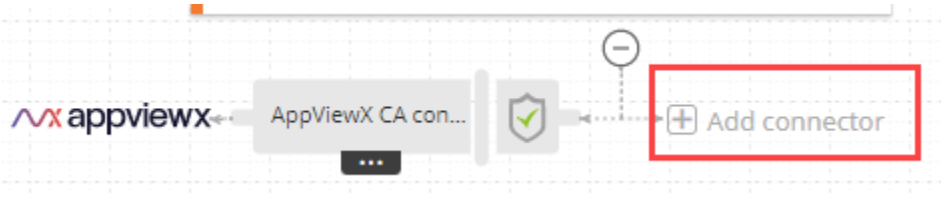
Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

MQClient (Windows)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows MQClient**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows MQClient devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

You can use the **Available Devices** dropdown list to filter devices based on functionality.

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the Windows IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Windows IBM Client server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

MQServer (Windows)

1. On the certificate holistic view, click **Add Connector**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows MQServer**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows MQServer devices already onboarded in AppViewX.

3. Under **SSL templates**:

   a. Based on the functionality required, select the **Profile**.

   b. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	This field is displayed only for the **Create KDB** profile. Enter the name of the KDB certificate file that will be pushed to the server.
***KDB password**	This field is displayed only for the **Create KDB** profile. Enter the password required to access the KDB certificate file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
QManager Name	This field is displayed only for the **Create KDB** profile. From the dropdown list, select the name of the MQServer's queue manager.
Server Certificate Label	This field is displayed only for the **Create KDB** and **Override** profiles. This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the MQServer, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	This field is displayed for the **Create Label** profile. If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

MS SQL

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **MSSQL**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **SSL templates** section is populated with the list of available MS SQL devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Registry Restart	To restart the Windows registry after the certificate is pushed, select this checkbox. **Note:** For Microsoft Registry, registry restart is mandatory.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***CA File Name**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the root certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

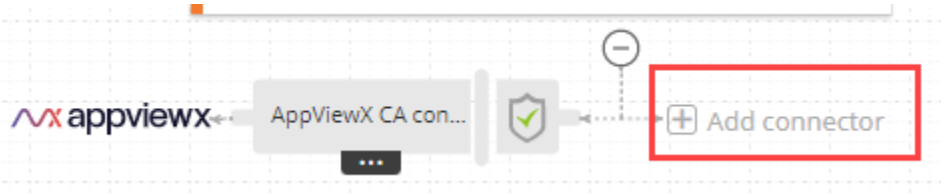
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

MySQL

1. On the certificate holistic view, click **Add Connector**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **MySQL**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available MySQL devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stod.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Intermediate Location**	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

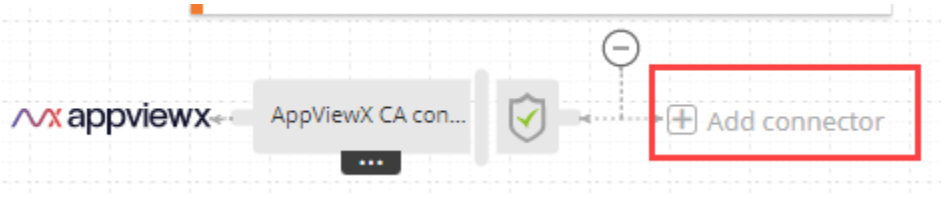
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Nginx

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Nginx**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Nginx devices already onboarded in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stod.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Rabbit MQServer

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **RabbitMQServer**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Rabbit MQServer devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stod.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Intermediate Location**	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.
Private key passphrase	Enter the password required to access the private key file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

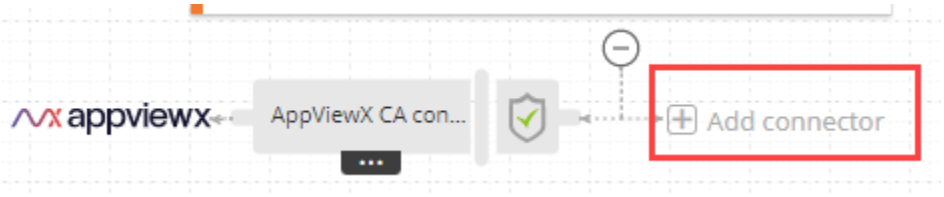
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

VMWare

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **VMWare**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available VMware devices already onboarded in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click  .

   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Web Dispatcher

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **WebDispatcher**.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Web Dispatcher devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
PSE Type	From the dropdown list, select the file type of the certificate to be pushed.
Service Restart	To restart the Web Dispatcher service immediately after the certificate is pushed, enable this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Weblogic (Linux)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Weblogic**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Weblogic devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Truststore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Key Location	This field is displayed when the **Private Key in Device** option is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the path to the location of the private key on the hardware device.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Weblogic (Windows)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows Weblogic**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Weblogic devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Truststore Location**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Websphere (Linux)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Websphere**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information entered here, the **Server selection** section is populated with the list of available Websphere devices already onboarded in AppViewX.
3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	This field is displayed only when **Customize Push Location** is selected. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed only when **Customize Push Location** is selected. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Truststore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Key Location	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Websphere (Windows)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows Websphere**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Websphere devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	Enter the password required to access the keystore file for the certificate to be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Push Root and Intermediate Certificates	This field is displayed only for JKS certificates. To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Truststore Location**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Key Location	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.

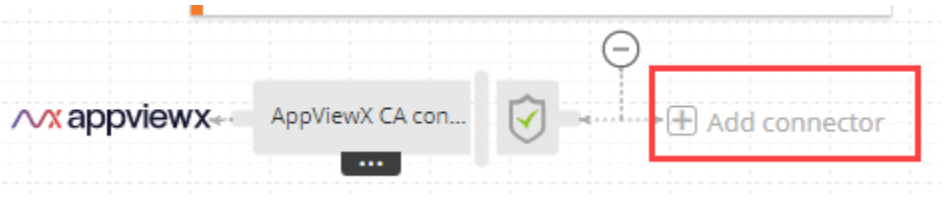
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Tomcat (Linux)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Tomcat**.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Tomcat devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate directory**	Enter the path to the location on your local system where the certificate file (to be pushed to the server) is stored.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key directory**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Key File Name**	Enter the name of the file that contains the private key associated with the certificate to be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	The file extension **.key** is automatically populated.
***KeyStore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore File Name**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)**. Enter the file name of the keystore file that contains the private keys and the associated certificates. The extension **.key** is automatically populated.
***Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Certificate Type** = **Default JKS (*.jks)** and **JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Service Restart	To restart the Tomcat service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
***CA File Name**	This field is displayed when **Push Root and Intermediate Certificates** is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the file name of the root certificate.
Intermediate File or Bundle Name	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the intermediate certificate.
***Truststore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Certificate Type** = **Default KS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the name of the truststore file for the JKS certificate to be pushed.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Tomcat (Windows)

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Windows Tomcat**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Tomcat devices already onboarded in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate directory**	Enter the path to the location on your local system where the certificate file (to be pushed to the server) is stored.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key directory**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Key File Name**	Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore File Name**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)**. Enter the file name of the keystore file that contains the private keys and the associated certificates. The extension **.key** is automatically populated.
***Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Certificate Type** = **Default JKS (*.jks)** and **JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Service Restart	To restart the Windows Tomcat service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***CA File Name**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the root certificate.
Intermediate File or Bundle Name	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the intermediate certificate.
***Truststore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Certificate Type** = **Default KS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the name of the truststore file for the JKS certificate to be pushed.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for Cloud Devices

AppViewX supports creating an application connector for the following Cloud device vendors:

- AWS
- Azure
- GCP

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Enter the **General Information** for the Cloud devices.

Field descriptions for the Certificate Details

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select the cloud vendor.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.
Service Types	From the dropdown list, select the cloud service to which the certificate will be pushed.
Target Profile	From the dropdown list, select the application gateway target profiles to which the certificate will be pushed. Currently, AppViewX supports the following target profiles: • Gateway SSL Profile (Configure TLS/SSL encryption for secure communication between gateway and clients.) • Gateway Listener Profile (Accept incoming HTTP/HTTPS requests on specific ports and paths.) • Gateway Backend Settings Profile (Route requests to specific application servers based on routing rules.)

Based on the information entered here, the **SSL templates** section is populated with the list of available cloud devices already onboarded in AppViewX.

2. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Certificate ARN	Enter the certificate's Amazon Resource Name.
Certificate Push Type	Test • **Upload a Certificate to Gateway**: • **Replace/Update existing Certificate in Gateway**:
Certificate Location (for AWS)	This field is displayed when **Vendor** = **AWS** and **Service Types** = **Cloudfront**. For CloudFront, certificates can be stored in either AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM). From the options given, select the certificate location.
Certificate Location (for Azure)	For the Azure Application Gateway, from the following options, select where the certificate will be stored after it is pushed: • **Upload directly to Application Gateway**: Upload certificates directly to the Application Gateway • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the Application Gateway configuration.
Certificate Location (for GCP Load Balancer)	For the GCP load balancer, from the following options, select where the certificate will be stored after it is pushed: • **Classic Certificates**: Upload your certificate and private key directly to the load balancer's configuration. • **Certificate Manager**: Reference certificates managed by Certificate Manager in your load balancer configuration.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
Default Certificate	In the event that a certificate cannot be pushed, a default certificate is pushed as a fall back option. To enable this, select the **Default Certificate** checkbox.
Upload Certificate as	• **New**: If you are uploading a new certificate to the GCP Certificate Manager, select this option. • **Update**: If you are updating a certificate existing in the GCP Certificate Manager, select this option.
Certificate Name	Enter the name of the certificate being pushed.
Scope of Certificate	From the following option, select the scope of the certificate being pushed: • **Global** (Certificate is available for use across all regions within a GCP project) • **Regional** (Certificate is limited to a specific region within a GCP project)
Certificate Description	Enter additional details related to the certificate being pushed.

4. Specify the **Certificate Tags**.

   To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** RRead the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** RRead the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** RRead the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for Firewalls

AppViewX supports creating an application connector for the following Firewall device vendors:

- CheckPoint
- Cisco
- Fortinet
- PaloAlto

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Firewall**.
***Vendor**	From the dropdown list, select the required firewall vendor.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information populated here, the **Profile Selection** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.
2. To select the device(s) to which the certificate will be pushed, under **Profile Selection**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Trust Point Name**	A trustpoint configuration is an element that includes details related to a certificate such as the certificate file, the private key file, the CA certificate, and other settings related to the certificate. In the **Trustpoint Name** field, enter the name of the trustpoint configured on the target system to which the certificate will be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Password	Enter the password required to access the certificate file/trust store.
Private Key Passphrase	Enter the password required to access the private key file associated with the certificate.
Push to Firewall	To push the certificate when it is updated directly to the firewall, select this checkbox.

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for MDMs

AppViewX supports creating an application connector for the following MDM vendors:

• MobileIron

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **MDM**.
***Vendor**	From the dropdown list, select the required firewall vendor.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information populated here, the **Device Groups** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.
2. To select the device(s) to which the certificate will be pushed, under **Device Groups**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Configuration name**	Enter the name of the configuration profile that includes the certificate to be pushed. A configuration profile defines the policies for managed devices.
***Certificate Category**	Enter the name of the certificate group to which the certificate to be pushed belongs.
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***PFX Password**	This field is displayed for the PKCS#12 certificates. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Adding Application Connectors for Cloud Connectors

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Internal**.
***Vendor**	From the dropdown list, select **Cloud Connector**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information populated here, the **SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.
2. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

   Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.

4. Enter/Select the **Push Details**.

   Field descriptions for the Push Details

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Adding Application Connectors for WAFs

After the WAF devices have been onboarded in AppViewX, you can push certificates to these devices.

AppViewX supports creating an application connector for the following WAF vendors:

- Barracuda
- Cloudflare
- F5
- Imperva

Barracuda

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **WAF**.
***Vendor**	From the dropdown list, select **Barracuda**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL profiles** section is populated with the list of available Barracuda server devices already onboarded in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Allow private key export	To export the private key associated with the certificate to be pushed from the WAF, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored.

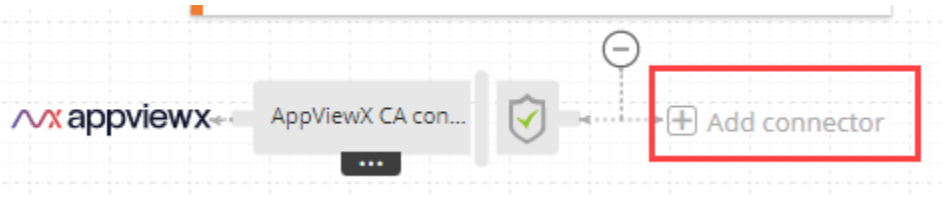
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Cloudflare

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **WAF**.
***Vendor**	From the dropdown list, select **Cloudflare**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL profiles** section is populated with the list of available Cloudflare server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click  .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Bundle Method**	Bundle method refers to a method of packaging or bundling multiple certificates and their associated private keys into a single file or bundle. • **User defined**: User manually creates a bundle file • **Compatible**: Certificates and private keys are bundled compatible with the WAF's requirements or specifications. • **Modern**: Certificates and private keys are bundled using modern or standardized formats.
***Private key restriction**	The **Private key restriction** field lets you specify the distribution restrictions for the certificate being pushed and its associated private key. From the dropdown list, select one of the following options: • **Distribute to all cloudflare data centers**: Distribute certificate and its private key to all Cloudflare data centers globally. • **Distribute only to U.S data centers**: Distribute certificate and its private key only to the Cloudflare data centers located in the United States.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Distribute only to E.U. data centers**: Distribute certificate and its private key only to the Cloudflare data centers located in the European Union. • **Distribute only to highest security data centers**: Distribute certificate and its private key only to the Cloudflare data centers that comply with the maximum number of security specifications.
***Legacy client support**	Legacy client support refers to the ability of the WAF to support older or outdated client devices or browsers. From the dropdown list, select the legacy client support supported by the WAF: • **Modern**: WAF provides support for modern SSL/TLS features and encryption standards • **Legacy**: WAF also provides support for legacy SSL/TLS features and encryption standards
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

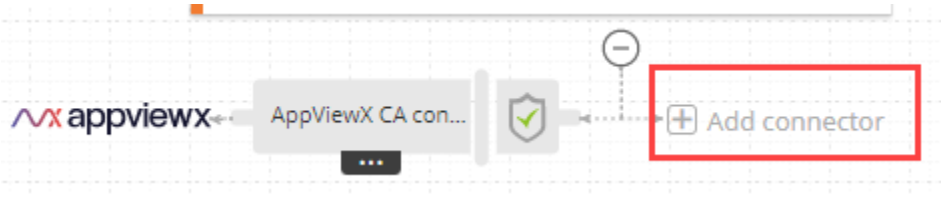
Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

F5

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **WAF**.
***Vendor**	From the dropdown list, select **F5**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL profiles** section is populated with the list of available F5 server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	The private key associated with a certificate is stored in a key file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Chain File or Bundle Name**	Enter the name given to the bundle of certificates and their associated private keys.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Imperva

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.



2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **WAF**.
***Vendor**	From the dropdown list, select **Imperva**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL profiles** section is populated with the list of available Imperva server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.

5. Enter/Select the **Push Details**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pre - and Post - Push Script Usage Steps

• Prerequisites
• Using Scripted Integrations for On-prem
• Using Scripted Integrations for SaaS
• Troubleshooting Script Usage Issues

Prerequisites

- If the scripts are written using Python:
  - Scripts for the on-prem deployment should start with

    ```
    #!/appviewx/dependencies/appviewx_addons/Python/bin/python
    ```

  - Scripts for the SaaS deployment should start with

    ```
    #!/usr/bin/python
    ```

- The script input can be consumed using the command line argument `sys.argv[1]`
- The script output should be in the JSON format, generated only using the `print` statement.
-

Script Output	Script Execution Status
`AppResponseCode:0`	Success
`AppResponseCode:-1` or any other script errors	Failure

- The script should be code-signed. Please contact AppViewX Support (help@appviewx.com) to get the script code signed.

Using Scripted Integrations for On-prem

1. Get the code-signed script from the AppViewX support team (help@appviewx.com). This will be a **.zip** file that includes the script and the signature.
2. Save the code-signed **.zip** file in all the AppViewX vendors pods running node file system.

   Default path: **<home>/appviewx/appviewx_dependencies/aps/**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Mention in the **.zip** filename in all the relevant fields in the CERT+ user interface.

> **Note:** The folder path for the file is not required. Custom folder paths are restricted.

Sample success script for the on-prem deployment:

```
#!/appviewx/dependencies/appviewx_addons/Python/bin/python

print({"status":"AppResponseCode:0"})
```

Using Scripted Integrations for SaaS

1. Get the code-signed script from the AppViewX support team (help@appviewx.com). This will be a **.zip** file that includes the script and the signature.
2. Save the **.zip** file in all machines with the AppViewX Cloud Connector at the following location: **<CC_INSTALLATION_PATH>/deps/aps/**.
3. Mention in the **.zip** filename in all the relevant fields in the CERT+ user interface.

> **Note:** The folder path for the file is not required. Custom folder paths are restricted.

Sample success script for the SaaS deployment:

```
#!/usr/bin/python

print({"status":"AppResponseCode:0"})
```

Troubleshooting Script Usage Issues

Error	Cause	Resolution
File not found	The python path mentioned in the script file is not correct.	Check the path in the vendors pod or the mid-server-platform pod.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

(continued)

Error	Cause	Resolution

		For Python scripts:
		• Scripts for the on-prem deployment should start with
		`#!/appviewx/dependencies/appviewx_addons/Python/bin/python`
		• Scripts for the SaaS deployment should start with
		`#!/usr/bin/python`

...bin/python^M: bad interpreter	The `^M` is a carriage return character. Linux uses the line feed character to mark the end of a line, whereas Windows uses the two-character sequence CR LF. Your file has Windows line endings, which is confusing Linux	Remove the spurious CR characters and then code sign the script. You can remove these characters using the command: `sed -i -e 's/\r$//' scriptname.py`

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.

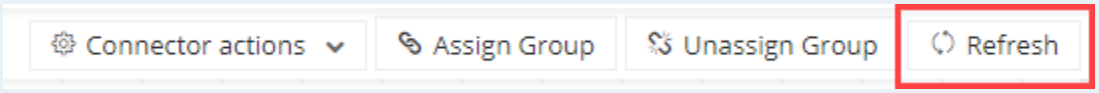
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Note: To refresh the certifcate topology view, from the top-right corner of the screen, click **Refresh**.



• Colour Codes Status

Colour Codes Status

The topological view follows a colour codes scheme to identify certificate status.

Full list of color codes and their descriptions

Colour	Description
Green	The certificate is available and valid.
Red	.The certificate has expired
Gray	Certificate push action failed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Full list of color codes and their descriptions (continued)

Colour	Description
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

Pushing a Client Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

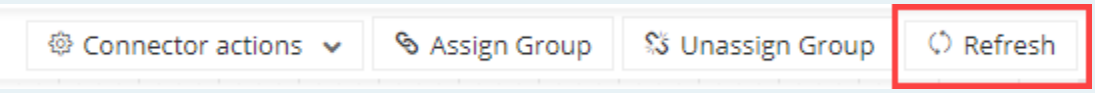
   The work order status displayed beside the connector updates to **Push-Review In Progress**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Note: To refresh the certifcate topology view, from the top-right corner of the screen, click **Refresh**.



• Colour Codes Status

Colour Codes Status

The topological view follows a colour codes scheme to identify certificate status.

Full list of color codes and their descriptions

Colour	Description
Green	The certificate is available and valid.
Red	.The certificate has expired
Gray	Certificate push action failed.
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

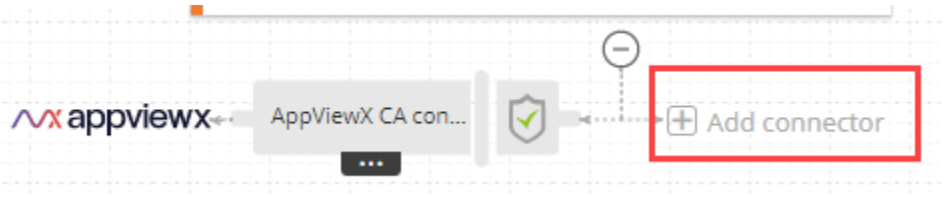
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Pushing an Intermediate Certificate to a Device

In the case of intermediate CA certificates or trust certificate renewal, the same should be pushed to the device in order to update the trust chain for the SSL communication. If this is not done, the SSL handshake will fail.

To push an intermediate certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Intermediate**.
   The **Intermediate Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. On the certificate topology page, click **Add Connector**.



4. Enter/select the **General Information** required for adding a connector.

Field descriptions for the General Information section

Field	Description
Category	Select the category from the dropdown list. The possible categories are: • ADC • Cloud • Firewall • MDM • Server • WAF.
Vendor	Select the desired vendor from the dropdown list.
Connector Name	Enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
Description	Enter the description in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

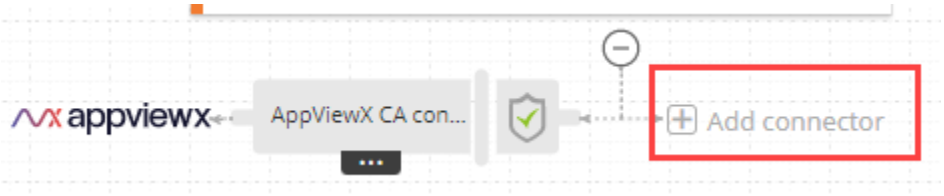
5. From the **SSL Template** section, to select a device listed under **Available devices**, click .
   The selected device is listed under the **Selected devices** list.

Pushing a Root Certificate to a Device

There can be renewal or change of root certificate in the trust store. In such occurrences, the user can push the root certificate to the desired endpoints to avoid the SSL handshake failure.

To push a root certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Root**.
   The **Root Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. On the certificate topology page, click **Add Connector**.



4. Enter/select the **General Information** required for adding a connector.

Field descriptions for the General Information section

Field	Description
Category	Select the category from the dropdown list. The possible categories are: • ADC • Cloud • Firewall • MDM • Server • WAF.
Vendor	Select the desired vendor from the dropdown list.
Connector Name	Enter a name for the connector that is descriptive enough when viewed within the Certificate topology.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Enter the description in this field.

5. From the **SSL Template** section, to select a device listed under **Available devices**, click .
   The selected device is listed under the **Selected devices** list.

Reissuing Certificates

To update or modify its parameters, a certificate can be reissued by the same certificate authority that issued it. A common use case will be the addition of SAN names.

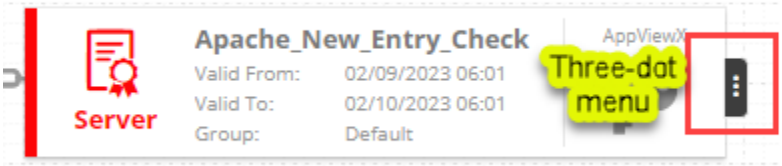
Note: Reissuing certificates will not be considered as a new order to the CA.

Note: You can reissue the certificates via the Certificate Inventory section also.

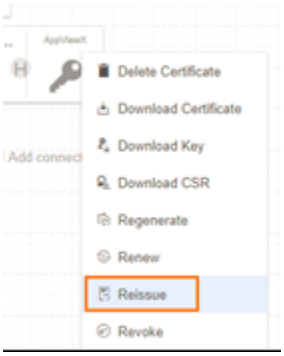
- Reissuing a Server Certificate
- Reissuing a Client Certificate

Reissuing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Reissue Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To reissue a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Renew**.



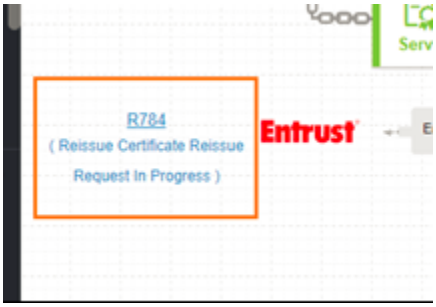
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Server Certificate** > **Reissue** page is displayed.

On the **Server Certificate** > **Reissue** page, if required, you can edit the **Subject Alternate Names**. The **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can also be modified.

4. Click **Reissue**.
5. In the **Reissue** dialog box, enter the **Reason** for removal and any additional details as **Comments.**
6. Click **Yes**.
   The reissue process is initiated, as is displayed in the certificate topology view, alongside the connector



If the **Approval Required** checkbox is enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

7. To approve the reissue request, from the certificate topology view, click **Approve**.



8. In the **Approve**dialog box, enter your **Comments**.
9. Click **Yes**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.



12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is reissued, the the status updates to **Completed**.

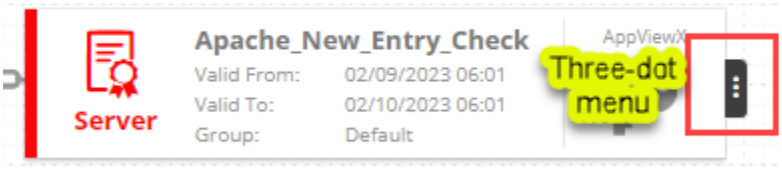


Reissuing a Client Certificate

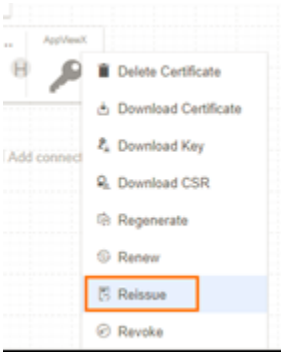
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Reissue Certificate** > **Client**.

   The **Client Certificate** page is displayed.
2. To reissue a certificate,under **Common Name**, select the required certificate name.

   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Renew**.



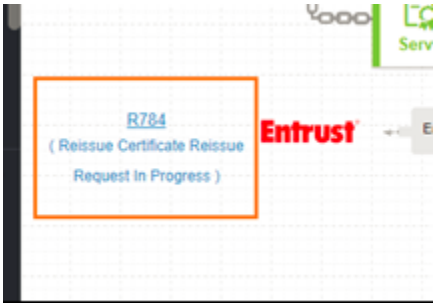
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Client Certificate** > **Reissue** page is displayed.

On the **Client Certificate** > **Reissue** page, if required, you can edit the **Subject Alternate Names**. The **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can also be modified.

4. Click **Reissue**.
5. In the **Reissue** dialog box, enter the **Reason** for removal and any additional details as **Comments.**
6. Click **Yes**.
   The reissue process is initiated, as is displayed in the certificate topology view, alongside the connector



If the **Approval Required** checkbox is enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

7. To approve the reissue request, from the certificate topology view, click **Approve**.



8. In the **Approve**dialog box, enter your **Comments**.
9. Click **Yes**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.



12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is reissued, the the status updates to **Completed**.



Revoking Certificates

Revocation is the process of making a certificate invalid. For example, you might need to revoke a certificate if the certificate is no longer required (or) certificate's private key is compromised. Make sure that you have permission to revoke a certificate and submit a request to the certificate authority. As soon as the certificate is revoked, it is not considered to be a trusted certificate. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.

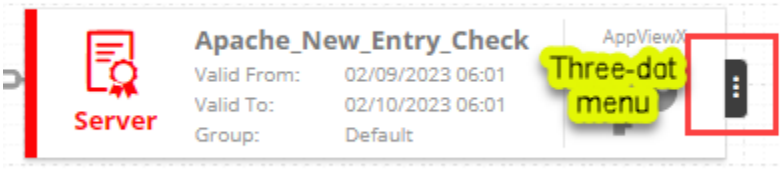
- Revoking a Server Certificate
- Revoking a Client Certificate
- Revoking a Device Certificate
- Revoking a Code Signing Certificate

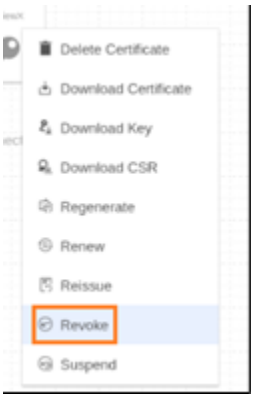
Revoking a Server Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Revoke**.





   The **Certificate Revoke** dialog box is displayed.
4. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
5. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.



   If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
6. On the certificate topology view, click **Approve** to proceed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

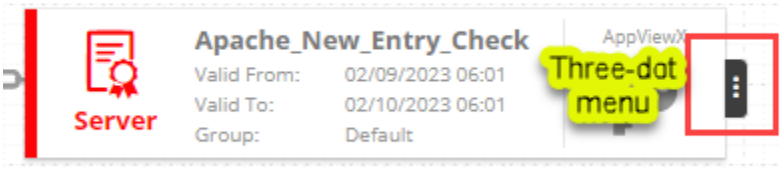


7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    After the certificate is revoked, the the status updates to **Completed**.

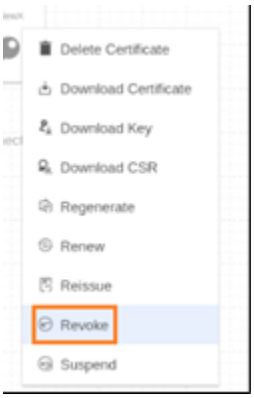
Revoking a Client Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Client**.
   The **Client Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Revoke**.

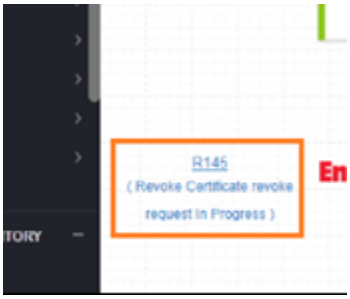


Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Certificate Revoke** dialog box is displayed.

4. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
5. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.



If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
10. Click **Implement**.
11. Click the **Implement** button to proceed.
12. In the **Implement** dialog box, enter your **Comments.**

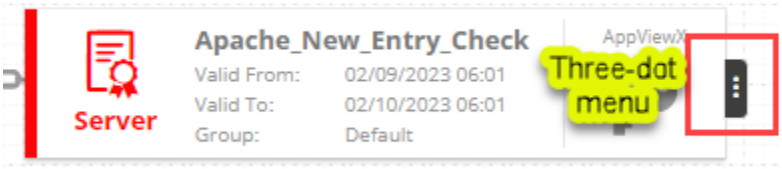
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

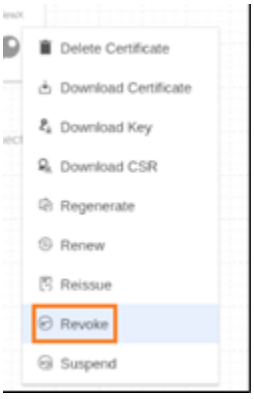
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    After the certificate is revoked, the the status updates to **Completed**.

Revoking a Device Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Device**.
   The **Server Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Revoke**.

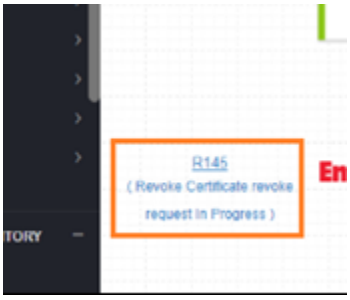




   The **Certificate Revoke** dialog box is displayed.
4. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
5. Enter your comments in the **Comments** text field (optional) and click **Yes**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The revoke process is initiated for the selected certificate.



If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
10. Click **Implement**.
11. Click the **Implement** button to proceed.
12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is revoked, the the status updates to **Completed**.

Revoking a Code Signing Certificate

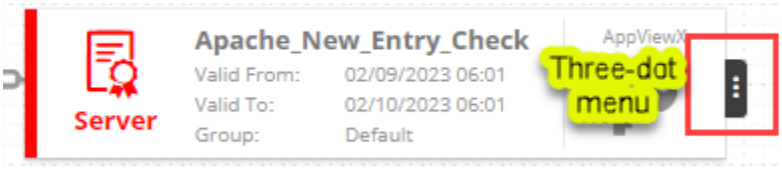
Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

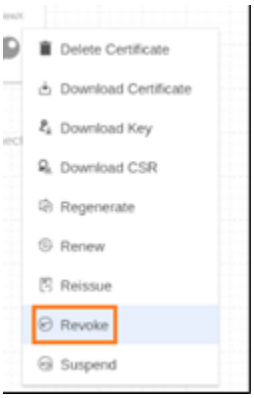
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Code Signing Certificate**.

   The **Code Signing Certificate** page is displayed.

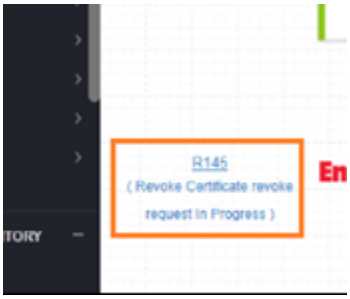
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Revoke**.





   The **Certificate Revoke** dialog box is displayed.
4. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
5. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.



   If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
6. On the certificate topology view, click **Approve** to proceed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
10. Click **Implement**.
11. Click the **Implement** button to proceed.
12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is revoked, the the status updates to **Completed**.

Regenerating Certificates

Certificate regeneration allows you to create a new certificate with the same parameters as an existing certificate. Certfiicate regeneration will be a new order to the Certificate authority. This will come in handy if the user wants to switch the CA for a certificate.

- Regenerating a Server Certificate
- Regenerating a Client Certificate
- Regenerating a Code Signing Certificate

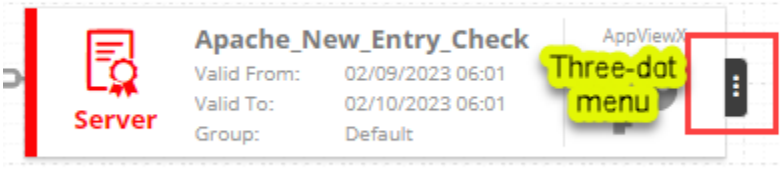
Regenerating a Server Certificate

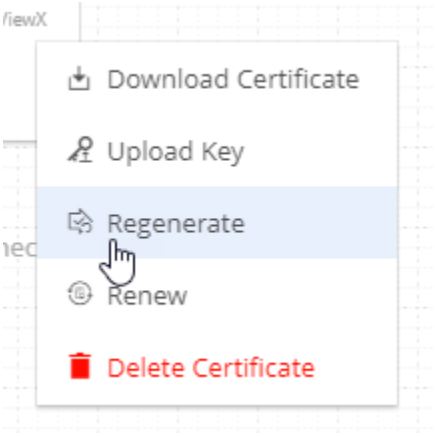
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.

   The **Server Certificate** page is displayed.
2. To regenerate a certificate,under **Common Name**, select the required certificate name.

   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





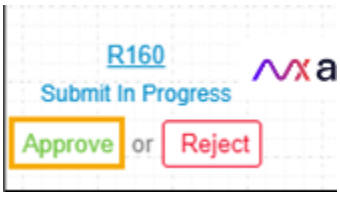
The **Server Certificate > Regenerate** page is displayed.

4. On the **Server Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

> **Note:** For instructions on entering inputs in the above sections, click here.

5. Click **Regenerate**.

   The regenerate process is initiated.
6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. Select the **Implementation Time** from the calendar field.
b. Enter the comments in the field.
c. Click **Yes**.

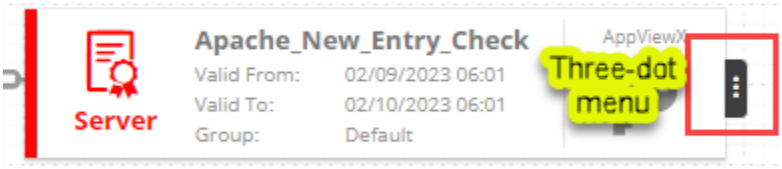
The approval process is initiated.

10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    a. Select the **Implementation Time** from the calendar field.
    b. Enter the comments in the field.
    c. Click **Yes**.

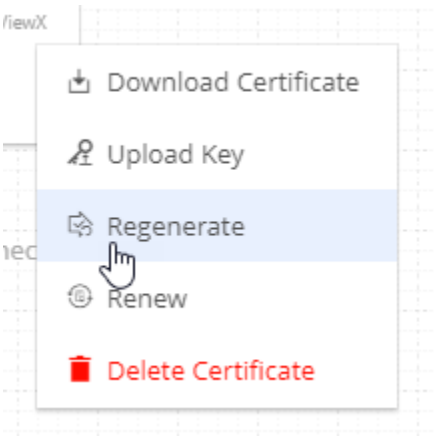
    After the certificate regeneration is complete, the the status updates to **Completed**.

Regenerating a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. To regenerate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Regenerate**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The **Client Certificate > Regenerate** page is displayed.

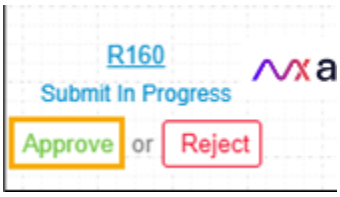
4. On the **Client Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

> **Note:** For instructions on entering inputs in the above sections, click here.

5. Click **Regenerate**.

   The regenerate process is initiated.

6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
   a. Select the **Implementation Time** from the calendar field.
   b. Enter the comments in the field.
   c. Click **Yes**.

   The approval process is initiated.

10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.

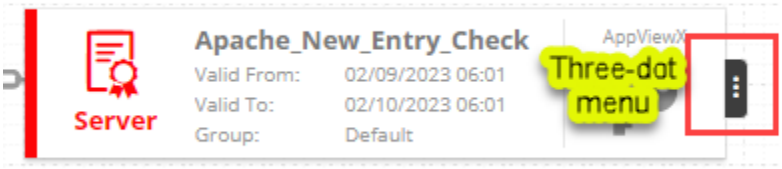
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

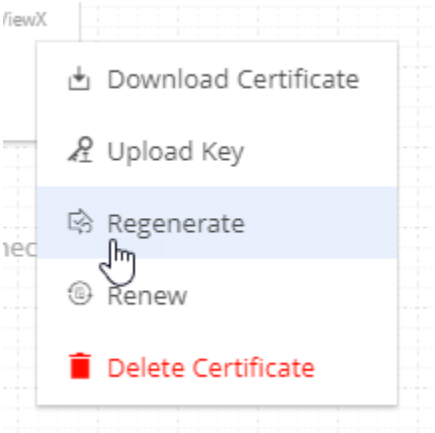
a. Select the **Implementation Time** from the calendar field.
b. Enter the comments in the field.
c. Click **Yes**.

After the certificate regeneration is complete, the the status updates to **Completed**.

Regenerating a Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. To regenerate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Regenerate**.





The **Code Signing Certificate > Regenerate** page is displayed.

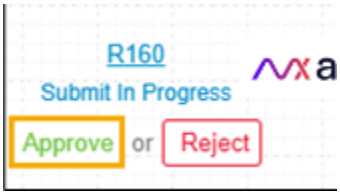
4. On the **Code Signing Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

> **Note:** For instructions on entering inputs in the above sections, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click **Regenerate**.

   The regenerate process is initiated.
6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve**dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
   a. Select the **Implementation Time** from the calendar field.
   b. Enter the comments in the field.
   c. Click **Yes**.

   The approval process is initiated.
10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    a. Select the **Implementation Time** from the calendar field.
    b. Enter the comments in the field.
    c. Click **Yes**.

    After the certificate regeneration is complete, the the status updates to **Completed**.

Reinstating Certificates

Reinstate is an action that can be applied only on the suspended certificate. Suspend is a temporary revocation of a certificate where the user is unsure about certificate usage. Once reinstated, the certificate will get resumed to serve its purpose normally. The suspend and reinstate are the actions supported only by a few CAs such as Microsoft, Entrust, and so on.

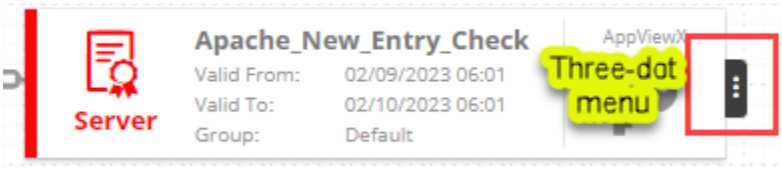
Note: Only the certificates issued by the Microsoft and EJBCA certificate authorities can be reissued.

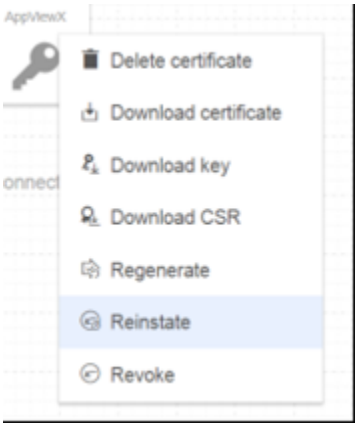
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Reinstating a Server Certificate
• Reinstating Client Certificate
• Reinstating Code Signing Certificate

Reinstating a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Reinstate**.



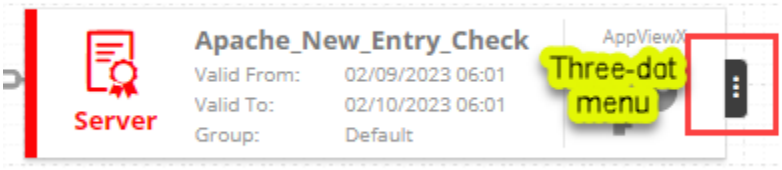


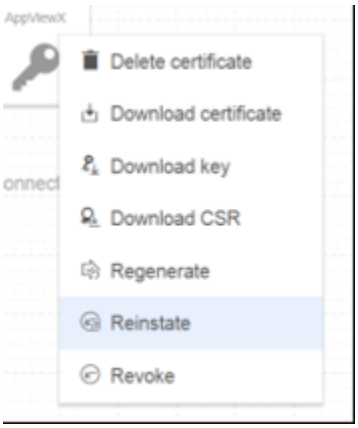
   The **Certificate Reinstate** dialog box is displayed.
4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certfiicate.
5. Enter you **Comments** in the text field and click **Yes**.

Reinstating Client Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Reinstate**.



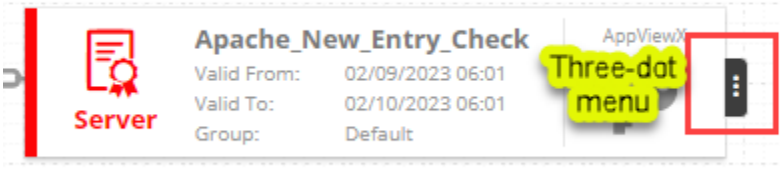


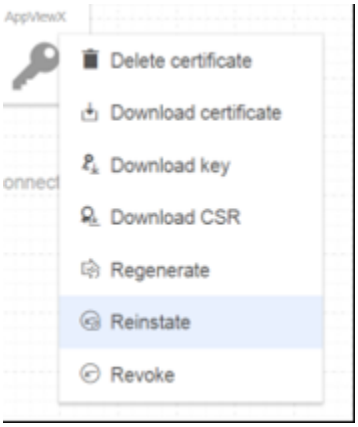
   The **Certificate Reinstate** dialog box is displayed.
4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certfiicate.
5. Enter you **Comments** in the text field and click **Yes**.

Reinstating Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the three-dot menu for the certificate, click **Reinstate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





The **Certificate Reinstate** dialog box is displayed.

4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certfiicate.
5. Enter you **Comments** in the text field and click **Yes**.

Running Revocation Check-OCSP

A sophisticated method of detecting revoked certificates is the Online Certificate Status Protocol (OCSP). Instead of downloading and parsing the entire CRL, the client can send the certificate in question to the CA. And then, the CA replies status of the certificate is good, revoked, or unknown. This method involves far less overhead than CRL and is also more reliable.

- Running Revocation Check for Server Certificate
- Running Revocation Check for Client Certificate
- Running Revocation Check for Device Certificate
- Running Revocation Check for Code Signing Certificate

Running Revocation Check for Server Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Server**.
   The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Running Revocation Check for Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Client**.
   The **Client Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Running Revocation Check for Device Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Device**.
   The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Running Revocation Check for Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Generating Certificate Signing Request (CSR)

CERT+ can be used as a CSR generation tool where you can choose either the keys that can be generated in the filesystem or any HSM device integrated with AppViewX. CSR, or Certificate Signing Request, consists of requester info in a standardized way. Based on an organization's needs and the business model, the CSR generation and approval flow can be customized.

• Generating Manual CSR for Server Certificate
• Generating Manual CSR for Code Signing Certificate

Generating Manual CSR for Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Generate CSR** > **Server**.
   The **Generate CSR : Server** page is displayed.
2. In the **Group details** section, from the **Assign Group** dropdown list, select the group of certificates you want to assign the CSR to.
3. Enter/Select the **CSR details**.

Field descriptions for the CSR details section

Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM
***Device Type**	Select the type of device as required: Options are: • **HSM Devices** • **ADC Devices**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Option	Description
***Device**	Select the device from the dropdown list.
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate. **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Option	Description
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

4. In the **Attachments** section, upload any attachments relevant to the CSR generation process.

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the **Upload** button to select the file.
Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Tip: You can use **the Search** option to find the attachments from the attachment list.

5. To generate the CSR and add it to the intended group, click **Add**.

Generating Manual CSR for Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Generate CSR** > **Code Signing Certificate**.
   The **Generate CSR : Code Signing** page is displayed.
2. In the **Group details** section, from the **Assign Group** dropdown list, select the group of certificates you want to assign the CSR to.
3. Enter/Select the **CSR details**.

Field descriptions for the CSR details section

Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM.
***Device Type**	Select the type of device as required: Options are: • **HSM Devices** • **ADC Devices.**
***Device**	Select the device from the dropdown list.
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Option	Description
	Note: No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Option	Description
	will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

4. In the **Attachments** section, upload any attachments relevant to the CSR generation process.

Field descriptions for the Attachments section

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

Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.

Tip: You can use **the Search** option to find the attachments from the attachment list.

5. To generate the CSR and add it to the intended group, click **Add**.

Migrating CAs (CA Switch)

The CA Switch feature in the **Inventory** module allows you to re-enroll certificates from one CA to another CA. Once triggered, the certificate migration readiness for every certificate will be shown in the **Process Explorer**, which needs to be validated before the CA switch is performed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Migrating the CA for Server Certificate
• Migrating the CA for Client Certificate

Migrating the CA for Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Server**.
   The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

> **Tip:** You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

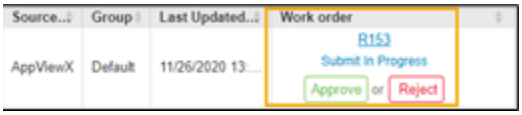
3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.
5. Click **Save**.
   The **CA Switch Summary** page is displayed.

Understanding the CA Switch Summary

Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. For the certificate you want to migrate, select the corresponding checkbox.
7. In the **Common Name** column, click the eye icon to view certificate details.
8. In the **CSR details** column, click **Update CSR** to review the details.
9. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
10. Click **Submit**.
11. Perform the required actions in the Work order column.



12. In the **Work order** column, click **Approve**.
    The **Approve**dialog box is displayed.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
14. Select the **Implementation Time** from the calendar field.
15. Enter the **Comments**.
16. Click **Yes**.
17. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
18. In the **Work order** column, click **Implement**.
    The **Implement** dialog box appears.
19. If the workflow request has to be approved automatically in the future, click **Schedule later**.
20. Select the **Implementation Time** from the calendar field.
21. Enter the **Comments** in the field.
22. Click **Yes**.
23. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
24. Click the refresh icon on the top-right of the page to update the Work Order status.
    After the CA Switch is completed, the Work order status changes to **Completed**.

Migrating the CA for Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Client**.
   The **Client Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

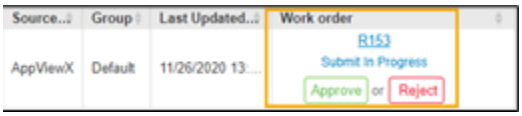
> **Tip:** You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.
5. Click **Save**.
   The **CA Switch Summary** page is displayed.

Understanding the CA Switch Summary

Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

6. For the certificate you want to migrate, select the corresponding checkbox.
7. In the **Common Name** column, click the eye icon to view certificate details.
8. In the **CSR details** column, click **Update CSR** to review the details.
9. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
10. Click **Submit**.
11. Perform the required actions in the Work order column.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

12. In the **Work order** column, click **Approve**.
    The **Approve**dialog box is displayed.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
14. Select the **Implementation Time** from the calendar field.
15. Enter the **Comments**.
16. Click **Yes**.
17. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
18. In the **Work order** column, click **Implement**.
    The **Implement** dialog box appears.
19. If the workflow request has to be approved automatically in the future, click **Schedule later**.
20. Select the **Implementation Time** from the calendar field.
21. Enter the **Comments** in the field.
22. Click **Yes**.
23. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
24. Click the refresh icon on the top-right of the page to update the Work Order status.
    After the CA Switch is completed, the Work order status changes to **Completed**.

Running the SSL Checker for a Certificate

SSL certificate deployment can be validated using the SSL checker feature in AppViewX. This validates the SSL certificate deployment, trustchain, ciphersuites, and supported TLS versions for a given service endpoint.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **SSL Checker**.
   The **SSL Checker** page is displayed.
2. Enter the **FQDN** and **IP address** details.
3. Click **Add**.
4. To run the SSL checker, click **Validate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Managing the Certificate Inventory

The certificate inventory allows you to take inventory of, and proactively manage all your certificates. This will be a single source of truth for all the certificates in the organization. Every certificate action can be performed from the inventory.

- Take inventory of all your digital certificates
- Keeps you informed of impending expirations
- Creates certificate tasks via workflows to renew expiring certificates
- Creates incidents for already expired certificates
- Prioritizes certificate importance
- Helps you proactively manage your certificates
- Helps you avoid manually tracking a large volume of certificates
- Prevents security breaches due to expired or expiring certificates

In the Certificate Inventory section, you can:

- enroll a certificate
- renew a certificate
- push to device
- reissue a certificate
- revoke a certificate
- regenerate a certificate
- reinstate a certificate
- revocation check
- upload a certificate
- download a certificate.

- Managing the Server Certificate Inventory
- Managing the Client Certificate Inventory
- Managing the Code Signing Certificate Inventory
- Managing the Device Certificate Inventory
- Managing the Intermediate Certificate Inventory
- Managing the Root Certificate Inventory
- Uploading a Certificate
- Downloading Certificates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Managing the Server Certificate Inventory

Server certificate inventory is where all the server certificates with the EKU (Extended/enhanced Key Usage) Server and Client authentication will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificate renewal, bulk certificates CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

On the **Certificate Inventory** > **Server Certificate** page, all the server certificates are listed. You can perform the following actions:

- Export Certificates - To export the server certificate.
- Delete - To delete the server certificate.
- Change Status - To change the server certificate status.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To Unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.
- Certificate Attributes - To update the certificate attributes.

- Exporting a Server Certificate
- Deleting Server Certificates
- Changing Server Certificate Status
- Assigning Certificate Group for Server Certificates
- Unassigning Certificate Group from Server Certificates
- Bulk Revoking Server Certificates
- Adding/Modifying Comments for Server Certificates
- Updating Certificate Attributes for Server Certificates
- Bulk Updating Certificate Attributes

Exporting a Server Certificate

You can export certificate(s) from the Server Certificate inventory in the form of columns and values. These certificates can be exported either in an **.xls** or **.csv** format. This can be used for reporting or making another inventory.

To export a server certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** pop-up window is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Deleting Server Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

- Deleting Individual Server Certificates from the Inventory
- Deleting Individual Certificates from the Holistic View
- Deleting all Server Certificates

Deleting Individual Server Certificates from the Inventory

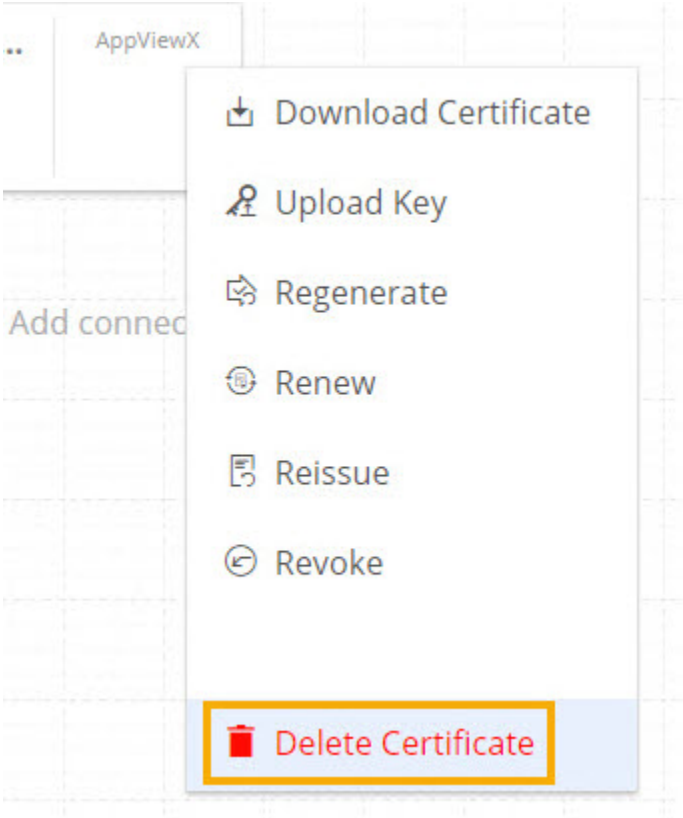
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Server Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Deleting Individual Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Server Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.

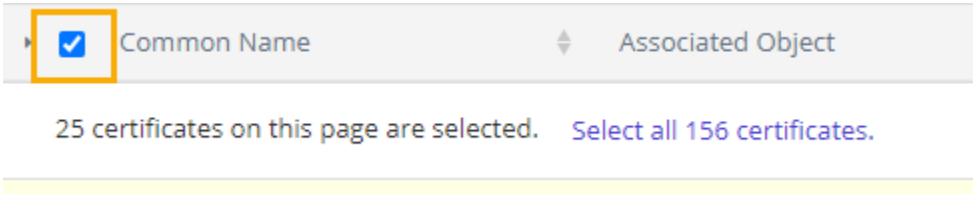


4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The server certificate is deleted from the AppViewX inventory.

Deleting all Server Certificates

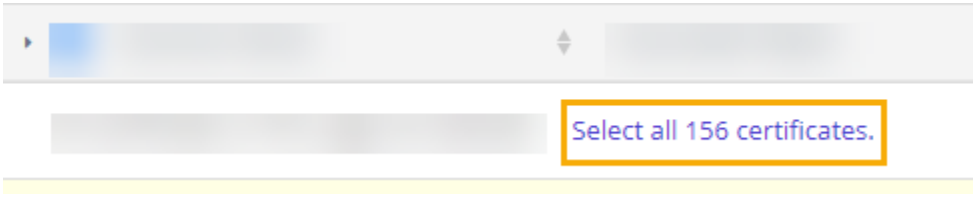
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. In the **Server Certificate** inventory, select the checkbox next to the **Common Name** field label.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

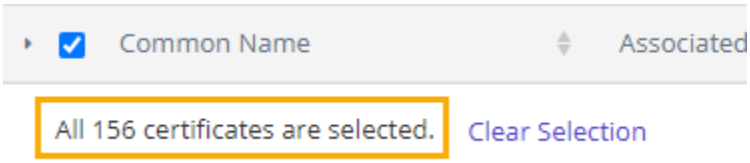


All certificates on the current page are selected.

3. To select all certificates in the server certificate inventory, click **Select all <no. of certificates> certificates**.



This will select all certificates across all pages in the server certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certficate** confirmation dialog box, cliek **Yes**.
   All certificates in the server certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificiates will be deselected.

Changing Server Certificate Status

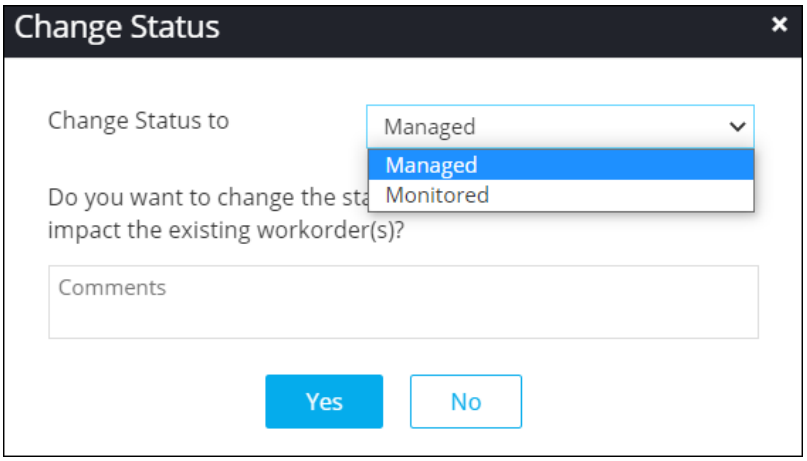
The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

can only view the certificate details in reports and in the inventory. When the certificates are set as Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the server certificate status:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate for which you want to change the status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** pop-up window that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.



5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group for Server Certificates

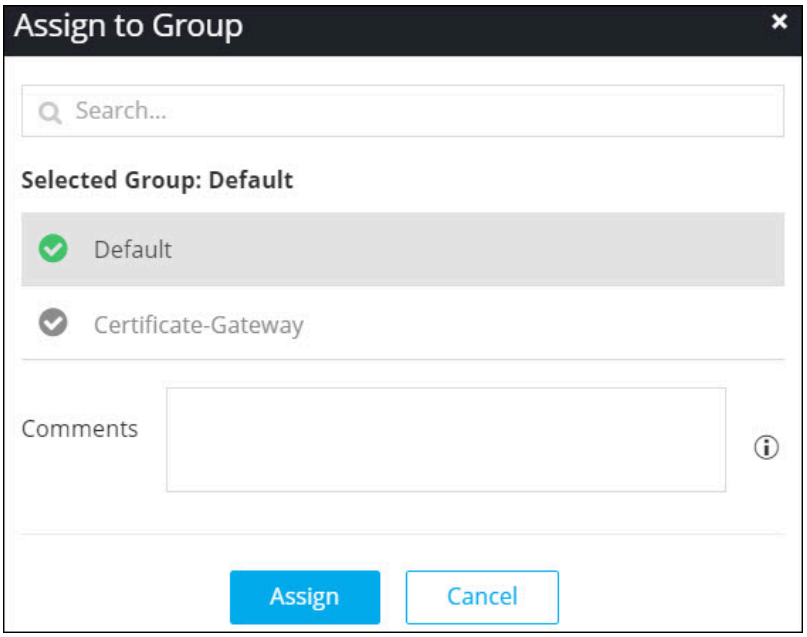
The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a server certificate to a group:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate that you want to assign to a group to.
3. From the **Actions** dropdown, click **Assign Group**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.



5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Server Certificates

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.
4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Bulk Revoking Server Certificates

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

To bulk revoke server certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the checkbox for the required certificate.
3. Click **Actions**, and then select **Revoke Certificate** from the list.
   The certificate revoke dialog box is displayed.

   The following table describes the options available on the revoke certificate page:

   Field descriptions for certificate revoke

Field	Description
***Reason**	The required option from the dropdown list. The possible options are, • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Enter any additional comments, if required.
**: Mandatory fields*	

4. Click **Yes**.

Adding/Modifying Comments for Server Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate that you want to revoke.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** dialog box that is displayed, enter a comment and click **Save**.

Updating Certificate Attributes for Server Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Downloading Failed Updates
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

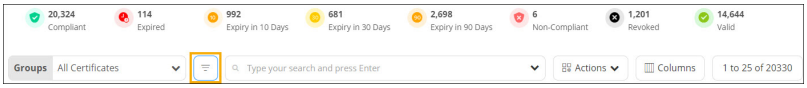
Managing the Client Certificate Inventory

Client certificate inventory displays all the client certificates with the EKU (Extended/enhanced key usage) client authentication, email protection. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform action such as bulk certificates renewal/revocation check/CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

The **Client Certificate** page is available under **Certificate Inventory** in the left menu.

The following table describes the options available on the client certificate inventory page:

Options available on the Client Certificate page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates.
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates. • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options available on the Client Certificate page (continued)

Options	Description
	• Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check
Columns	Allows you to select the columns to be displayed on the Client Certificate inventory page.
Toggle	Allows you to toggle between the following display options for the Server Certificate inventory: • **Reports**: Displays reports related to server certificates. For more information, click here. • **List**: Displays the list of server certificates.

• Exporting a Client Certificate
• Deleting Client Certificates
• Changing Client Certificate Status
• Assigning Certificate Group to Client Certificates
• Unassigning Certificate Group from Client Certificates
• Bulk Revoking Client Certificates
• Adding/Modifying Comments for Client Certificates
• Updating Certificate Attributes for Client Certificates
• Bulk Updating Certificate Attributes

Exporting a Client Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

To export a client certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Server Certificate** page is displayed.
2. On the **Client Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Deleting Client Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

- Deleting Individual Client Certificates from the Inventory
- Deleting Client Certificates from the Holistic View
- Deleting all Client Certificates

Deleting Individual Client Certificates from the Inventory

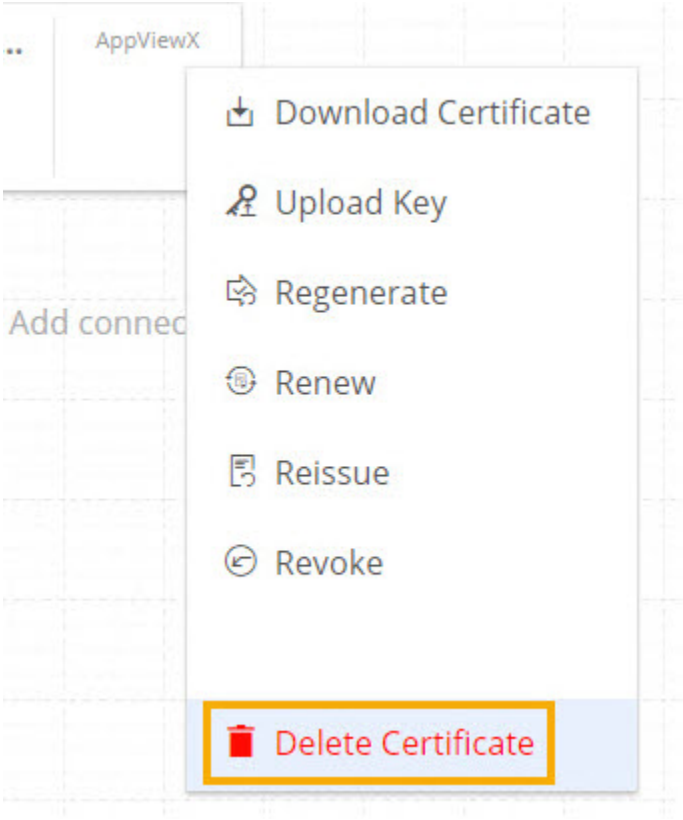
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. From the **Client Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Deleting Client Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

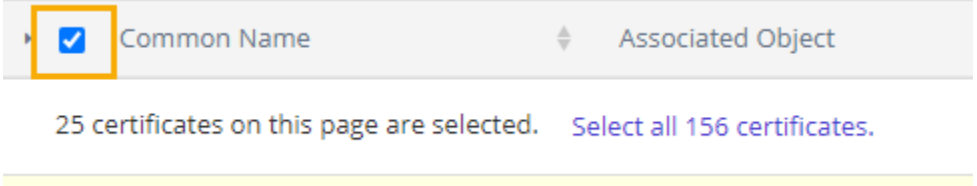
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. From the **Client Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.



4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The client certificate is deleted from the AppViewX inventory.

Deleting all Client Certificates

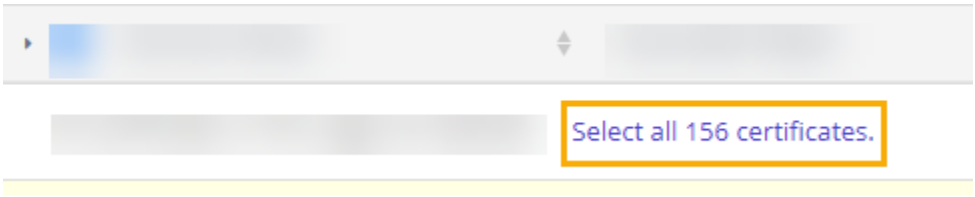
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. In the **Client Certificate** inventory, select the checkbox next to the **Common Name** field.



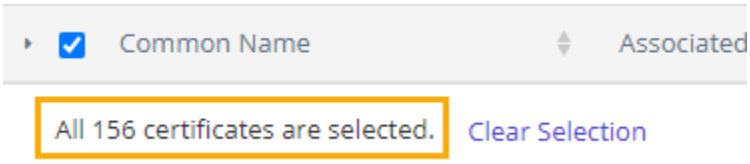
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

All certificates on the current page are selected.

3. To select all certificates in the client certificate inventory, click **Select all <no. of certificates> certificates**.



This will select all certificates across all pages in the client certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certficate** confirmation dialog box, clieck **Yes**.
   All certificates in the client certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificiates will be deselected.

Changing Client Certificate Status

The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you can only view the certificate details in reports and in the inventory. When the certificates are set as Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the client certificate status:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate for which you want to change status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** pop-up window that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.
5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group to Client Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a client certificate to a group:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Client Certificates

The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. In the **Common Name** column certificate list, select the desired certificate(s) that you want to unassign the certificate group.
3. Click the **List** toggle button on the right top corner of the client certificate page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

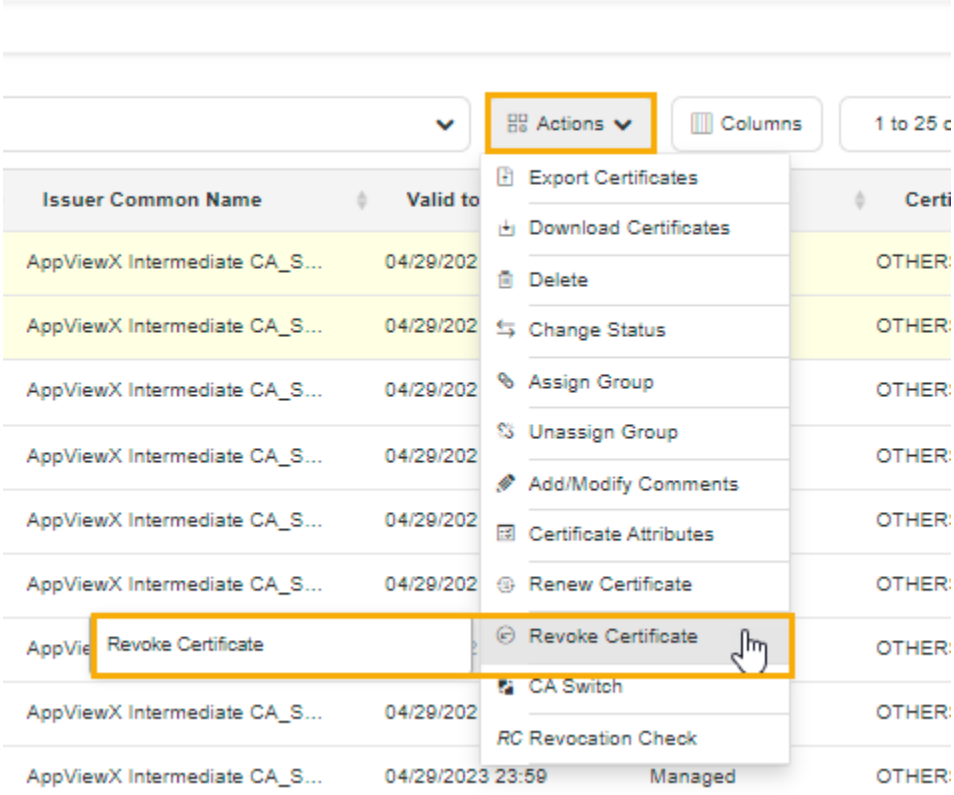
4. Click **Actions**, and then select **Unassign Group** from the drop-down list.
5. The selected certificate is assigned to the default group.
   The following message is displayed: **<certificate_name> assign to undefined**.

Bulk Revoking Client Certificates

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

To bulk revoke a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. Click the **List** toggle button on the right top corner of the server certificate page.



3. Select the required certificate check box.
4. Click **Actions**, and then select **Revoke Certificate** from the list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The certificate revoke dialog box is displayed.

The following table describes the options available on the revoke certificate page:

Field description for certificate revoke

Field	Description
***Reason**	The required option from the dropdown list. The possible options are: • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Enter additional details, if required.
**: Mandatory fields*	

5. Click **Yes**.

Adding/Modifying Comments for Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** pop-up window that is displayed, enter a comment and click **Save**.

Updating Certificate Attributes for Client Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate for which you want to update attributes.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

• Bulk Updating Attributes using a CSV File
• Bulk Updating Attributes for a Certificate Group
• Downloading Failed Updates
• Bulk Updating Attributes using a CSV File
• Bulk Updating Attributes for a Certificate Group
• Bulk Updating Attributes using a CSV File
• Bulk Updating Attributes for a Certificate Group
• Bulk Updating Attributes using a CSV File
• Bulk Updating Attributes for a Certificate Group

Bulk Updating Attributes using a CSV File

1. Go to  (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

   Note: Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to  (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

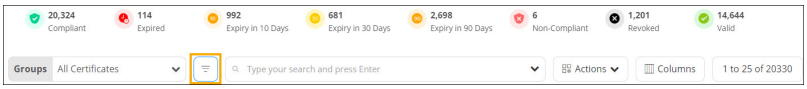
Managing the Code Signing Certificate Inventory

Code signing certificate inventory displays all the code certificate with the EKU (Extended/enhanced key usage) code signing will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificates revocation check, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

The **Code Signing Certificate** page is available under **Certificate Inventory** in the left menu.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options available on the Code Signing Certificate page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates.
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords.
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates.
Columns	Allows you to select the columns to be displayed on the Code Signing Certificate inventory page.
Toggle	Allows you to toggle between the following display options for the Server Certificate inventory: • **Reports**: Displays reports related to server certificates. For more information, click here. • **List**: Displays the list of server certificates.

- Exporting a Code Signing Certificate
- Deleting Code Signing Certificates
- Changing Code Signing Certificate Status
- Assigning Certificate Group for Code Signing Certificates
- Unassigning Certificate Group from Code Signing Certificates
- Adding/Modifying Comments for Code Signing Certificates
- Updating Certificate Attributes for Code Signing Certificates
- Bulk Updating Certificate Attributes

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Exporting a Code Signing Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

To export a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Deleting Code Signing Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any of the reports and alerts.

- Deleting Individual Code Signing Certificates from the Inventory
- Deleting Code Signing Certificates from the Holistic View
- Deleting all Code Signing Certificates

Deleting Individual Code Signing Certificates from the Inventory

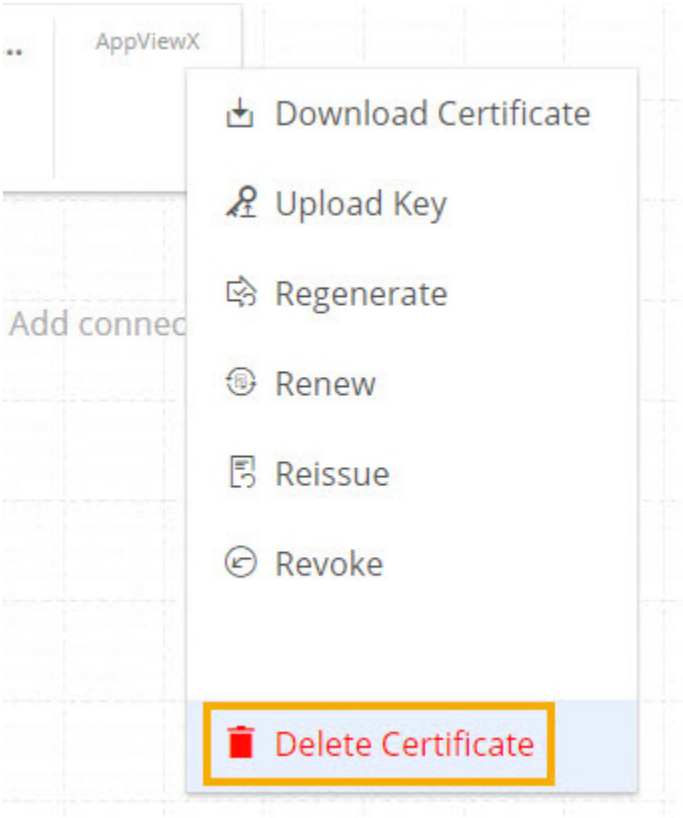
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. From the **Code Signing Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Deleting Code Signing Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. From the **Code Signing Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) button and from the menu displayed, click **Delete Certificate**.

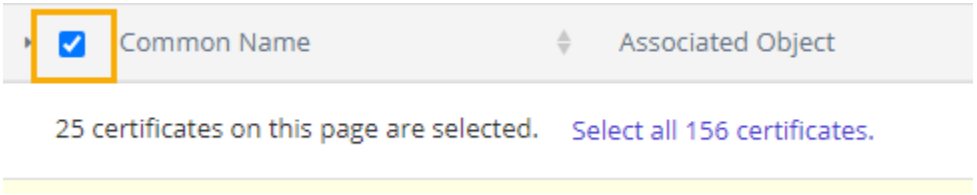


4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The code signing certificate is deleted from the AppViewX inventory.

Deleting all Code Signing Certificates

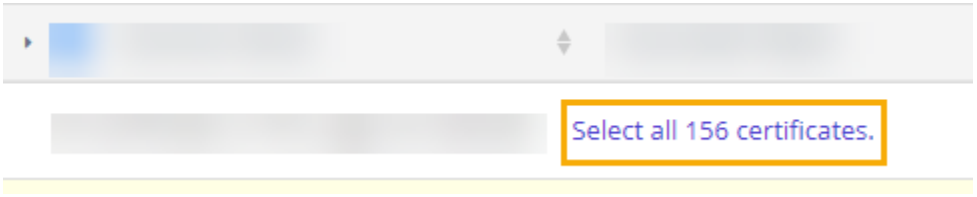
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. In the **Code Signing Certificate** inventory, select the checkbox next to the **Common Name** field.

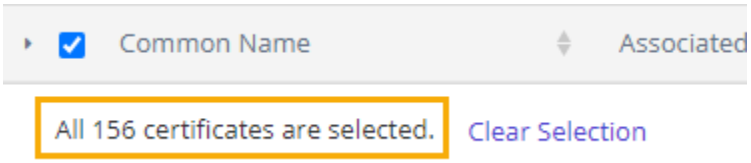


All certificates on the current page are selected.

3. To select all certificates in the code signing certificate inventory, click **Select all <no. of certificates> certificates**.



This will select all certificates across all pages in the code signing certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certficate** confirmation dialog box, clieck **Yes**.
   All certificates in the code signing certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificiates will be deselected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Changing Code Signing Certificate Status

The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you can only view the certificate details in reports and in the inventory. When the certificates are set as Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the code signing certificate status:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate for which you want to change status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** dialog box that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.
5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group for Code Signing Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a certificate group to a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** dialog box that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Unassigning Certificate Group from Code Signing Certificates

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.
4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Adding/Modifying Comments for Code Signing Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** pop-up window that is displayed, enter a comment and click **Save**.

Updating Certificate Attributes for Code Signing Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attributes for a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Bulk Updating Certificate Attributes

- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Downloading Failed Updates
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing**.
   The **Code Signing Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing**.
   The **Code Signig Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

Managing the Device Certificate Inventory

Device certificate inventory displays all the management interface certificates. Currently, in this inventory, only F5 vendor certificates are shown.

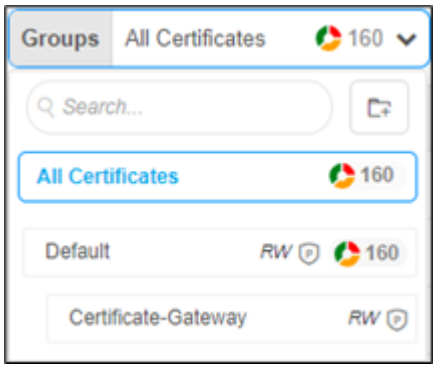
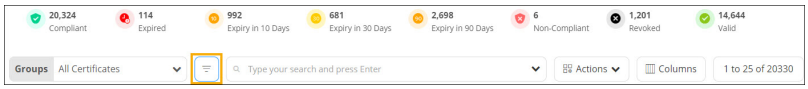
The **Device Certificate** page is available under **Certificate Inventory** in the left menu.

Options available on the Device Certificate inventory page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options available on the Device Certificate inventory page (continued)

Options	Description
	
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates.
Columns	Allows you to select the columns to be displayed on the Device Certificate inventory page.
Toggle	Allows you to toggle between the following display options for the Server Certificate inventory: • **Reports**: Displays reports related to server certificates. For more information, click here. • **List**: Displays the list of server certificates.

- Exporting a Device Certificate
- Deleting Device Certificates
- Assigning Certificate Group to Device Certificates
- Unassigning Certificate Group from Device Certificate Groups
- Adding/Modifying Comments for Device Certificates
- Updating Certificate Attributes for Device Certificates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Bulk Updating Certificate Attributes
- Downloading Failed Updates

Exporting a Device Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

To export a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Deleting Device Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

- Deleting Individual Device Certificates from the Inventory
- Deleting Device Certificates from the Holistic View
- Deleting All Device certificates

Deleting Individual Device Certificates from the Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.

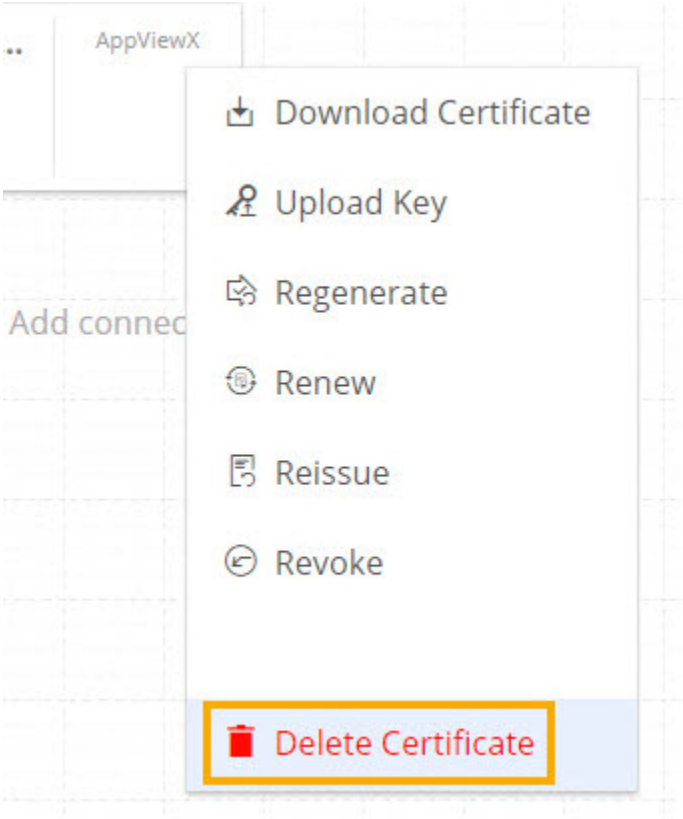
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Deleting Device Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.

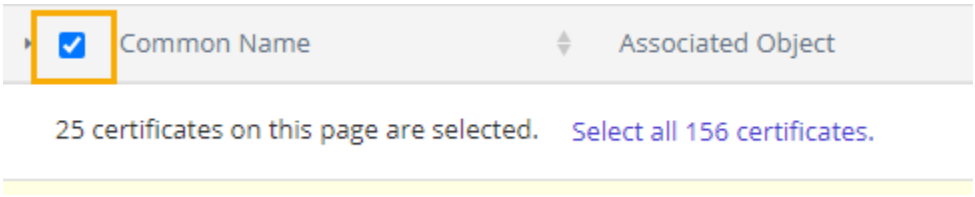


4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The device certificate is deleted from the AppViewX inventory.

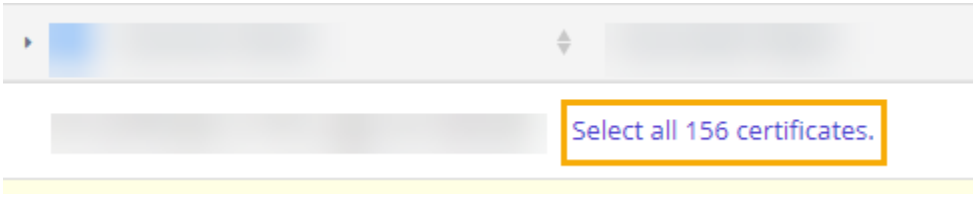
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Deleting All Device certificates

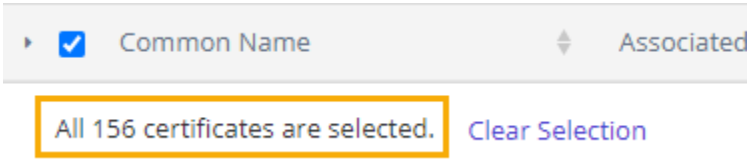
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, select the checkbox next to the **Common Name** field.



   All certificates on the current page are selected.
3. To select all certificates in the device certificate inventory, click **Select all <no. of certificates> certificates**.



   This will select all certificates across all pages in the device certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certficate** confirmation dialog box, clieck **Yes**.
   All certificates in the device certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificiates will be deselected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Assigning Certificate Group to Device Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a certificate group to device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Device Certificate Groups

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.
4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Adding/Modifying Comments for Device Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to revoke.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** dialog box that is displayed, enter a comment and click **Save**.

Updating Certificate Attributes for Device Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attributes for a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Downloading Failed Updates
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group
- Bulk Updating Attributes using a CSV File
- Bulk Updating Attributes for a Certificate Group

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
   The **Device Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
   The **Device Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

Managing the Intermediate Certificate Inventory

Intermediate certificate inventory is where the issuer certificates apart from the root certificate will be displayed. In the chain of trust, if there is more than one layer of the intermediate certificate (excluding root and end certificate), all those certificates will be shown in this inventory. From this inventory, the user can get into the holistic view where the user can perform the push operation of the intermediate and its root certificates.

Options available on the Intermediate Certificate page

Options	Description
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords and by Certificate Authority.
Actions	Displays the list of actions you can perform on the certificates. **Note:** This dropdown is enabled only when you select at least one certificate from the inventory.
Columns	Allows you to select the columns to be displayed on the **Intermediate Certificate** page.

• Deleting an Intermediate Certificate

Deleting an Intermediate Certificate

You can delete a certificate from the intermediate certificate inventory in AppViewX. Once the certificate gets deleted from the inventory, the same will not be displayed in reports and alerts.

To delete an intermediate certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
2. On the **Intermediate Certificate** page, select the certificate that you want to delete.
3. From the **Actions** dropdown menu, select **Delete**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. In the **Delete Certificate** dialog box that is displayed, click **Yes**.
   The intermediate certificate is deleted from AppViewX inventory.

Managing the Root Certificate Inventory

Root certificate inventory displays the root certificates for all the issuers. For any chain of trust certificates, there can be only one root certificate. From this inventory, you can get into the holistic view and perform the push operation for the root certificate only.

Options available on the Root Certificate page

Options	Description
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords and by Certificate Authority.
Actions	Displays the list of actions you can perform on the certificates. **Note:** This dropdown is enabled only when you select at least one certificate from the inventory.
Columns	Allows you to select the columns to be displayed on the **Intermediate Certificate** page.

• Deleting a Root Certificate

Deleting a Root Certificate

You can delete a certificate from the root certificate inventory in AppViewX. Once the certificate gets deleted from the inventory, the same will not be displayed in reports and alerts.

To delete a root certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
2. On the **Root Certificate** page, select the certificate that you want to delete.
3. From the **Actions** dropdown menu, select **Delete**.
4. In the **Delete Certificate** dialog box that is displayed, click **Yes**.
   The root certificate is deleted from AppViewX inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Uploading a Certificate

You can upload either the end certificate or trust store certificates in the certificate inventory. Once uploaded, the certificate will be applied by the policy based on the associated certificate group.

To upload a certificate,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Upload**.
   The **Upload Certificate** page is displayed.
2. Enter/Select the **Upload Certificate**details.

Field descriptions on for uploading a certificate

Field	Description
Certificate Type	Click the check box to select the desired certificate type. The possible types are: • End Certificate • CA Certificate.
Certificate Group	Select the desired group from the dropdown list.
***Certificate**	Click **Browse** to upload the certificate-key files from your computer.
Comments	Enter a description in this field. **Note:** Character limit: **2000 characters**

3. Click **Upload**.

Note: Ensure that the uploaded **Certificate-Keys** file is stored in the Certificate Group.

Downloading Certificates

- Downloading Server Certificates
- Downloading Client Certificates from the Holistic View
- Downloading Device Certificates from the Holistic View
- Downloading Code Signing Certificates from the Inventory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Downloading Intermediate Certificates
• Downloading Root Certificates

Downloading Server Certificates

• Downloading Server Certificates from the Inventory
• Downloading Server Certificates from the Holistic View

Downloading Server Certificates from the Inventory

Server certificates can be downloaded from the server inventory as well as in the holistic view. In the server inventory, the user can select one or more certificates and download them in <*.crt*> format with/without private keys and also with/without their respective trust store certificates.

To download server certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
3. Click **Actions**, and then select **Download Certificates** from the list.
   The **Download Certificates** dialog box is displayed.
   a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
   b. You can also enable/disable **the Download Truststore Certificates** option along with the end certificates.

   > **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

   c. The system enables the **Secret Passphrase** field when you select **Certificates and Keys**. Enter a passphrase to encrypt the contents into a <.zip> file.
4. Click **Download**.
   The certificate is downloaded to your local machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

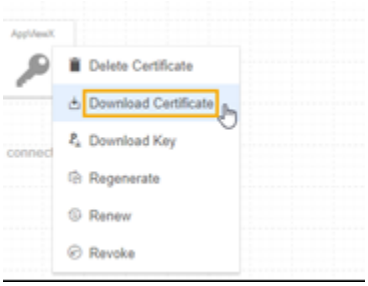
5. To view details of the certificate, unzip the file and open the security certificate file.
6. Click **Details**.

Downloading Server Certificates from the Holistic View

Server certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download server certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, click the **Common Name** of the certificate you want to download.
   The holistic view of the certificate is displayed.
3. Hover your mouse over and select **Download Certificate** from the options displayed.



   The **Download Certificate** pop-up window is displayed.
4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

> **Note:** For PEM and DER certificate types, you can use turn the **Download Truststore Certificates** toggle On/Off.

   The certificate(s) is downloaded to your local machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Downloading Client Certificates from the Holistic View

Client certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download client certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. On the **Client Certificate** page, click on the **Common Name** of the certificate that you want to download.
   The holistic view of the certificate is displayed.
3. Hover your mouse over and select **Download Certificate** from the options displayed.
   The **Download Certificate** dialog box is displayed.
   a. Select the file format from the **Certificate Type** list.
   b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.
4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

   Note: For PEM and DER certificate types, you can use turn the **Download Truststore Certificates** toggle On/Off.

   The certificate(s) is downloaded to your local machine.

Downloading Device Certificates from the Holistic View

Device certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download device certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
   The **Device Certificate** page is displayed.
2. On the **Device Certificate** page, click the **Common Name** of the certificate you want to download.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The holistic view of the certificate is displayed.

3. Hover your mouse over  and select **Download Certificate** from the options displayed.
   The **Download Certificate** dialog box is displayed.
4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

   > **Note:** For PEM and DER certificate types, you can use turn the **Download Truststore Certificates** toggle On/Off.

   The certificate(s) is downloaded to your local machine.

Downloading Code Signing Certificates from the Inventory

Code Signing certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download code signing certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. On the **Code Signing Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download Certificates**.
   The **Download Certificates** pop-up window is displayed.
   a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
   b. You can also enable/disable **Download Truststore Certificates** option along with the end certificates.

      > **Note:** If you have permission to view the restricted content, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

   c. The system enables the **Secret Passphrase** field when you select the **Certificates and Keys** option. Enter a passphrase to encrypt the contents into a *<.ZIP>* file.
4. In the **Download Certificate** dialog box, enter or select the requested filed information.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Download Certificate

Field	Description
Choose Download Type	Select the certificate download type as: • **Certificate Only** • **Certificate and Keys**
Download Truststore Certificates	Turn on this toggle to download truststore certificates.
Set Password for Keystore	Enter a passphrase to encrypt the contents into a **.zip** file.

a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.

b. You can also enable/disable **the Download Truststore Certificates** option along with the end certificates.

> **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

c. The system enables the **Secret Passphrase** field when you select **Certificates and Keys**. Enter a passphrase to encrypt the contents into a <.zip> file.

5. Click **Download**.
6. To view details of the certificate, unzip the file and open the security certificate file.
7. Click **Details**.

Downloading Intermediate Certificates

- Downloading Intermediate Certificates from the Inventory
- Downloading an Intermediate Certificate from the Holistic View

Downloading Intermediate Certificates from the Inventory

You can download intermediate certificate(s) in PEM format with or without its trust store certificates.

To download internediate certificates:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
   The **Intermediate Certificate** page is displayed.
2. On the **Intermediate Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download**.
   The certificate is downloaded to your local machine.
4. To view details of the certificate, unzip the file and open the security certificate file.
5. Click **Details**.

Downloading an Intermediate Certificate from the Holistic View

Intermediate certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download an intermediate certificate via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
2. On the **Intermediate Certificate** page, click the **Common Name** of the certificate that you want to download from the holistic view.
   The holistic view of the certificate is displayed.
3. Hover your mouse over the (**More**) button and click **Download Certificate**.
4. In the **Download Certificate** pop-up window that is displayed, select the **Certificate type** from the options available in the dropdown.
5. For PEM and DER certificate types, turn on the **Download Truststore Certificates** toggle.
6. Click **Yes**.
   The certificate is downloaded to your local machine.

Downloading Root Certificates

- Downloading Root Certificates from the Inventory
- Downloading a Root Certificate from the Holistic View

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Downloading Root Certificates from the Inventory

Download root certificate is the action to download root certificate, the certificate get downloaded in PEM **.*crt** format from the inventory.

To download root certificates from the inventory:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
   The **Root Certificate** page is displayed.
2. On the **Root Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download**.
   The certificate is downloaded to your local machine
4. To view details of the certificate, unzip the file and open the security certificate file.
5. Click **Details**.

Downloading a Root Certificate from the Holistic View

Download root certificate is the action to download root certificate in PEM format with or without its trust store certificates.

To download a root certificate via the holistic view,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
   The **Root Certificate** page is displayed.
2. In the **Common Name** column certificate list, select the desired certificate that you want to download the CA.
   The holistic view is displayed.
3. Click the (**More**) icon in the holistic view, and then select **Download Certificate** from the list.
   The **Download Certificate**dialog box is displayed.
4. Select the file format from the **Certificate type** list.
5. Click **Yes**.
   The certificate is downloaded to your local machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Reporting and Monitoring

Once the certificates in the infrastructure are discovered in AppViewX, they can be monitored as the reports in the Dashboards. In the dashboards, the user can track the certificates expiry, compliance, security details as the reports in the dashboard.

Reporting and monitoring the certificates are essential for an administrator to get complete visibility of all the certificates across multiple vendors and data centers in one single window pane. Certificates have a finite life span and are set to expire at different dates and times. Due to advancements in cryptography, there are high chances that the infrastructure will carry the weaker algorithm certificates which will be vulnerable to several attacks which will cause business outages. Using the dashboards and reports, the administrator can continuously monitor the status of the certificates in terms of expiry, security, compliance and so on.

- Accessing the Dashboard
- Creating a Dashboard
- Exporting Dashboard Information
- Importing a Dashboard
- Understanding Certificate Reports on the Dashboard
- Searching for Dashboard, Object, or Widget
- Deleting a Dashboard

Accessing the Dashboard

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. To go to the Dashboard inventory, form the top left corner of the screen, click **Dashboard**.

> **Note:** You can also click from the command bar.

The **Dashboard** page is displayed.

Dashboard page Actions

Options	Description
Search bar	Search using the required keyword(s)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Description
	The research result is a list of items that match the specified keywords(s).
+	Allows users to create a **New** dashboard.
	Allows users to **Delete** a dashboard from the list.
	Allows users to **Export** a dashboard from the list.
	Allows users to **Import** a file to create a dashboard.
	**Refresh** the dashboard page
	Allows users to **Auto-sort** the dashboards alphabetically.

Creating a Dashboard

1. Go to  (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. From the command bar on the top right corner of the page, click +.
   The **Create dashboard/widget** pop-up window is displayed.
3. In the **Create dashboard/widget** dialog box, enter or select the requested field information as described in the table below.

Field Description for Create dashboard/widget

Field	Description
***Dashboard name**	Enter the name of the dashboard.
***Select solution**	Select a solution from the options available in the dropdown.
***Widget type**	Select the type of the widget you want to create. The options are: • **Custom**: Select this option to create a customized Widget. • **Default**: Select this option to create a default Widget.
***Choose widgets**	Select the widget(s) from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when you select **Widget type** as **Default**.
***Select widget**	Select the widget from the customized widgets displayed in the dropdown.
***Widget name**	Enter the name of the Widget.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Create**.
   The dashboard is created.

Note: To discard the changes, click **Cancel**.

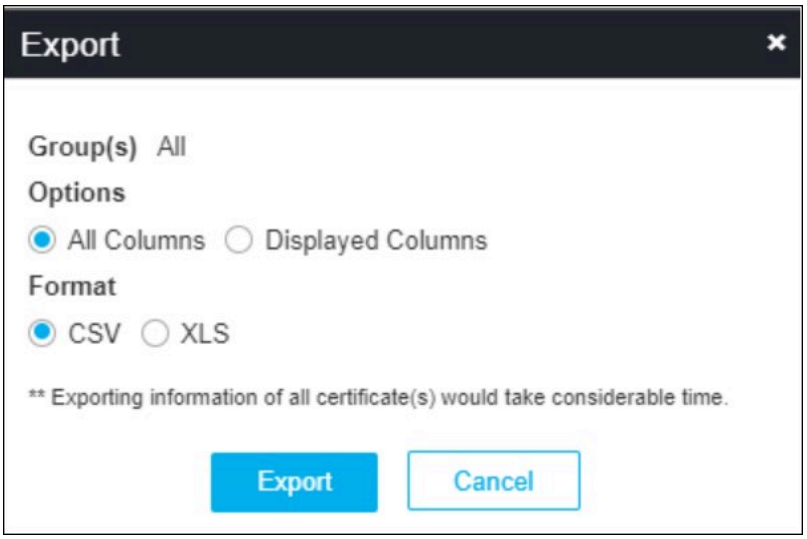
Exporting Dashboard Information

You can export the dashboards in **.csv** or **.json** format. The dashboards that are exported in the **.json** format can be imported to another build of the AppViewX platform.

To export dashboard information:

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. Select the dashboard to be exported and from the command bar at the top right corner of the screen, click the export icon.
   The **Export** pop-up window is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



3. Select the required **Options** and **Format**.
   The selected dashboard(s) are exported to your local machine.

Importing a Dashboard

You can import the list of dashboards, which has the **Application View** widget. The import file must be in the **.text** and/or **.json** format and zipped.

To import a dashboard:

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. From the command bar at the top right corner of the dashboard page, click **Import**.
   The **Import** page is displayed.
3. Browse and open the dashboard import file in **.zip** format and click **Upload**.
4. Once the file is uploaded, click **Submit**.
   The selected dashboard(s) are imported to AppViewX platform.

Understanding Certificate Reports on the Dashboard

Certificate Reports give you visibility over all certificates and host information in the CERT+ inventory through different modes of discovery. With the available data, you can validate whether these certificates fall under the organization's security policy. CERT+ reports give insights on all important aspects of the product.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

All these reports are categorized and available as multiple dashboards as default in AppViewX. Provided with that, custom dashboards with custom reports can also be created.

- Viewing Certificate Reports
- Default Reports
- Understanding the Server Certificate Dashboard
- Understanding the Client Certificate Dashboard
- Report by Certificate Authority
- Understanding the Code Signing Dashboard
- Stale Certificate Report
- Count of issuer
- Server Certificate Security Dashboard
- Understanding the Client Certificate Security Dashboard
- Understanding the Server Endpoint Security Dashboard
- Understanding the Client Endpoint Security Dashboard
- Understanding the Server Standard Dashboard
- Understanding the Client Standard Dashboard
- Understanding the Trust Store Certificates Dashboard
- Report Customization
- Security Posture Determination and Interpretation
- License Report
- Google 90 Day Dashboard

Viewing Certificate Reports

1. Go to  (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > <type of certificate you want the reports for>.
   The certificate inventory page, for the selected certificate type, is displayed.
2. From the top right corner of the page, click the **Reports** toggle.
   Reports for selected certificate type are displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Although each certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets in the report:

- **Report by Certificate Authority -** A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month -** A bar chart that shows the total number of certificates expiring each month.
- **Policy Compliance -** A pie chart that shows the number of compliant and non-compliant certificates in the system, with each sector in the chart representing a different kind of policy such as Strict or Suggestive. You can also export the report details from the Policy Compliance Report widget.
- **Stale Certificate -** A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary -** A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Report by Certificate Authority widget. You can also configure the report settings from the Certificate Summary Report widget.

- **Count by Issuer -** A doughnut chart that shows the total number of certificates managed by the issuer such as Root CA or the Intermediate CA. You can also configure the report settings from the Count by Issuer widget.

Default Reports

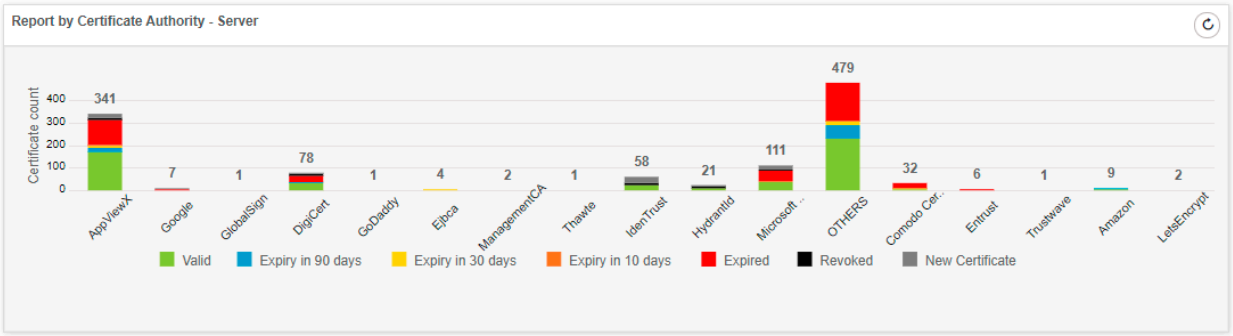
AppViewX CERT+ has a few in-built reports (recommended) that are available as default reports. These reports can be triggered directly to take necessary actions. The primary risk to be addressed is to enforce security compliance. Compliance reports that are provided as in-built reports can be used to categorize certificates based on the non-compliant parameter. This information (value addition) can be used to enforce the application team to onboard for automation.

Understanding the Server Certificate Dashboard

The certificates from the Server inventory will be shown in this dashboard as the following reports:

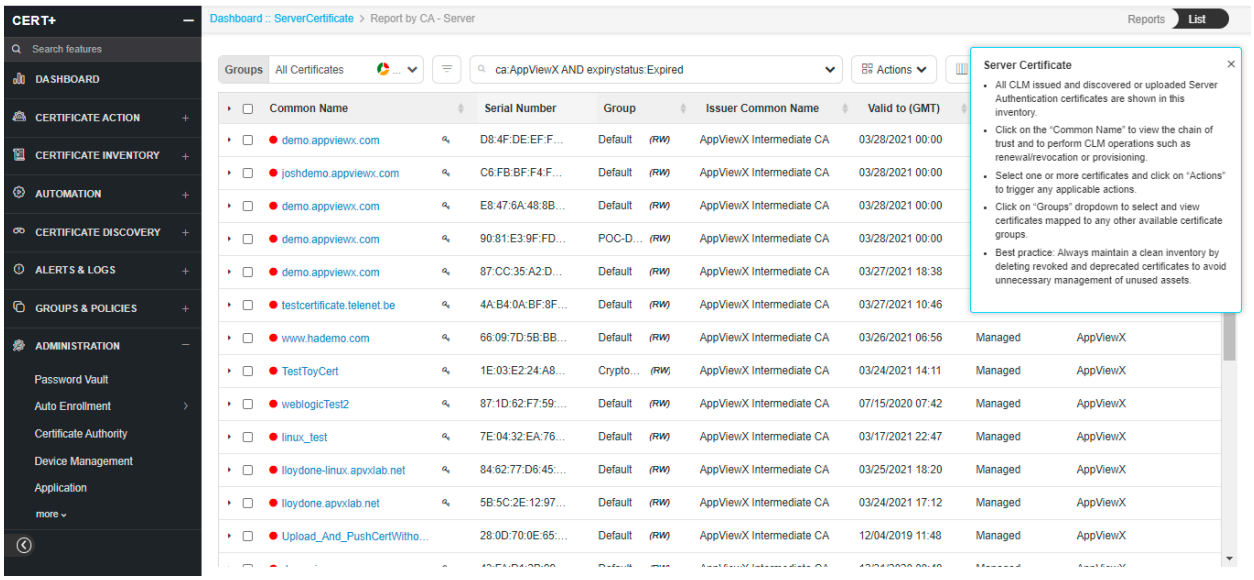
Report by Certificate Authority - Server

This report shows the count of certificates in the server inventory with respect to the certificate authorities and the expiry information.



On click of any of the bar of this report, the filtered inventory view will be shown as below to proceed any further actions:

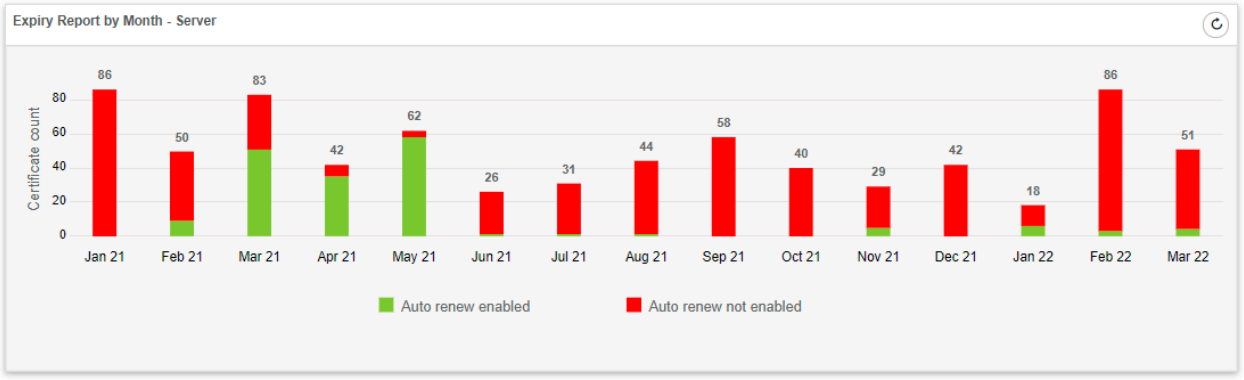
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- Expiry Report by Month
- Validation Status
- Policy Compliance Status
- Report by Source
- Orphan Certificate Report
- Stale Certificate Report
- Certificate Summary Report
- Count by Issuer
- Cipher Suite Report

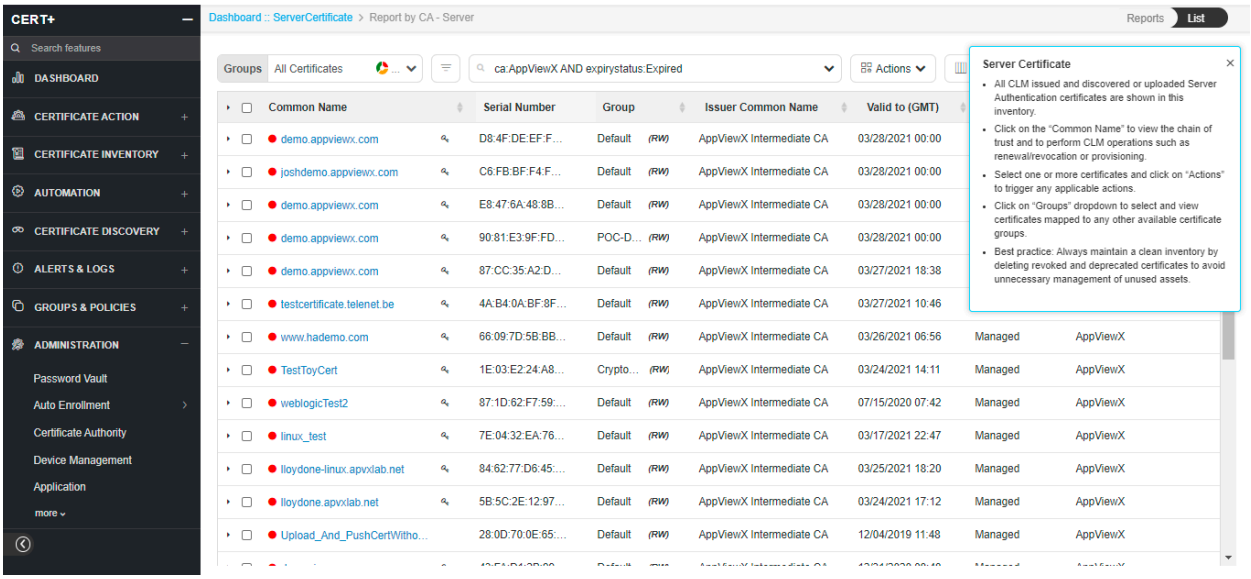
Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

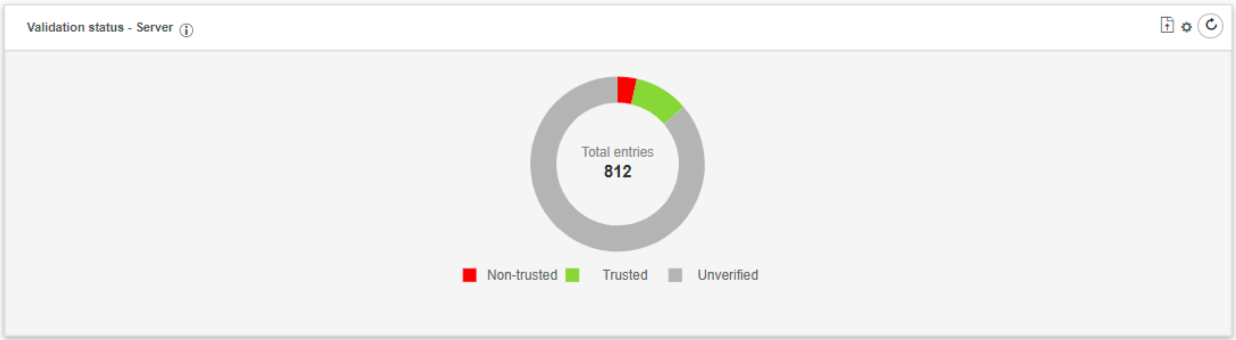
On click of any of the bar, the filtered certificates inventory will be shown as below to perform any inventory actions:



Validation Status

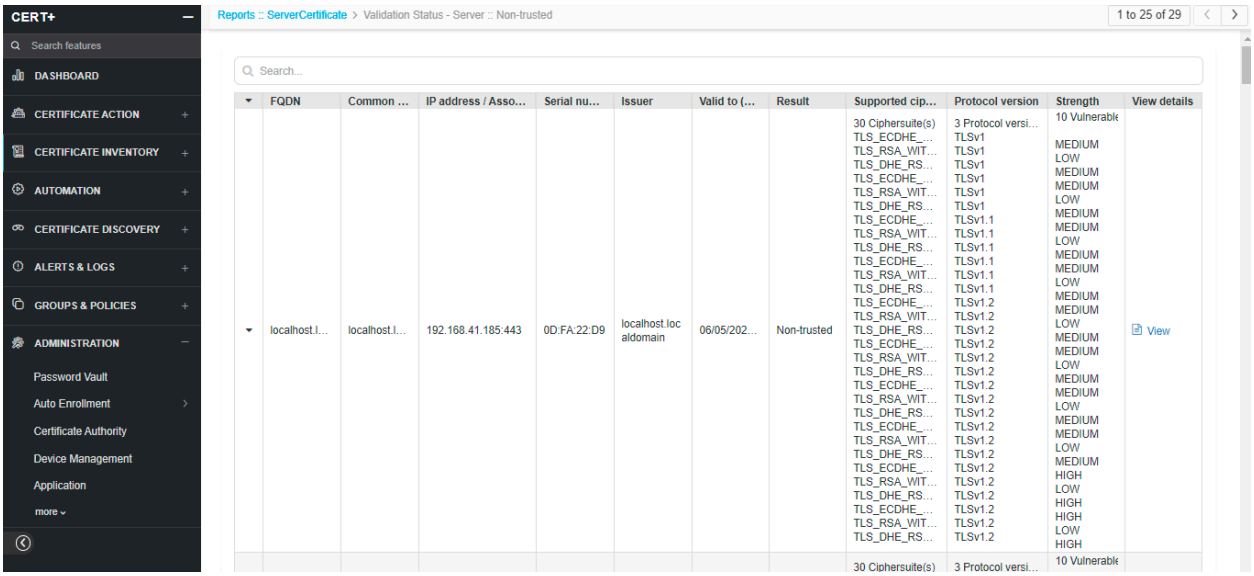
This report shows the count of server certificates with respect to the following:

- Trusted – When the chain of trust can be formed with the end server certificate it will be categorized as a trusted certificate.
- Non-trusted – When the chain of trust cannot be formed with the end server certificate it will be categorized as non-trusted.
- Unverified – When the server certificates are yet to be taken for validation, they will be categorized as unverified.



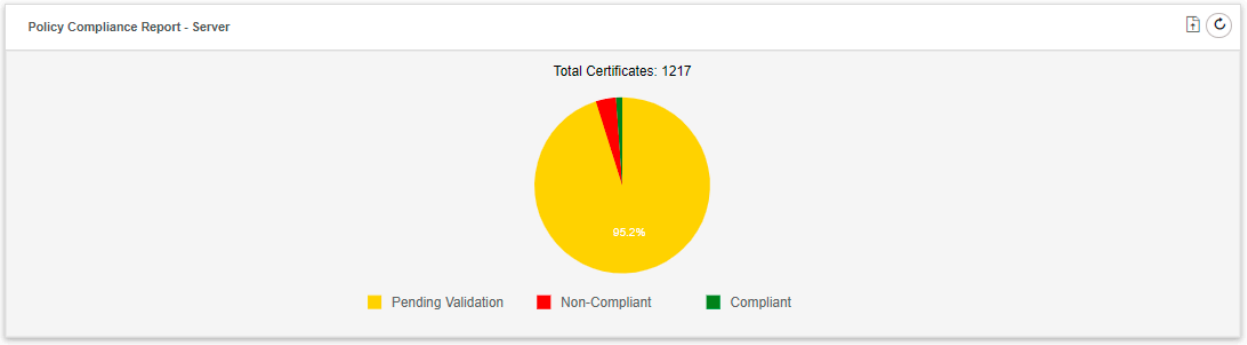
On click of anywhere in this pie chart, the filtered certificates data will be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



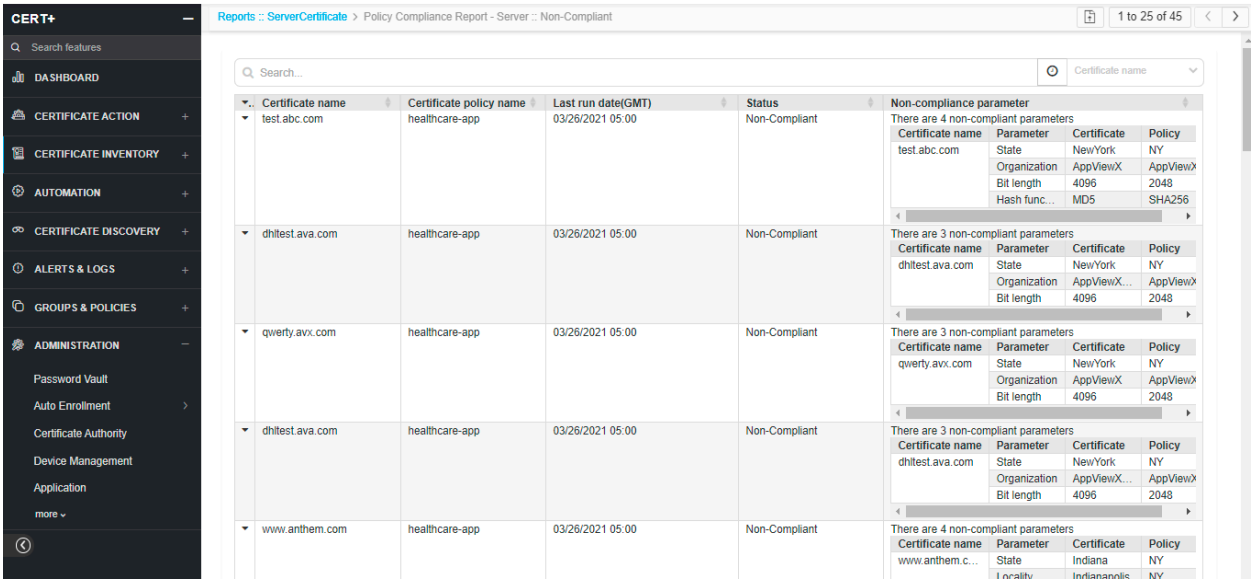
Policy Compliance Status

This report shows the count of server certificates as compliance or non-compliance based on the certificate group policy associated with the certificates.



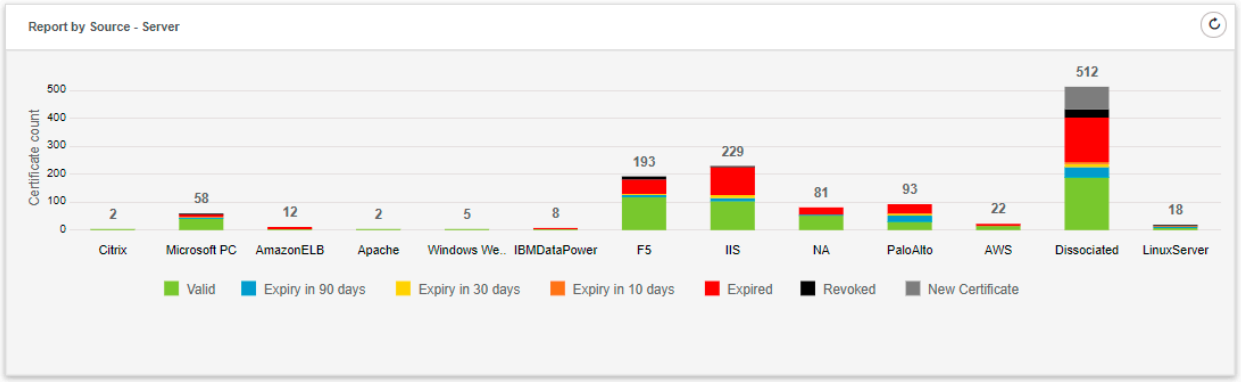
On click of anywhere in the pie chart, the filtered certificates data will be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



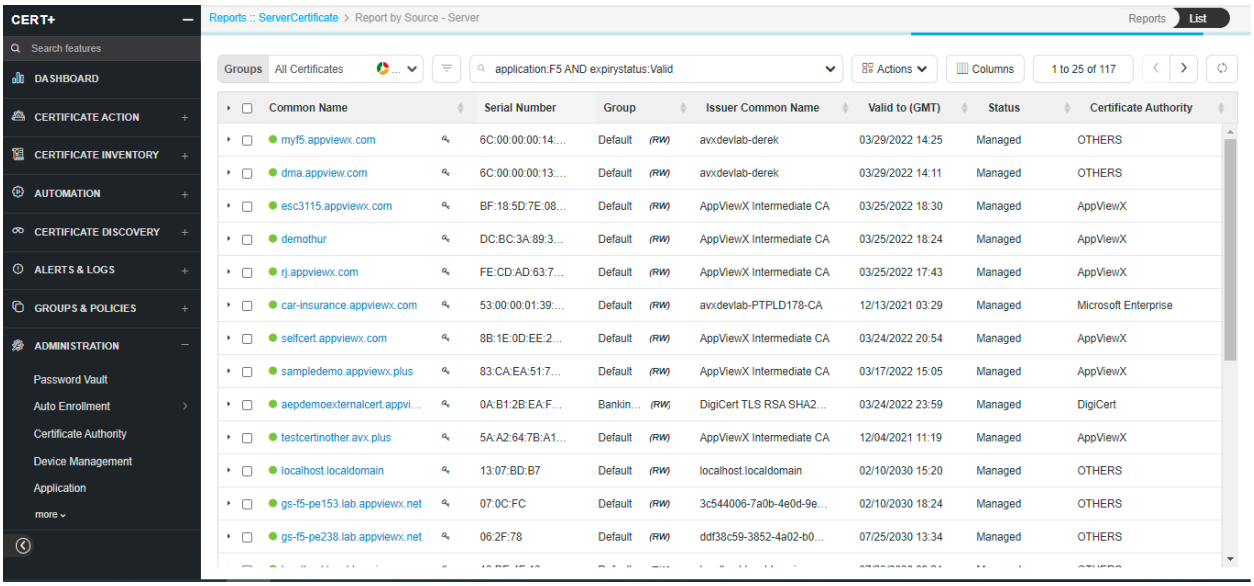
Report by Source

This report shows the count of server certificates with respect to the source from where the certificates are discovered along with the expiry status.



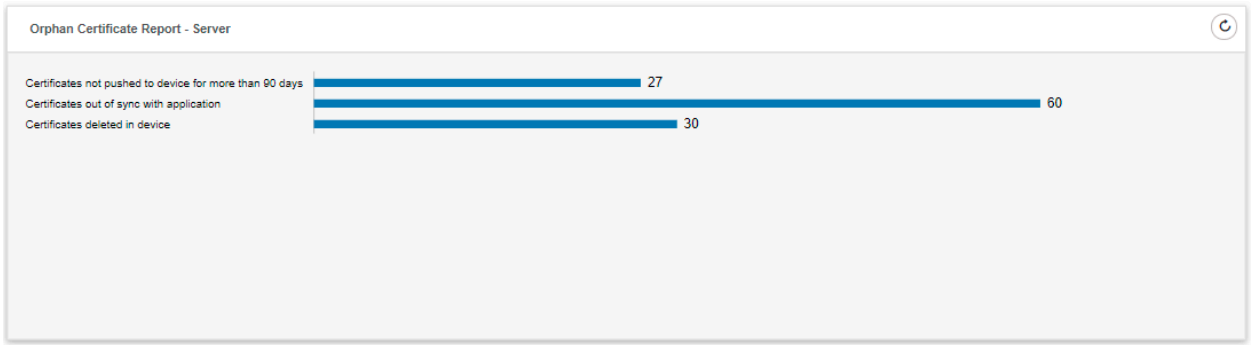
On click of anywhere in the bar chart, the filtered certificates data will be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Orphan Certificate Report

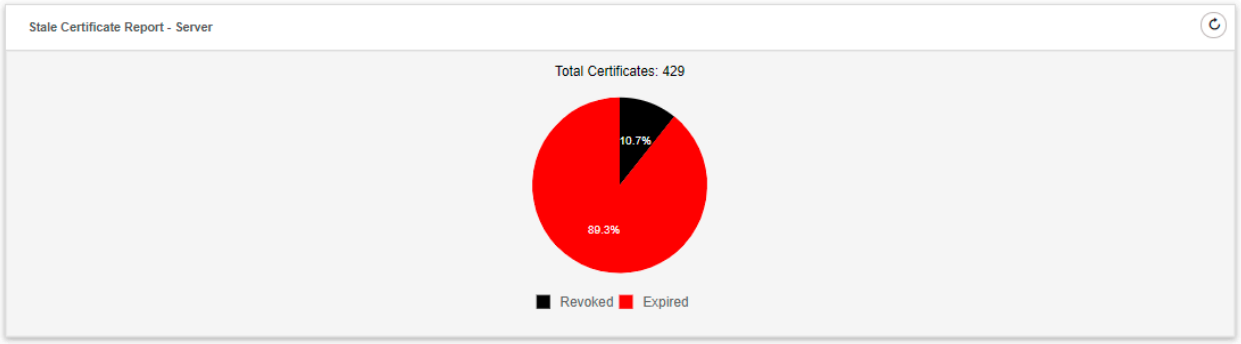
This report shows the count of server certificates that are not associated/installed in any device/server.



Stale Certificate Report

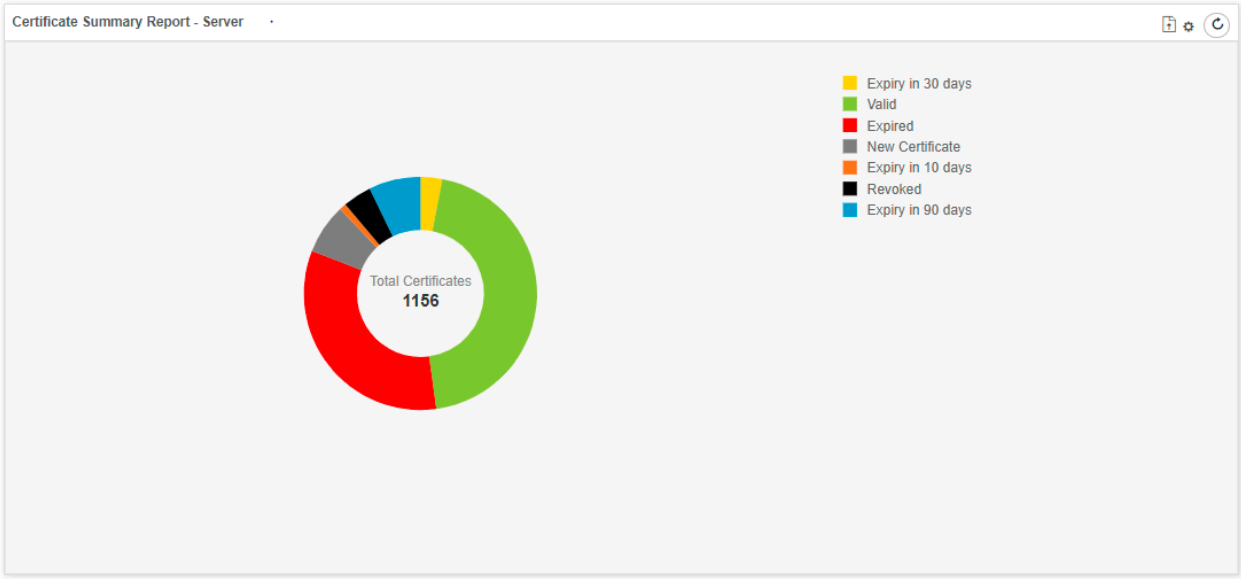
This report shows the count of server certificates that are either revoked or expired.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate Summary Report

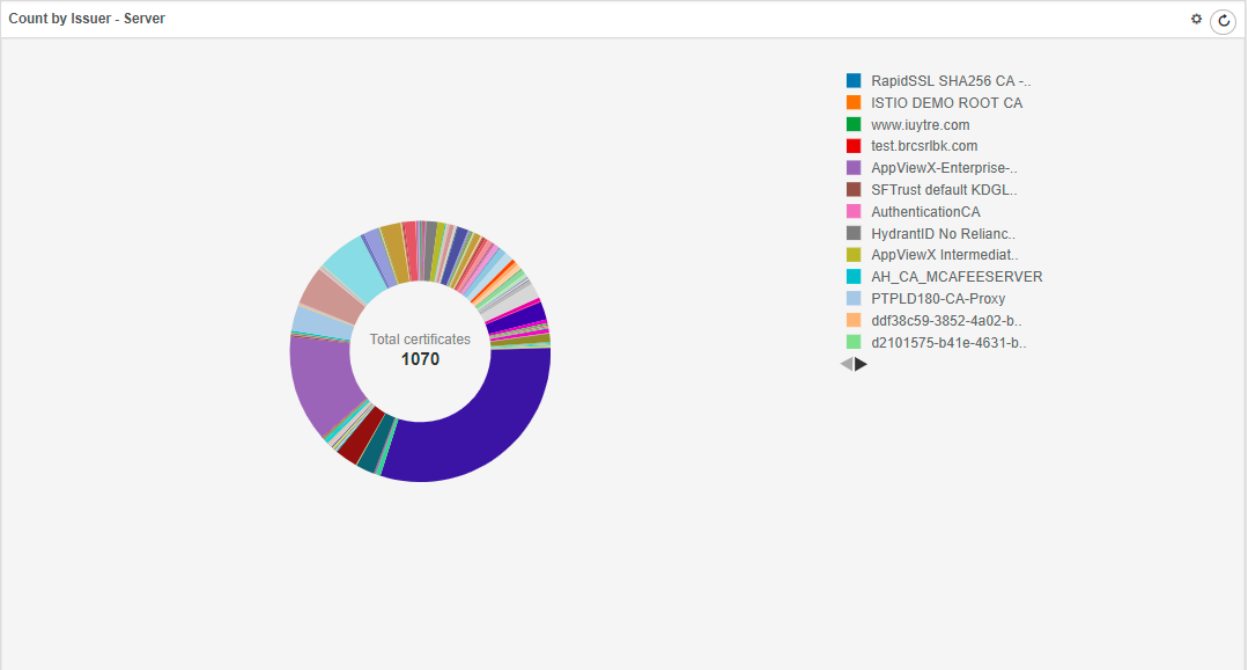
This report shows the count of certificates with respect to their expiry status.



Count by Issuer

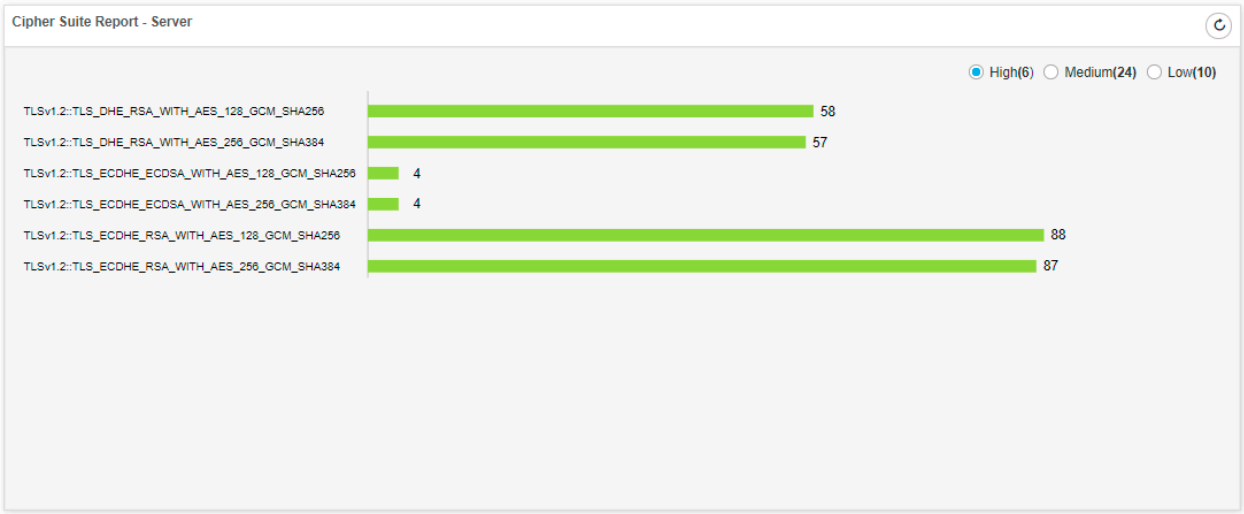
This report shows the count of certificates with respect to the issuer details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Cipher Suite Report

This report shows the count of certificates with respect to the cipher suites. They are also categorized as Low, Medium, and High based on the cipher suites.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

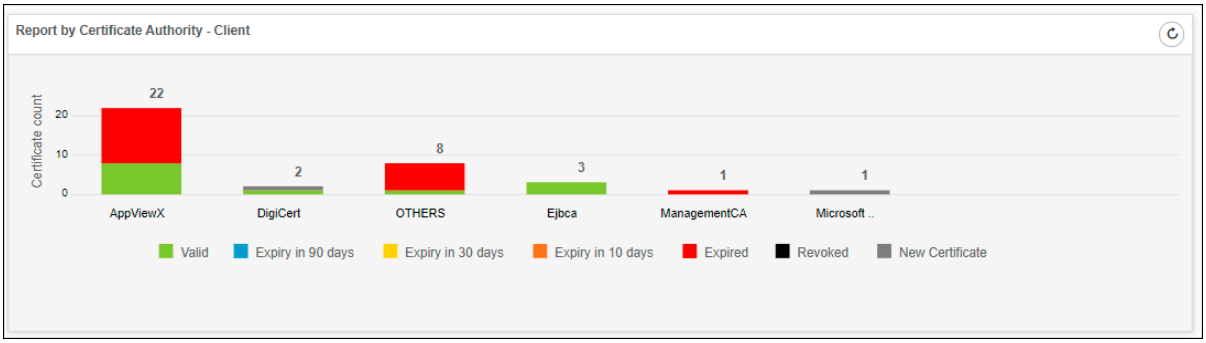
Understanding the Client Certificate Dashboard

This dashboard displays reports related to the certificates from the Client certificate inventory. You can also access this dashboard from the **Client Certificate** inventory page, by selecting **Reports** in the toggle at the top right corner of the page.

- Report by Certificate Authority
- Expiry Report by Month
- Policy compliance status
- Stale certificate report
- Certificate Summary Report
- Count of issuer

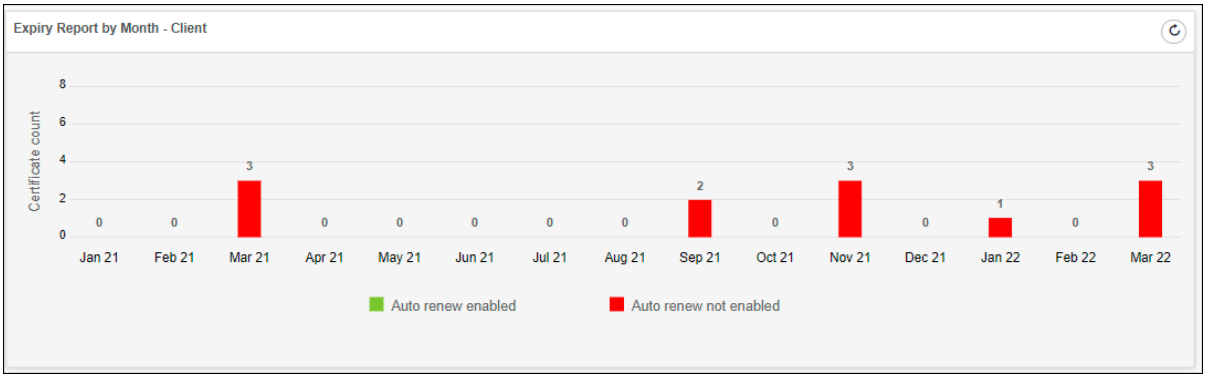
Report by Certificate Authority - Client

This report shows the count of certificates in the client inventory with respect to the certificate authorities and the expiry information.



Expiry Report by Month - Client

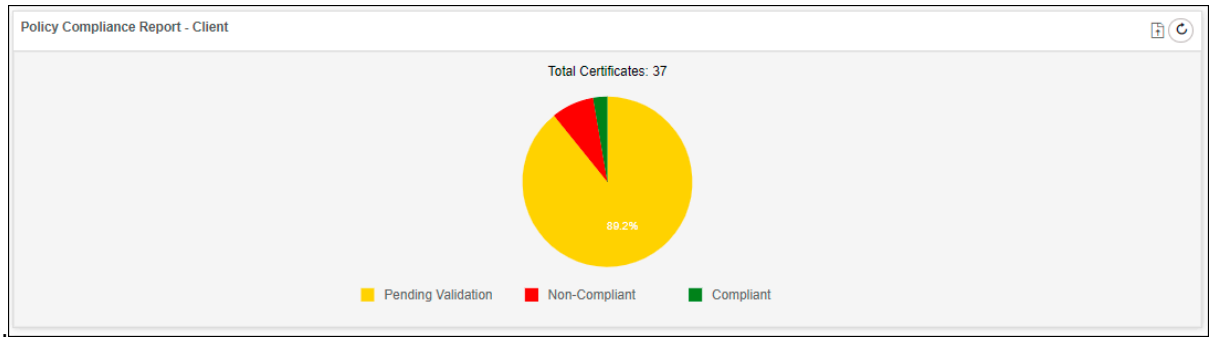
This report shows the count of certificates with respect to expiry month information.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

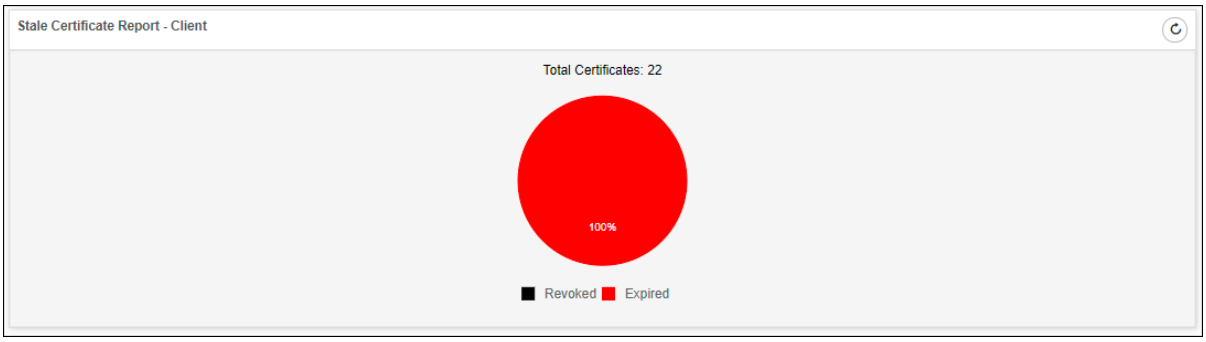
Policy Compliance Report - Client

This report shows the count of client certificates as compliant or non-compliant based on the group policy assigned to the certificate.



Stale Certificate Report - Client

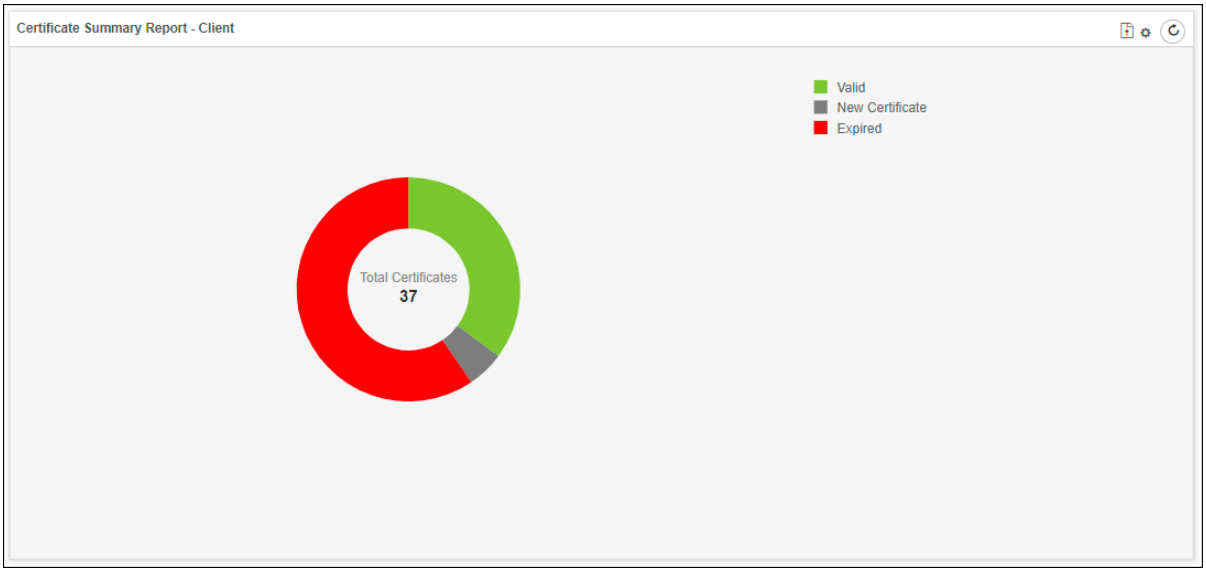
This report shows the count of client certificates that are either revoked or expired.



Certificate Summary Report - Client

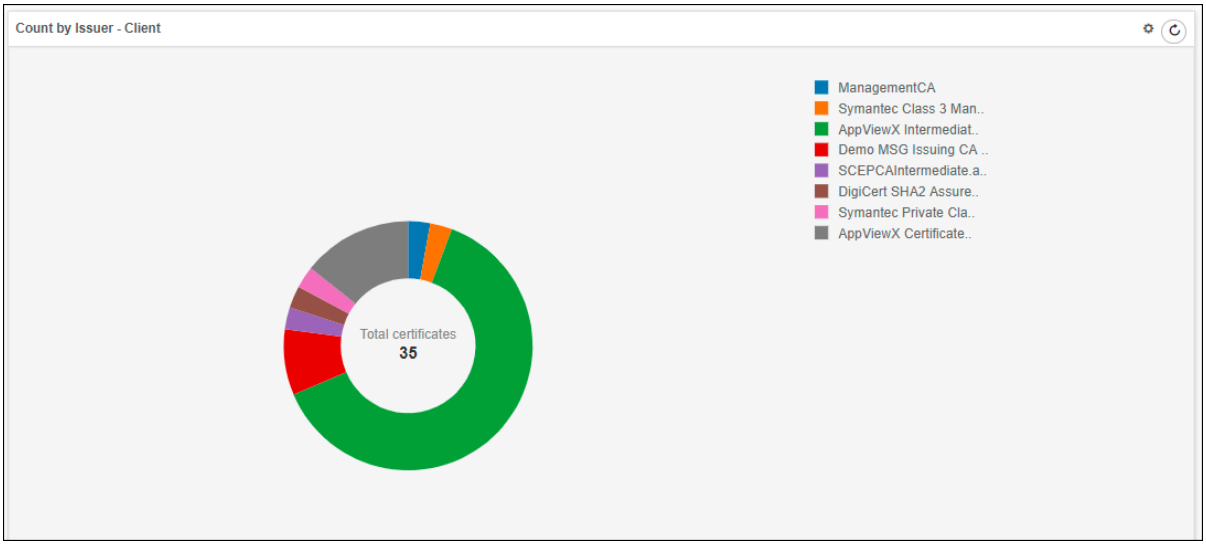
This report shows the count of certificates with respect to their expiry status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Count by Issuer - Client

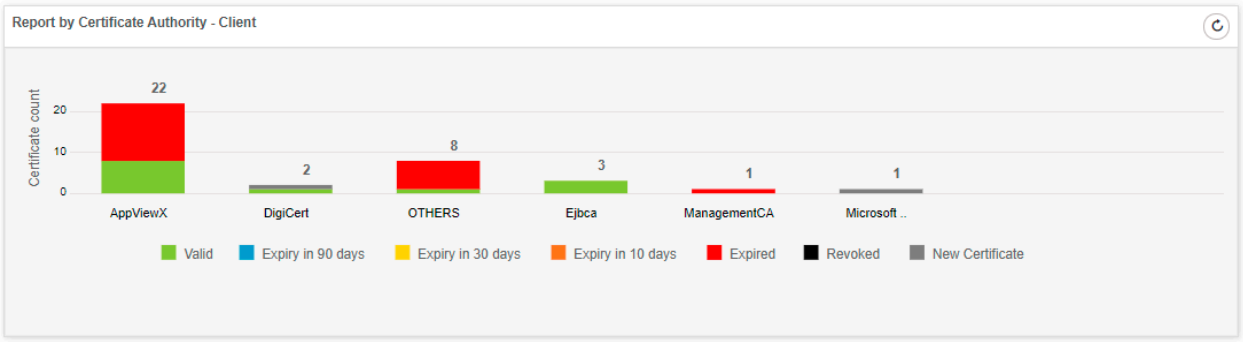
This report shows the count of client certificates with respect to the issuer details.



Report by Certificate Authority

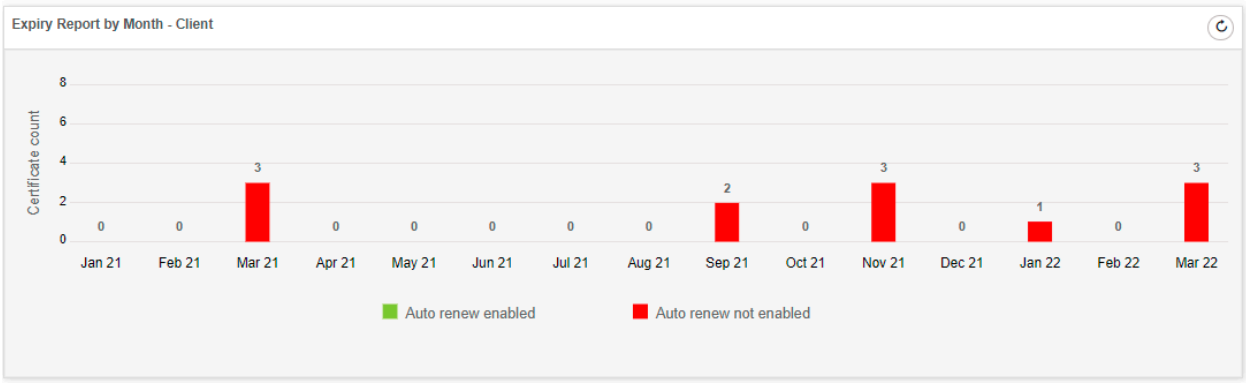
This report shows the count of certificates in the client inventory with respect to the certificate authorities and the expiry information.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



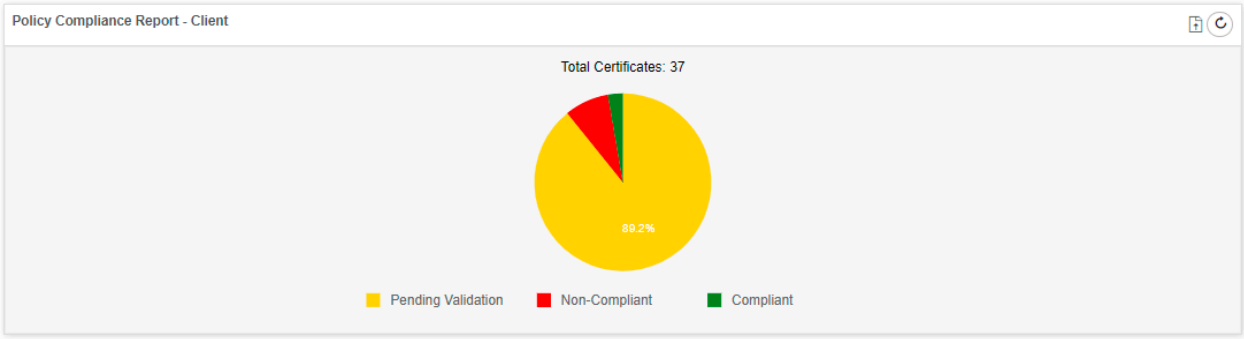
Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



Policy compliance status

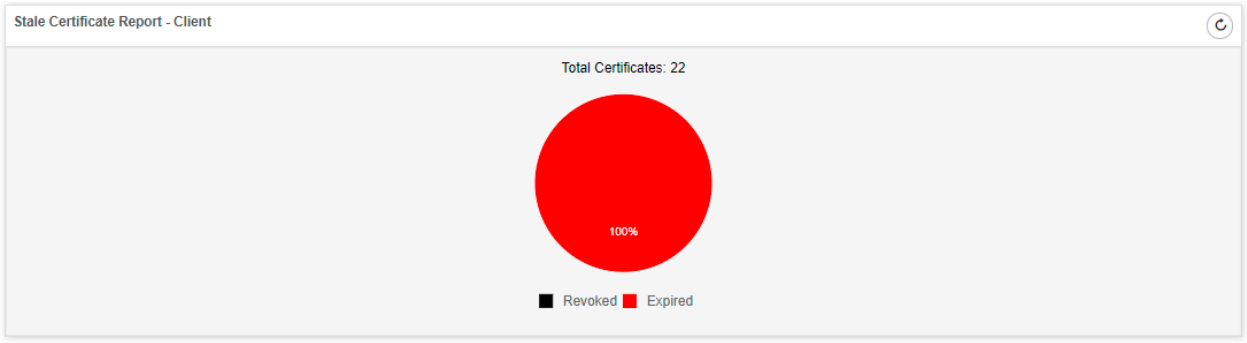
This report shows the count of client certificates as compliance or non-compliance based on the group policy assigned to the certificate.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

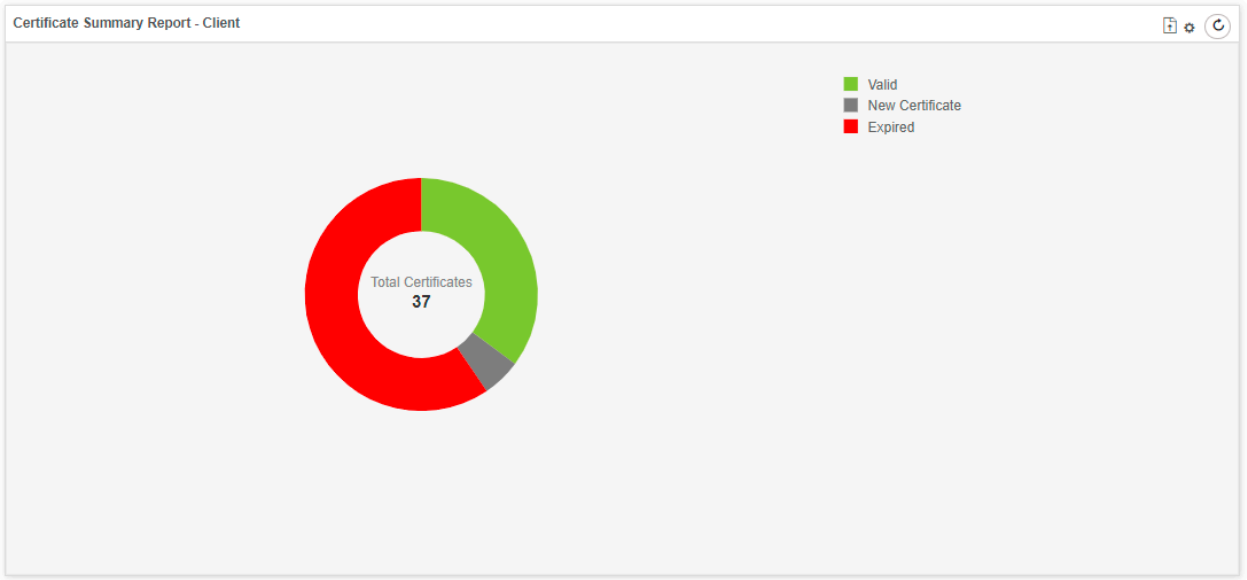
Stale certificate report

This report shows the count of client certificates that are either revoked or expired.



Certificate Summary Report

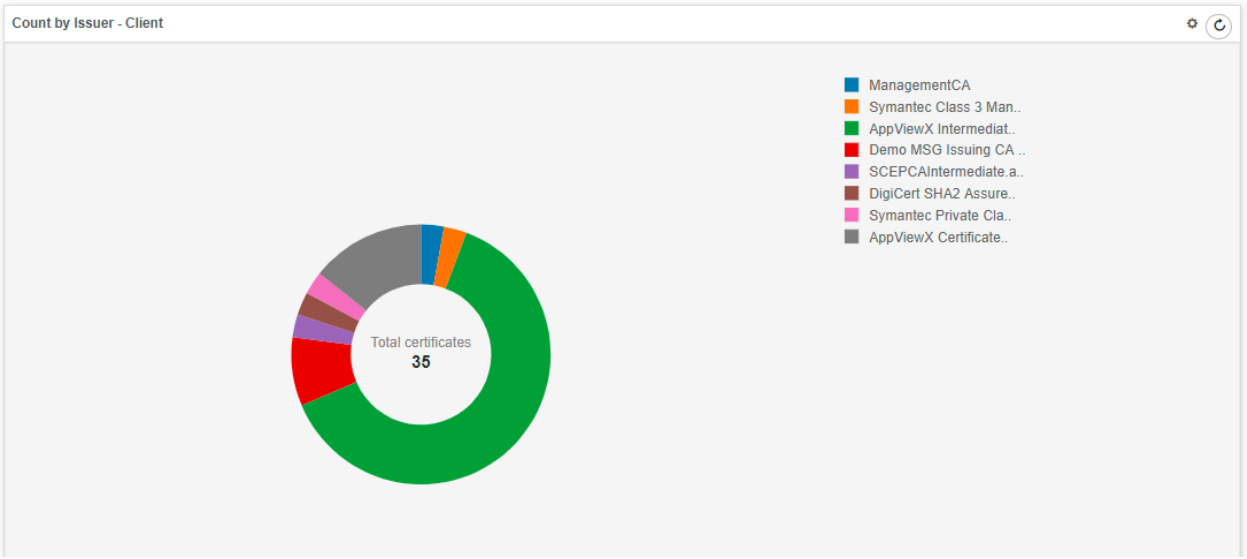
This report shows the count of certificates with respect to their expiry status.



Count of issuer

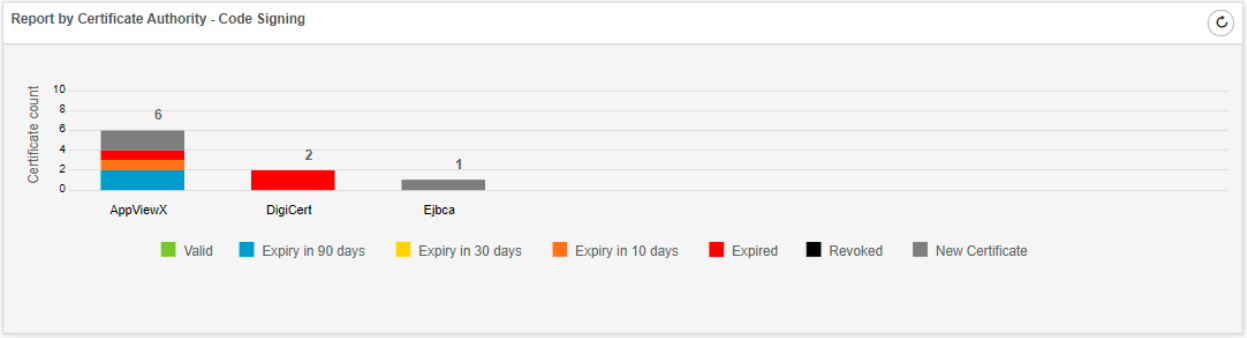
This report shows the count of client certificates with respect to the issuer details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Report by Certificate Authority

This report shows the count of certificates in the code signing inventory with respect to the certificate authorities and the expiry information.



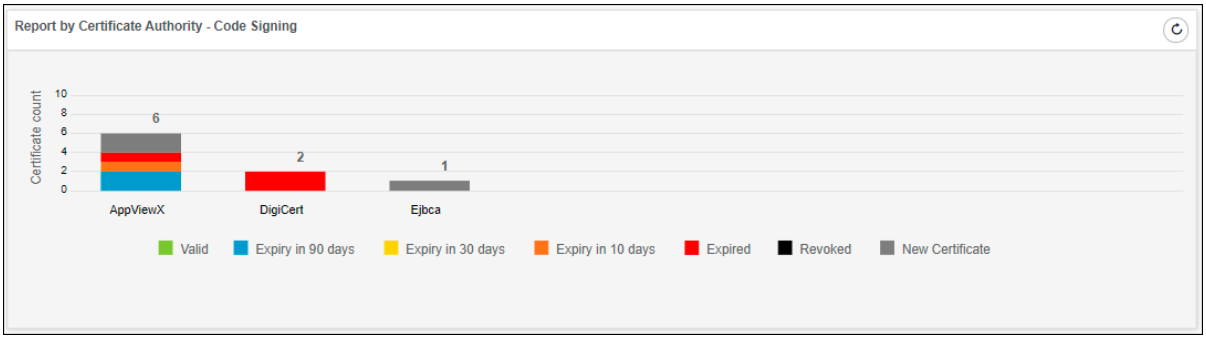
Understanding the Code Signing Dashboard

This dashboard displays reports related to the certificates from the Code Signing certificate inventory. You can also access this dashboard from the **Code Signing Certificate** inventory page, by selecting **Reports** in the toggle at the top right corner of the page.

Report by Certificate Authority - Code Signing

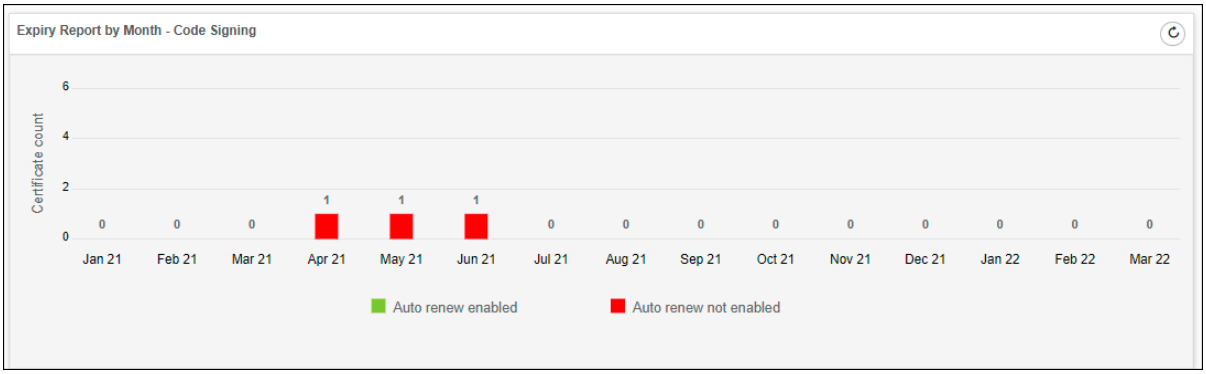
This report shows the count of certificates in the code signing inventory with respect to the certificate authorities and the expiry information.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



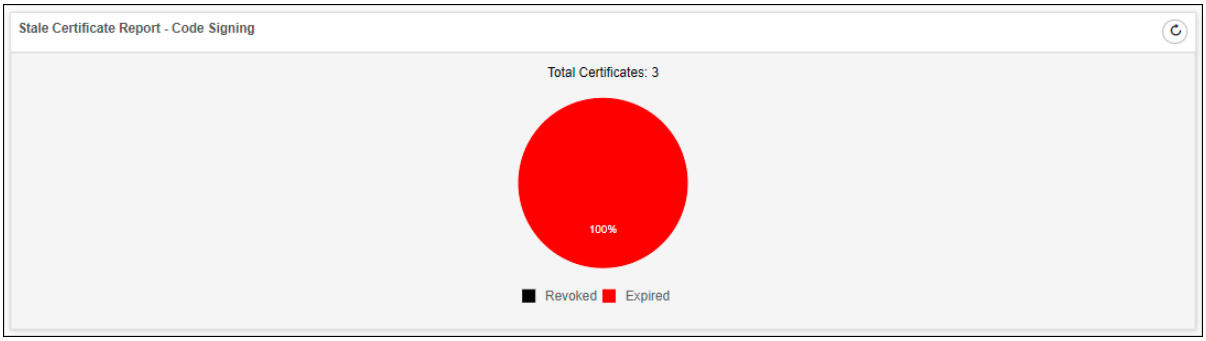
Expiry Report by Month - Code Signing

This report shows the count of code signing certificates with respect to expiry month information.



Stale Certificate Report - Code Signing

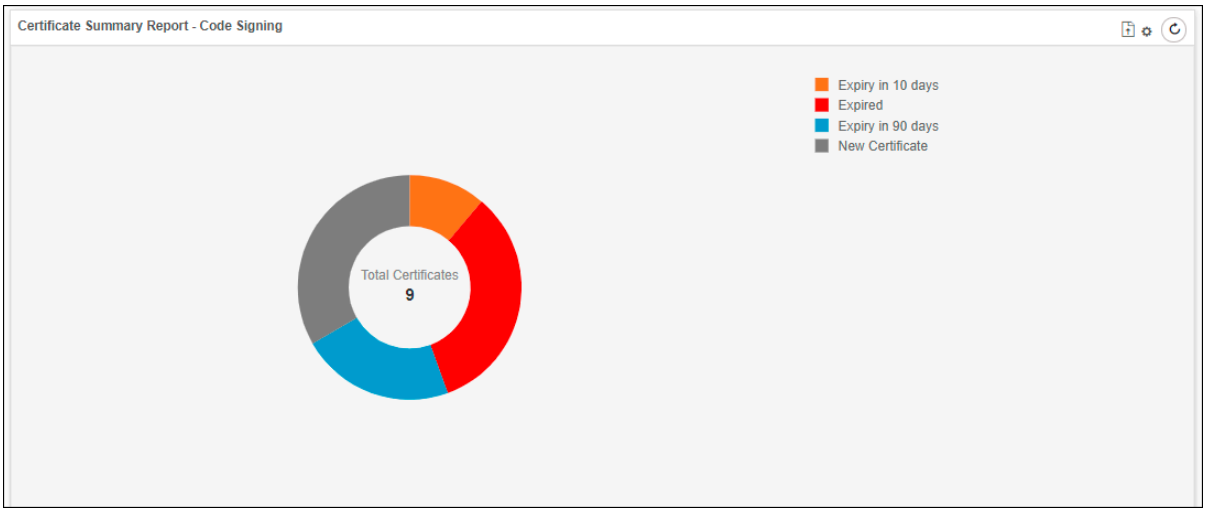
This report shows the count of code signing certificates that are either revoked or expired.



Count by Issuer - Code Signing

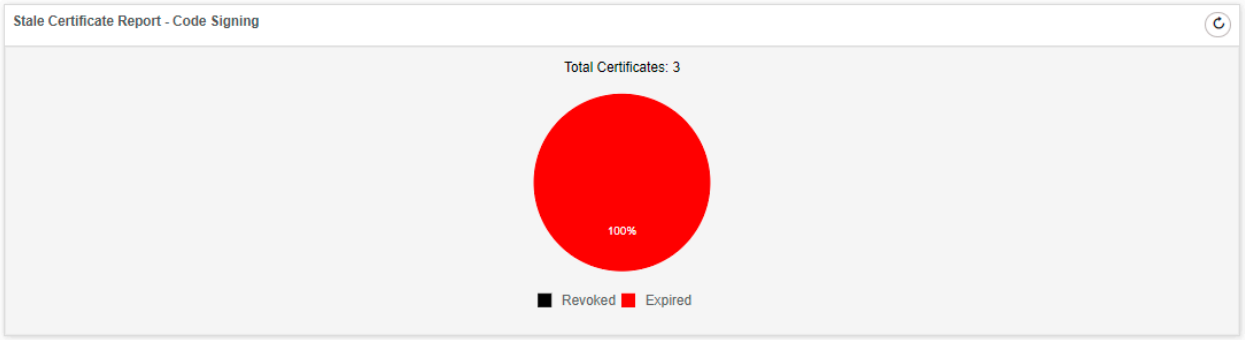
This report shows the count of client certificates with respect to the issuer details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Stale Certificate Report

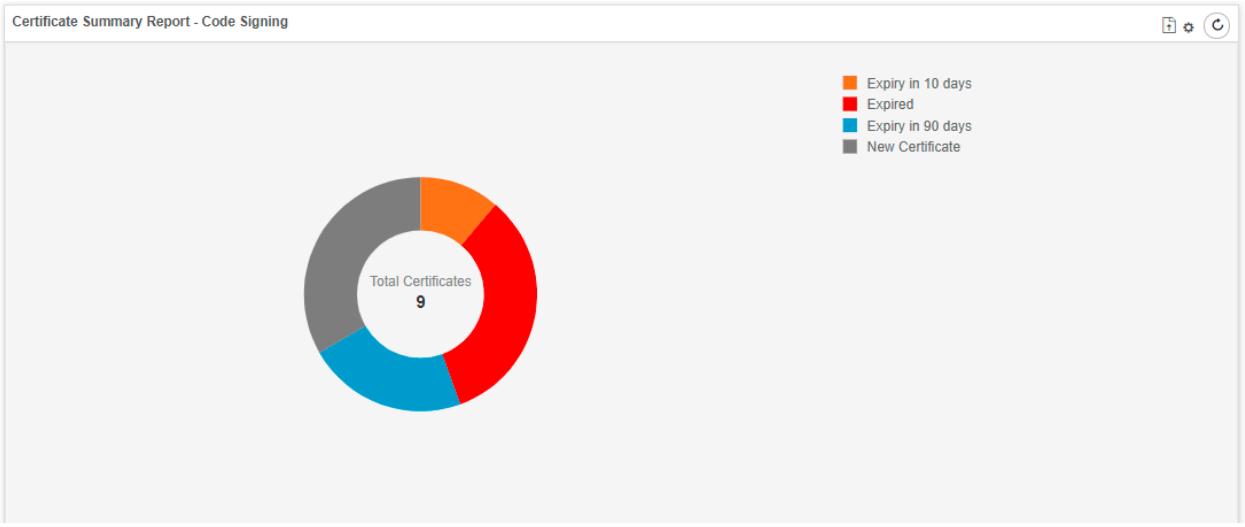
This report shows the count of code signing certificates that are either revoked or expired.



Count of issuer

This report shows the count of client certificates with respect to the issuer details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Server Certificate Security Dashboard

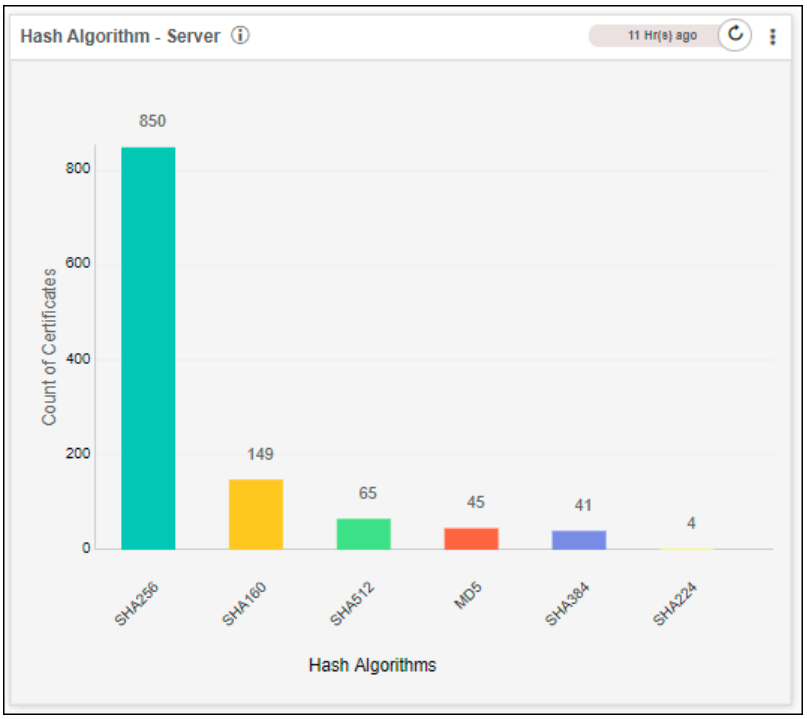
For the certificates in the Server inventory, this dashboard displays the following reports:

- Hash Algorithm - Server
- Key Algorithm - Server
- CAA Record – Server
- Certificate transparency – Server

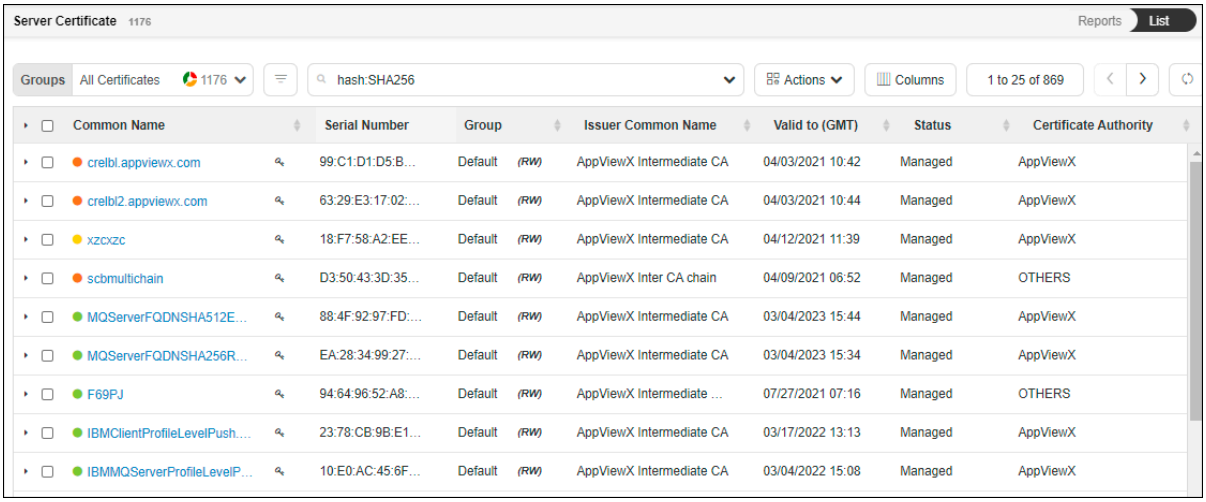
Hash Algorithm - Server

This report shows the count of certificates with respect to the hash algorithm available in the server inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



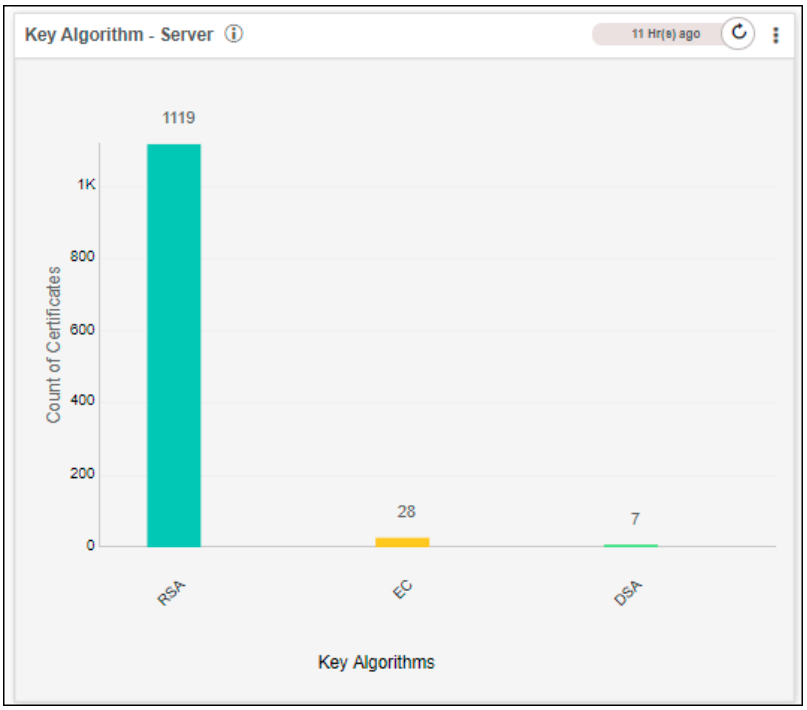
On clicking any bars of the report, the filtered data of certificates is displayed.



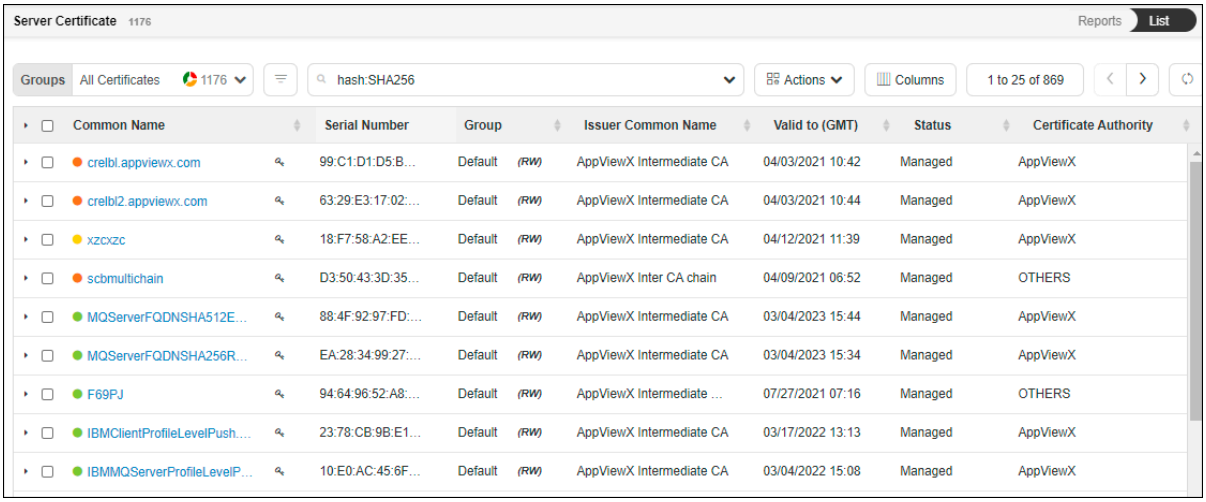
Key Algorithm - Server

This report shows the count of certificates with respect to the key algorithms available in the server inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



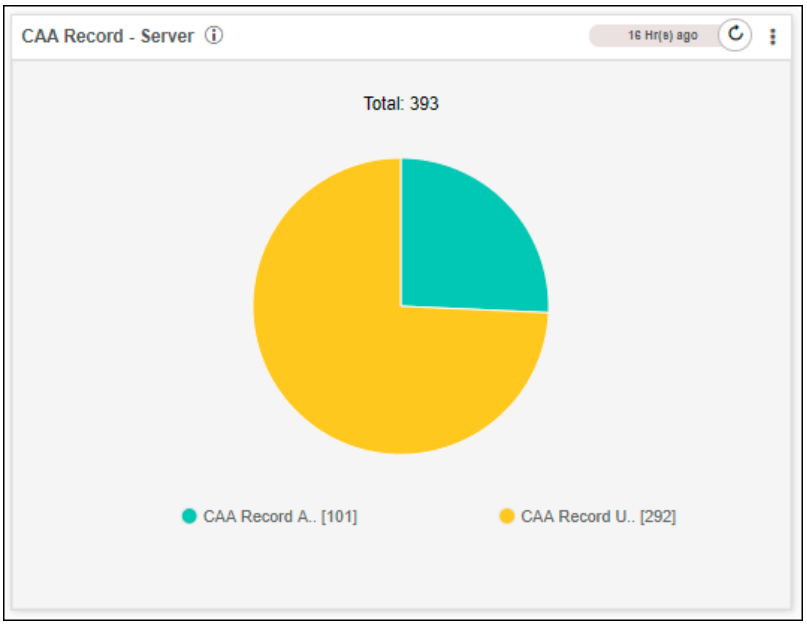
On clicking any bars of the report, the filtered data of certificates is displayed.



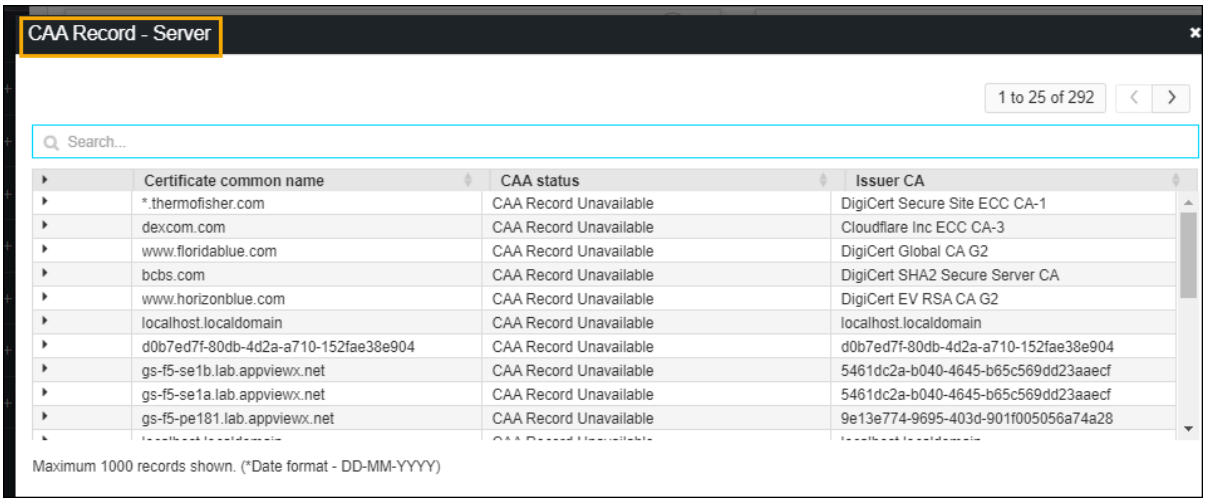
CAA Record - Server

This report shows the count of certificates with and without CAA records in the server inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



On clicking any parts of the report, the filtered data of certificates is displayed.



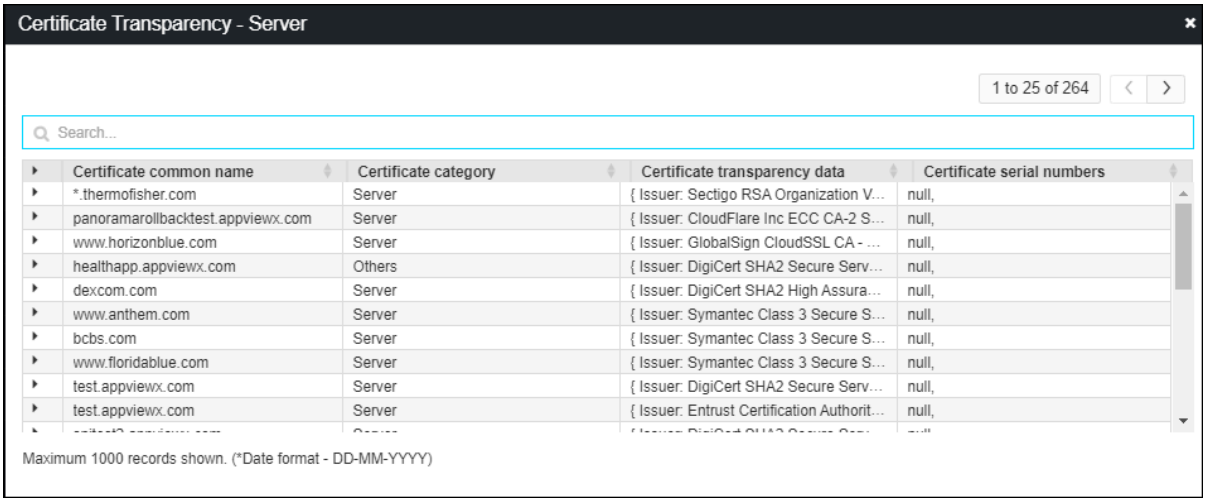
Certificate Transparency - Server

This report shows the count of application/FQDNs for which more certificates are available and only a few are managed/monitored in server certificate inventory. Currently the report is disabled.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

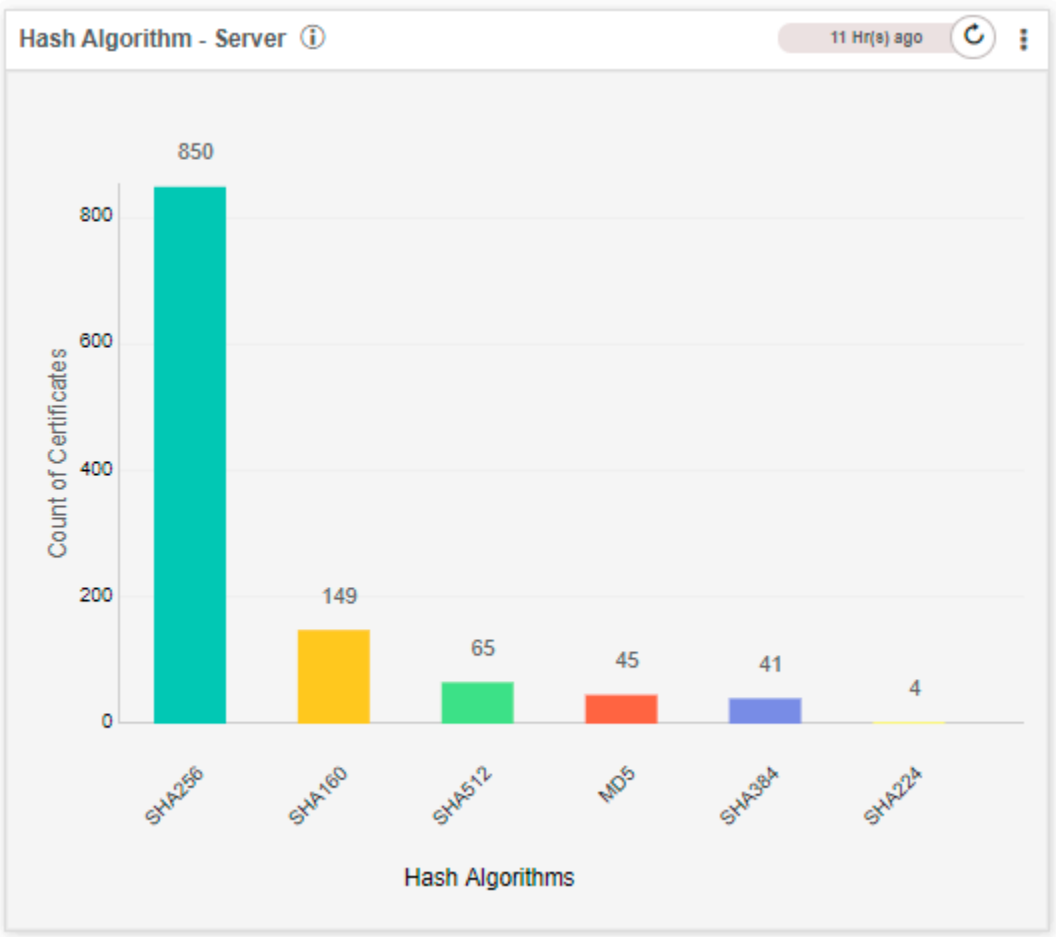
On clicking any parts of the report, the filtered data of certificates is displayed.



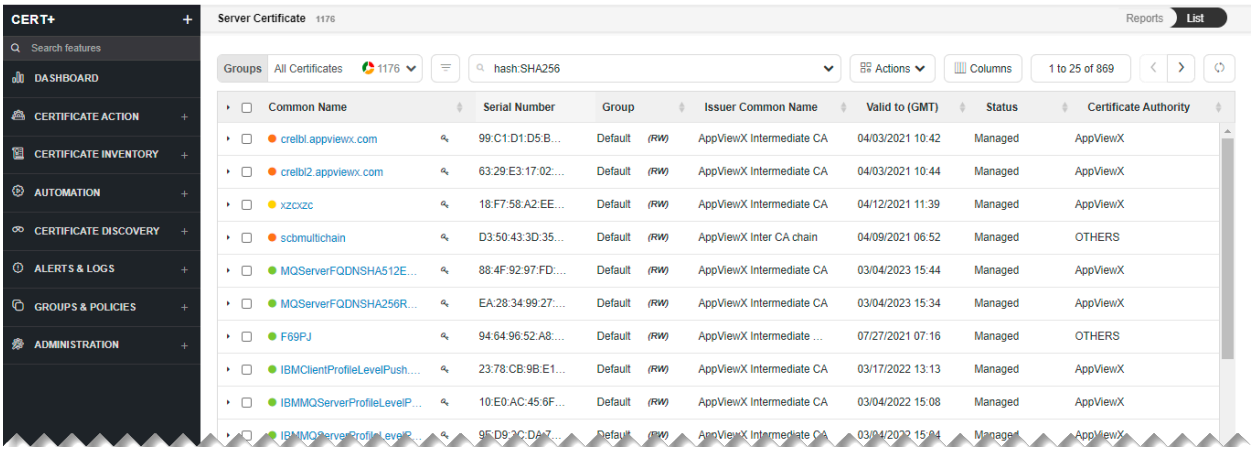
Hash Algorithm - Server

This report shows the count of certificates with respect to the hash algorithm available in the server inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



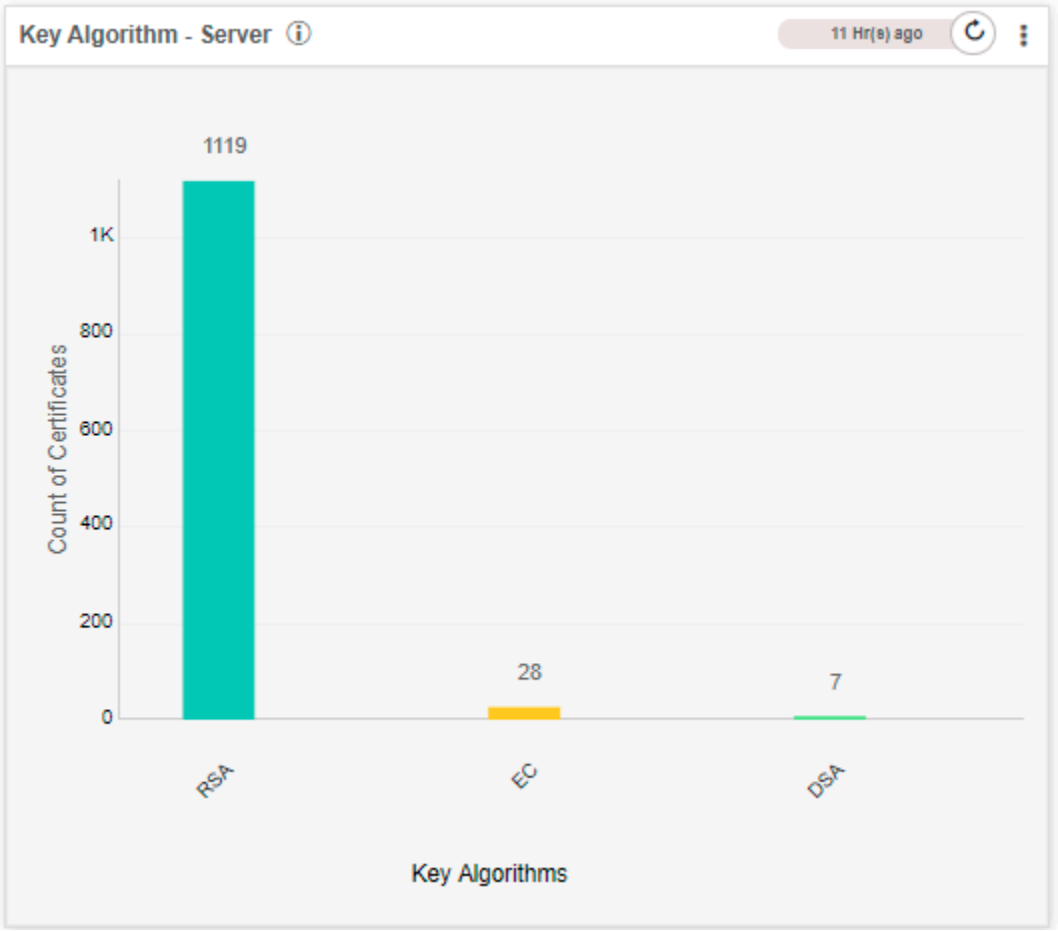
On click of the report, the filtered data of certificates will be shown as below:



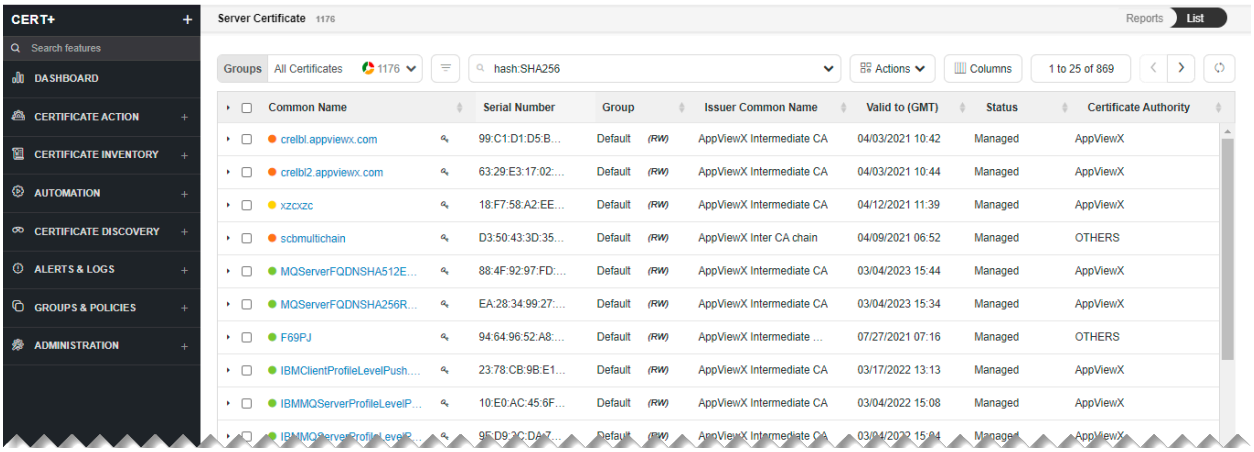
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Key Algorithm - Server

This report shows the count of certificates with respect to the key algorithms available in the server inventory.



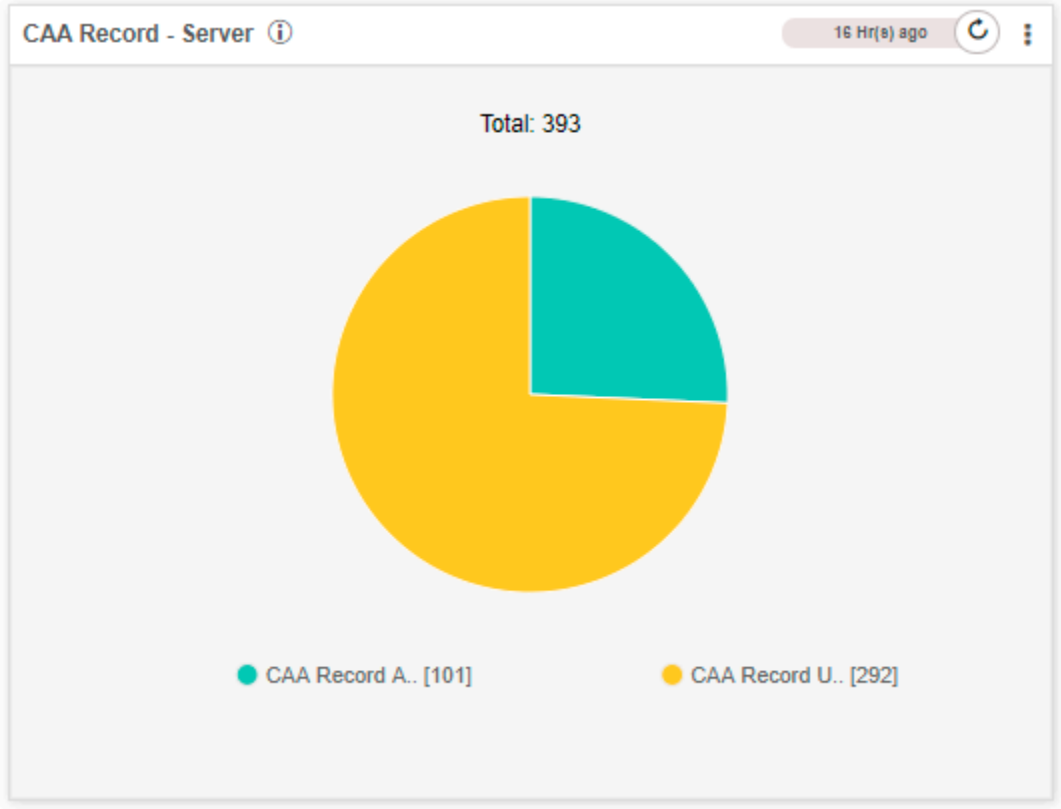
On click of the report, the filtered data of certificates will be shown as below:



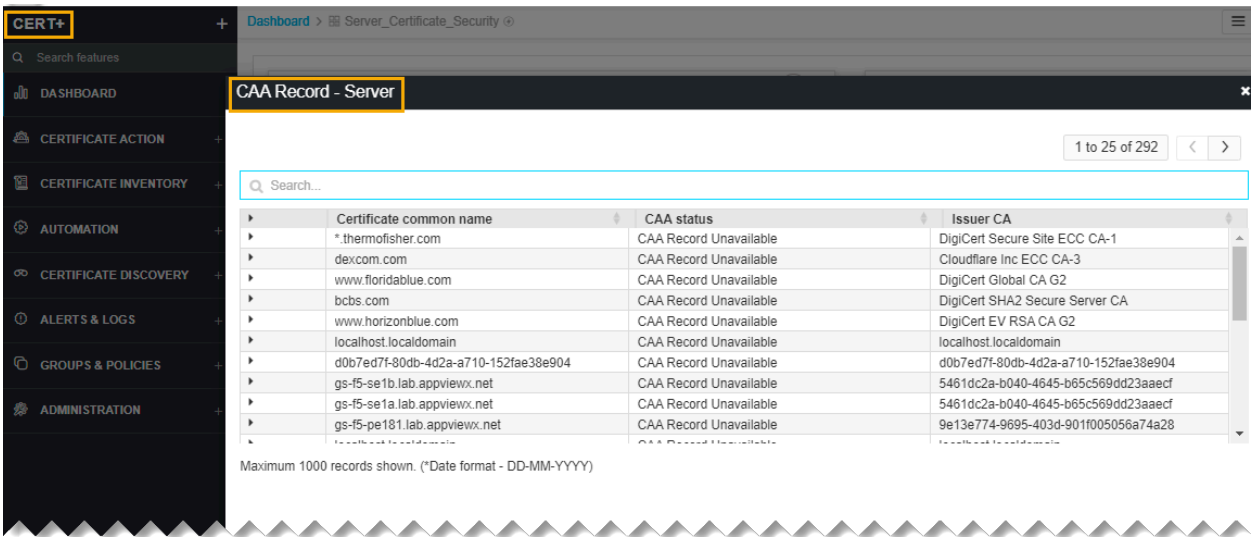
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CAA Record – Server

This report shows the count of certificates with and without CAA records in the server inventory.



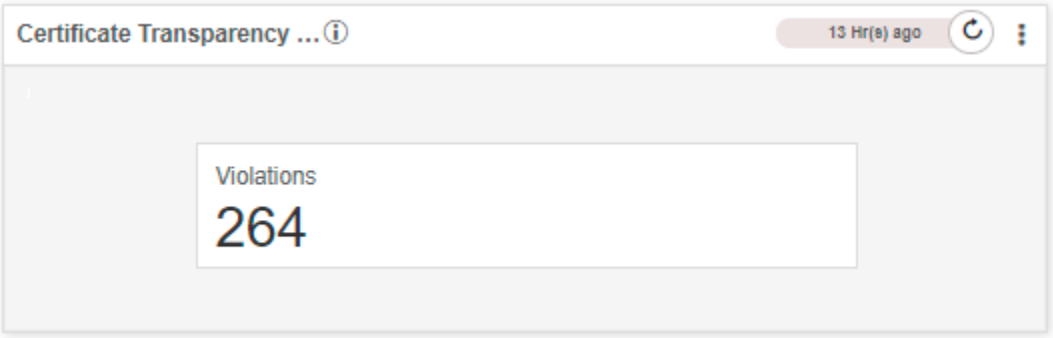
On click of the report, the filtered data of certificates will be shown as below:



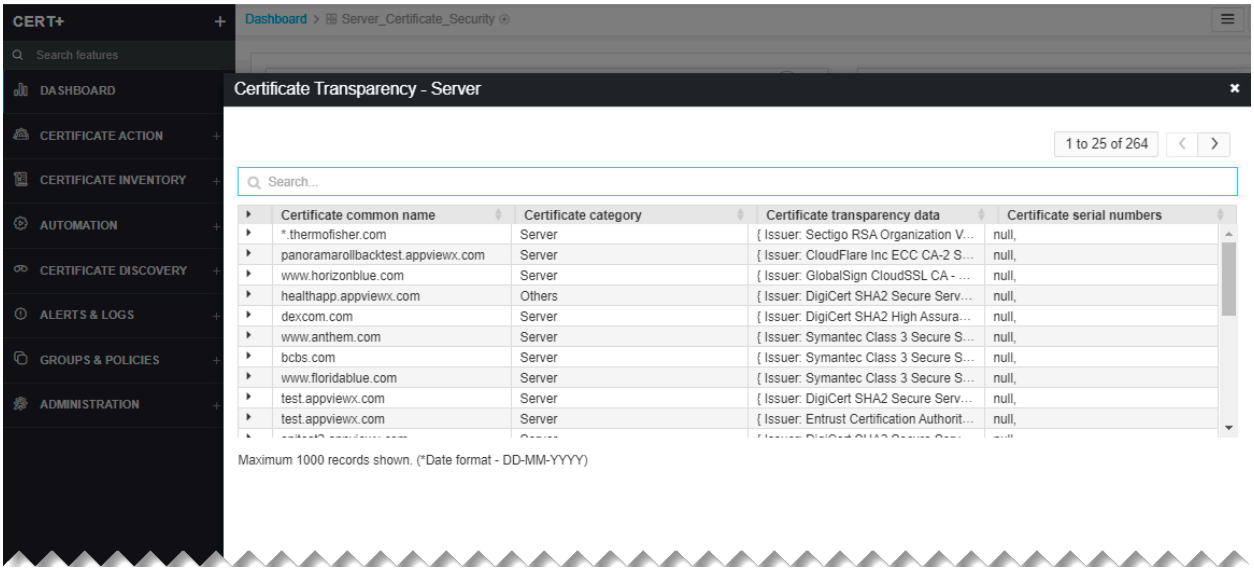
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate transparency – Server

This report shows the count of application/FQDNs for which more certificates are available and only a few are managed/monitored in server certificate inventory. Currently the report is disabled.



On click of the report, the filtered data of certificates will be shown as below:



Understanding the Client Certificate Security Dashboard

For the certificates in the Client inventory, this dashboard will be shown as the reports:

- Hash Algorithm - Client
- Key Algorithm - Client

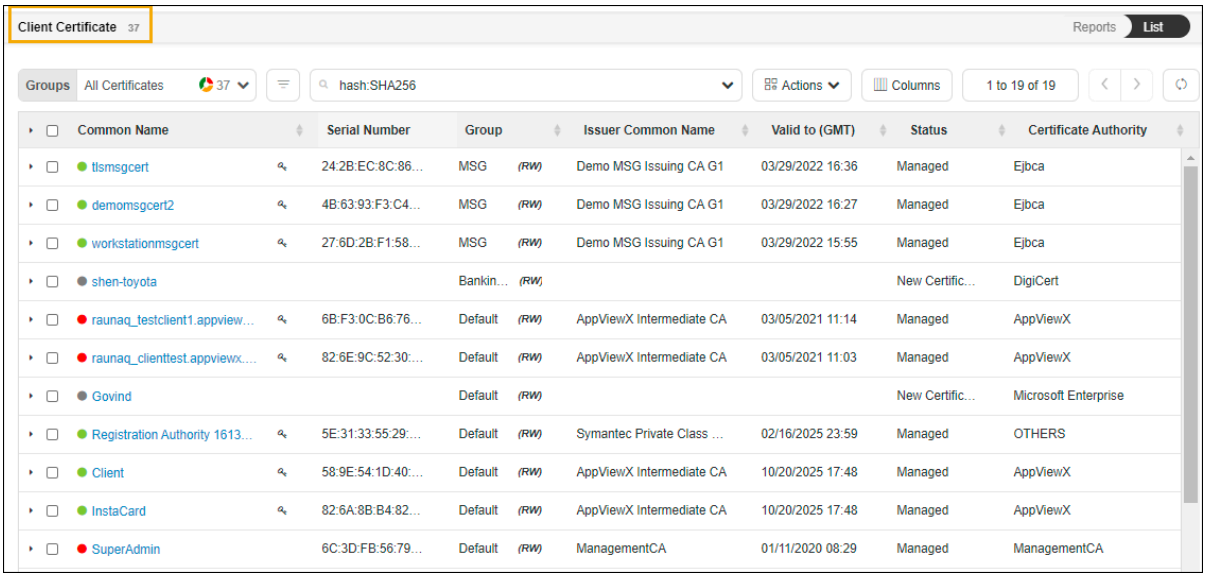
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Hash Algorithm - Client

This report shows the count of certificates with respect to the hash algorithm available in the Client inventory.



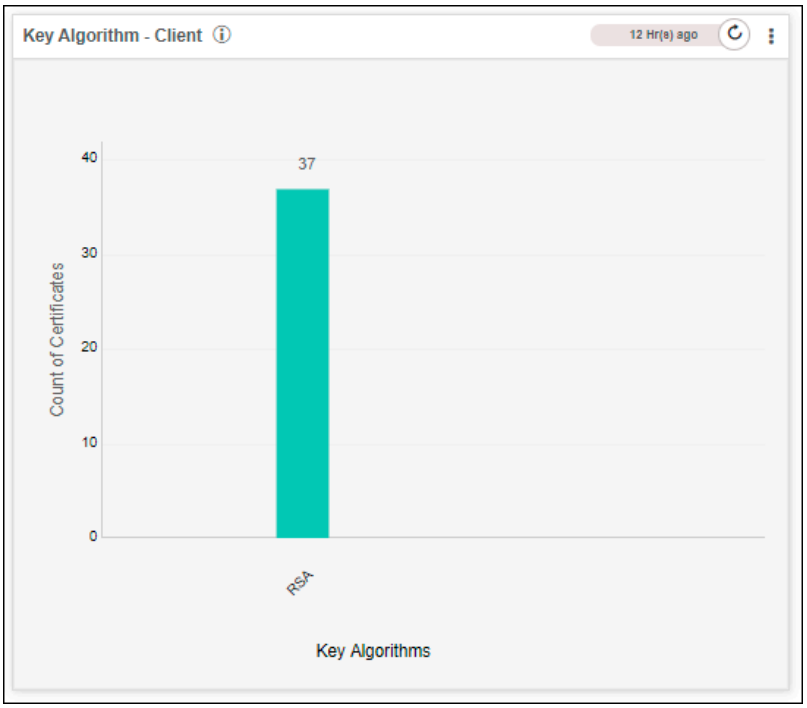
On clicking any bars of the report, the filtered data of certificates is displayed.



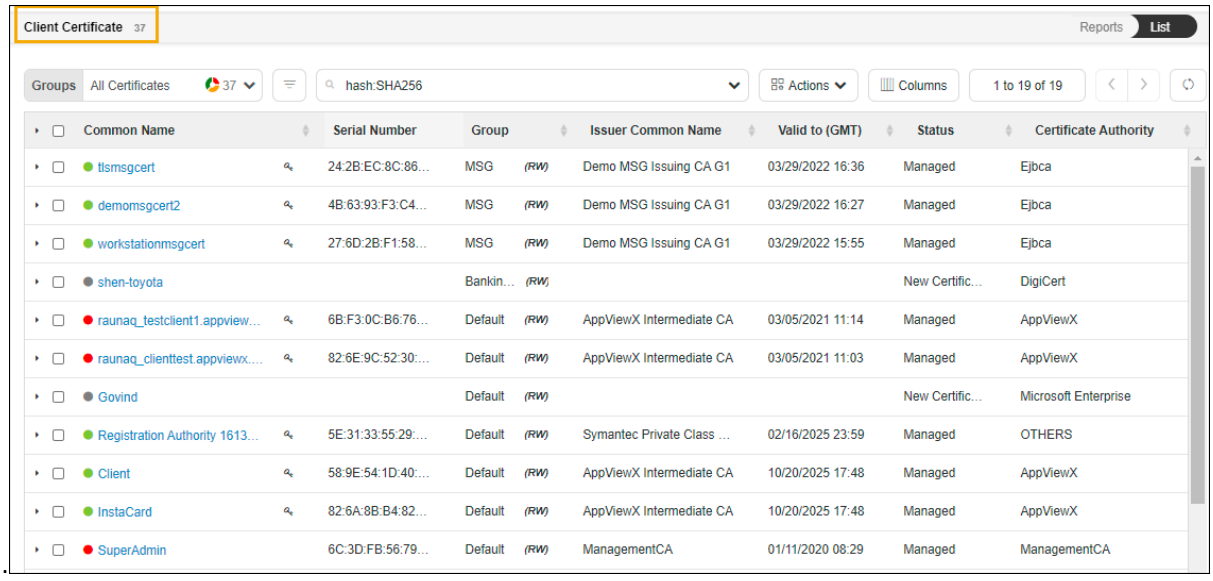
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Key Algorithm - Client

This report shows the count of certificates with respect to the key algorithms available in the Client inventory.



On clicking any bars of the report, the filtered data of certificates is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

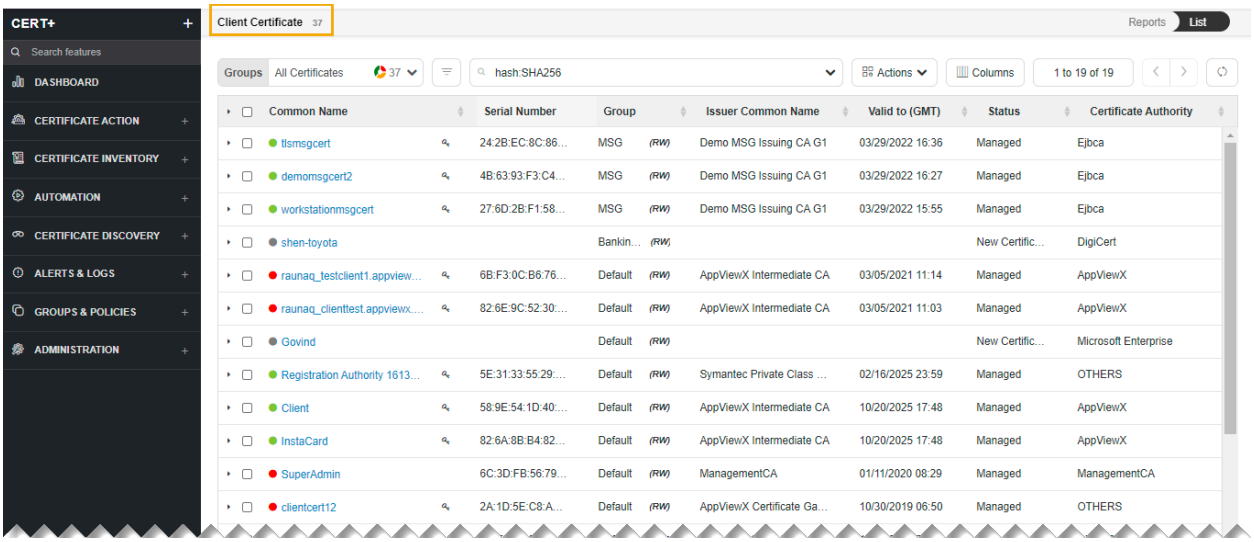
Hash Algorithm - Client

This report shows the count of certificates with respect to the hash algorithm available in the Client inventory.



On click of anywhere in the report, the filtered data of certificates will be shown as below:

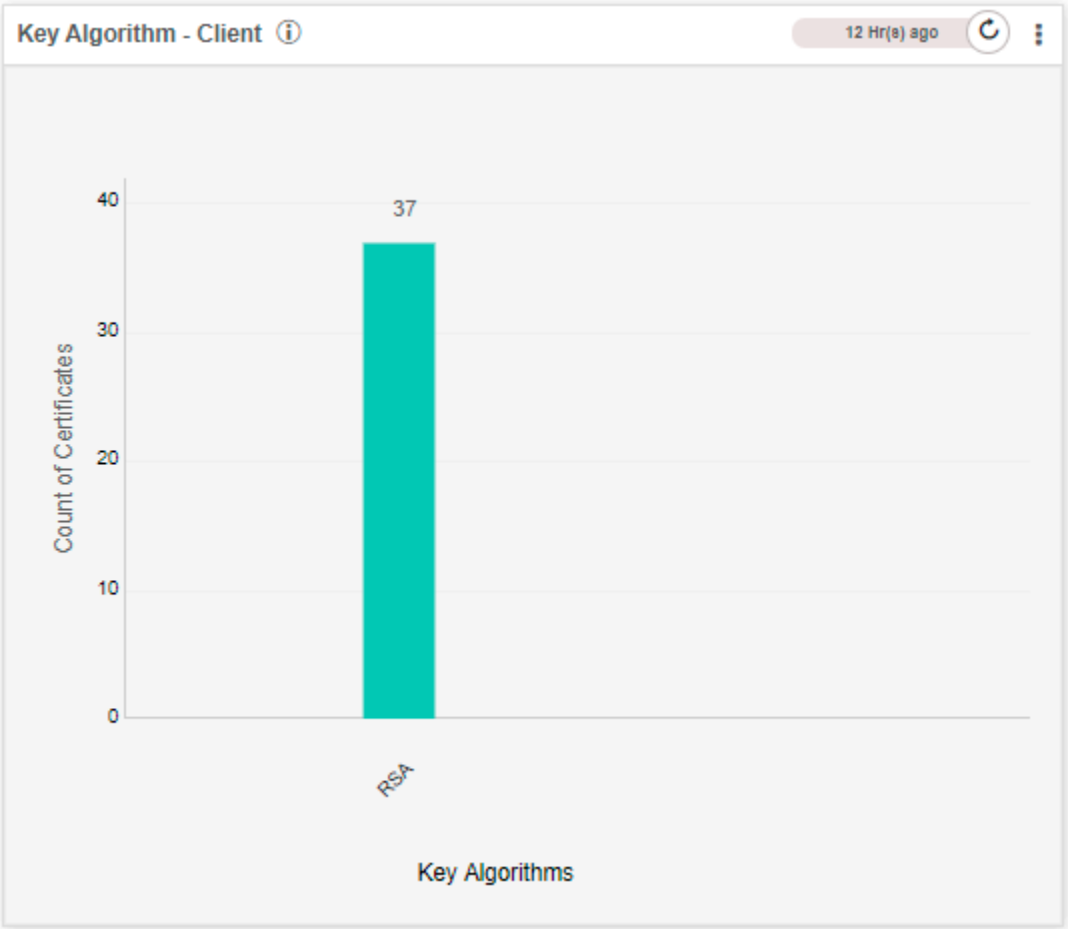
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Key Algorithm - Client

This report shows the count of certificates with respect to the key algorithms available in the Client inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



On click of anywhere in the report, the filtered data of certificates show the details.

Understanding the Server Endpoint Security Dashboard

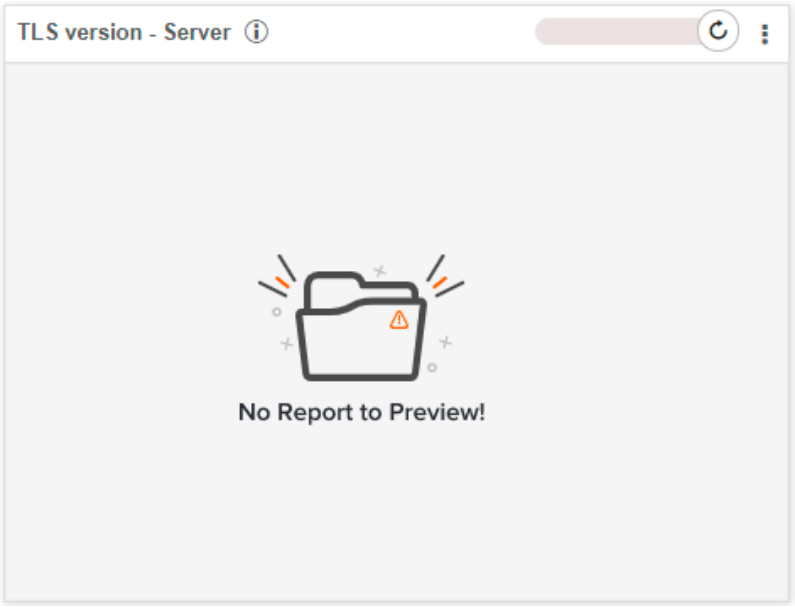
For the certificates in the Server inventory which are associated with the endpoints, from a security perspective, the following reports are available:

- TLS version - Server
- Cipher suites - Server
- Heartbleed & Poodle report - Server
- Certificate Monitor Statuses - Server
- Certificate Auto Push - Server

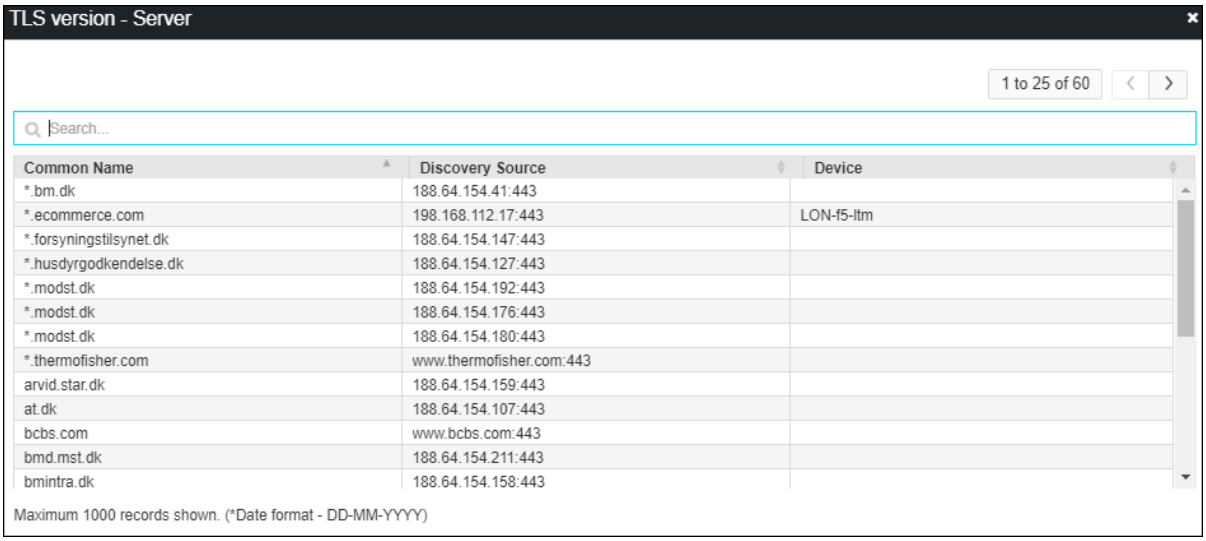
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

TLS Version - Server

This report shows the count of certificates with respect to the TLS versions available in the server inventory.



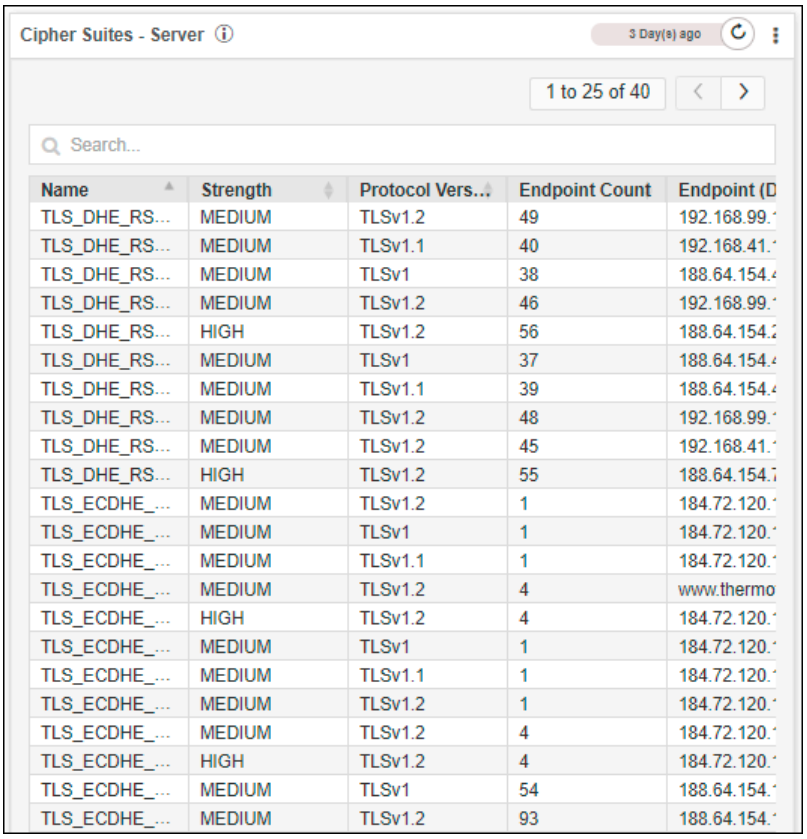
Clicking the **Endpoint Count** value in the report displays the respective data of certificates.



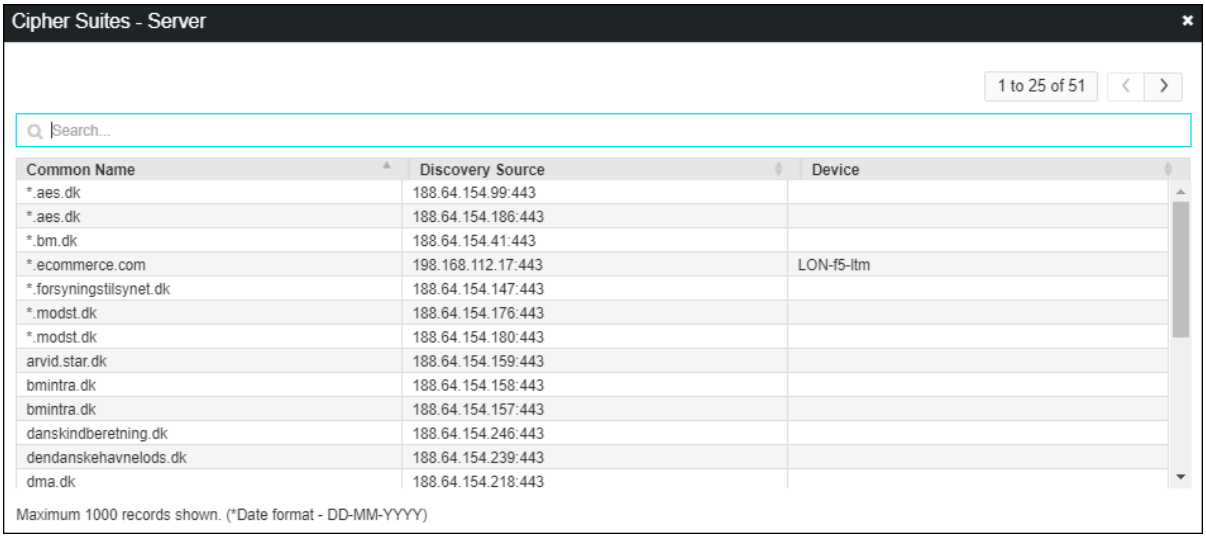
Cipher Suites - Server

This report shows the count of certificates with respect to the cipher suite details and the TLS versions. The cipher suites are shown based on the priority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



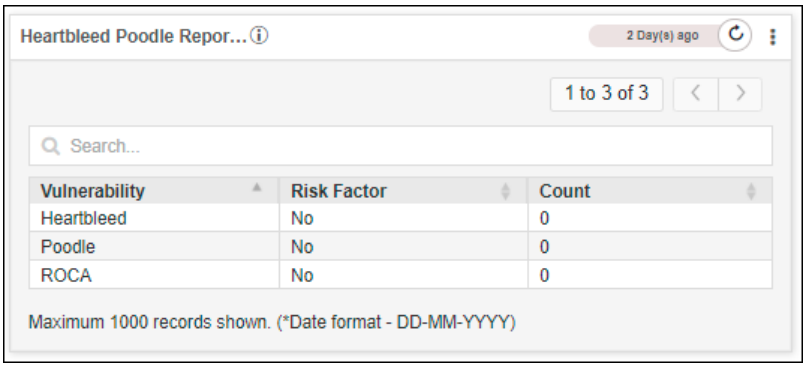
Clicking on the **Endpoint Count** value in the report displays the respective data of certificates.



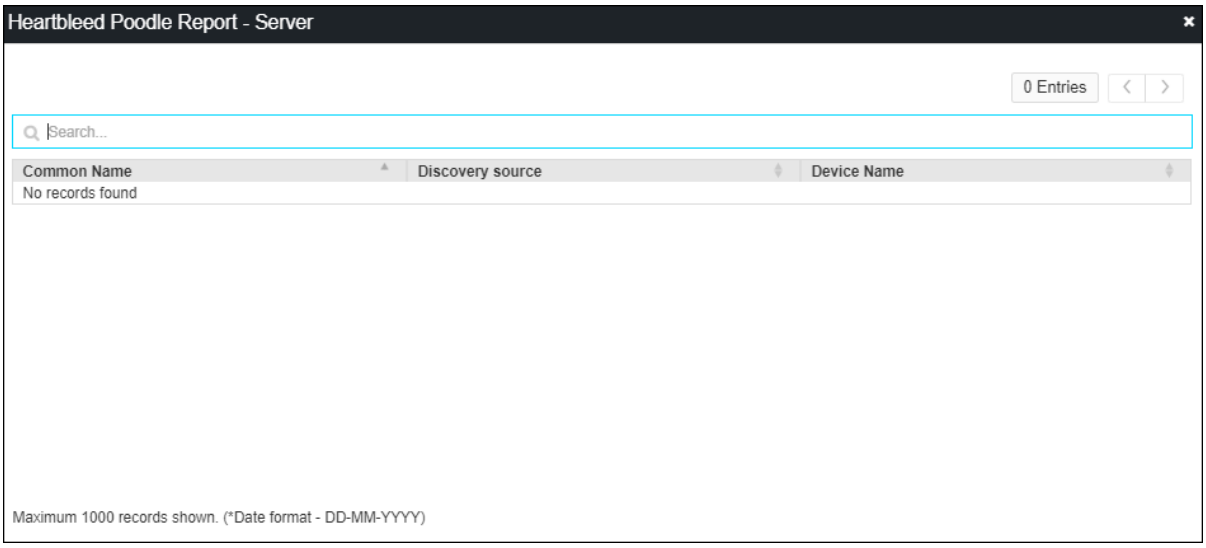
Heartbleed & Poodle Report - Server

This report shows the count of device endpoints are exposed to Heartbleed, Poodle, and ROCA vulnerabilities.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



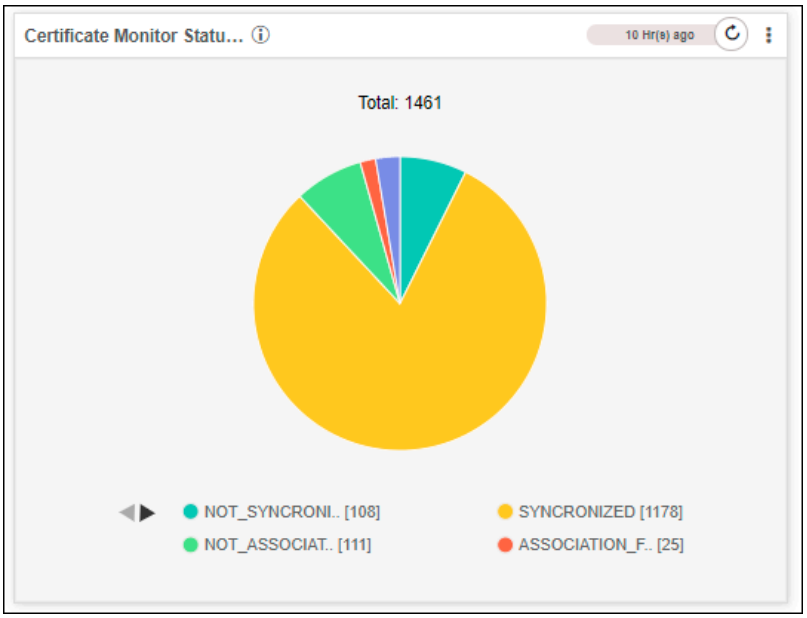
Click on the **Count** value in the report displays the respective data of certificates.



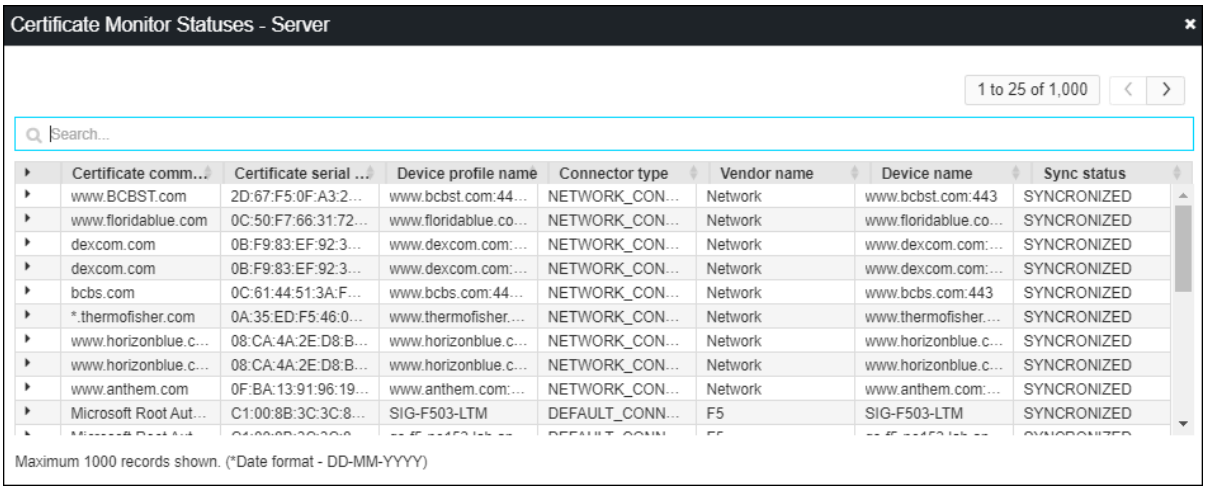
Certificate Monitor Statuses - Server

This report shows the count of domain names for which more certificates are available and only a few are managed/monitored in the Client certificate inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



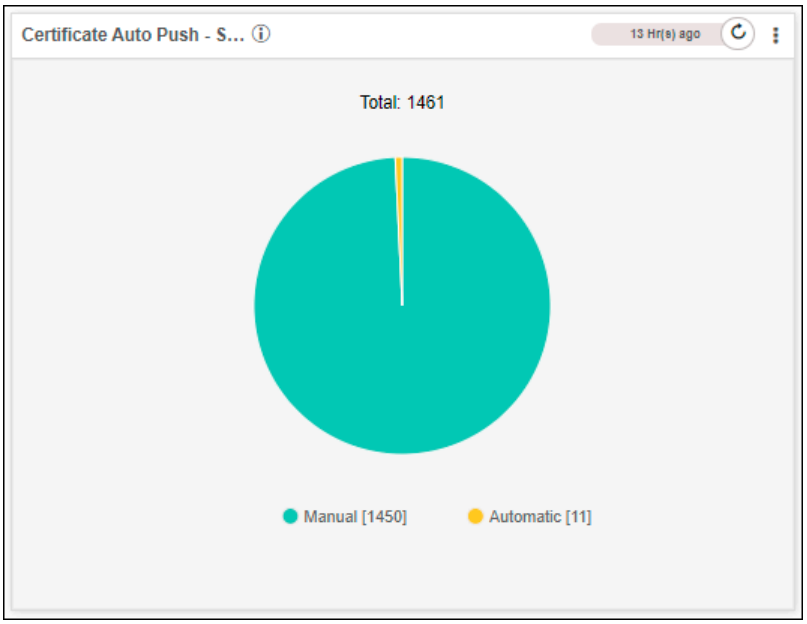
Clicking on any sections of the pie chart displays the respective data of certificates.



Certificate Auto Push - Server

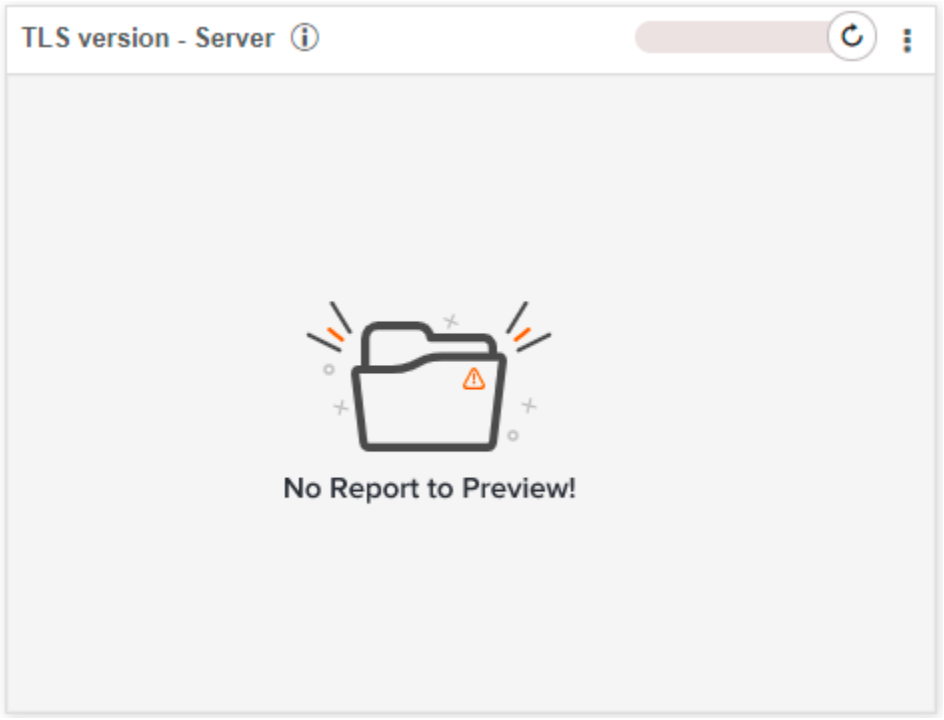
This report shows the count of certificates in the Server inventory which are enabled and not enabled with auto push feature.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



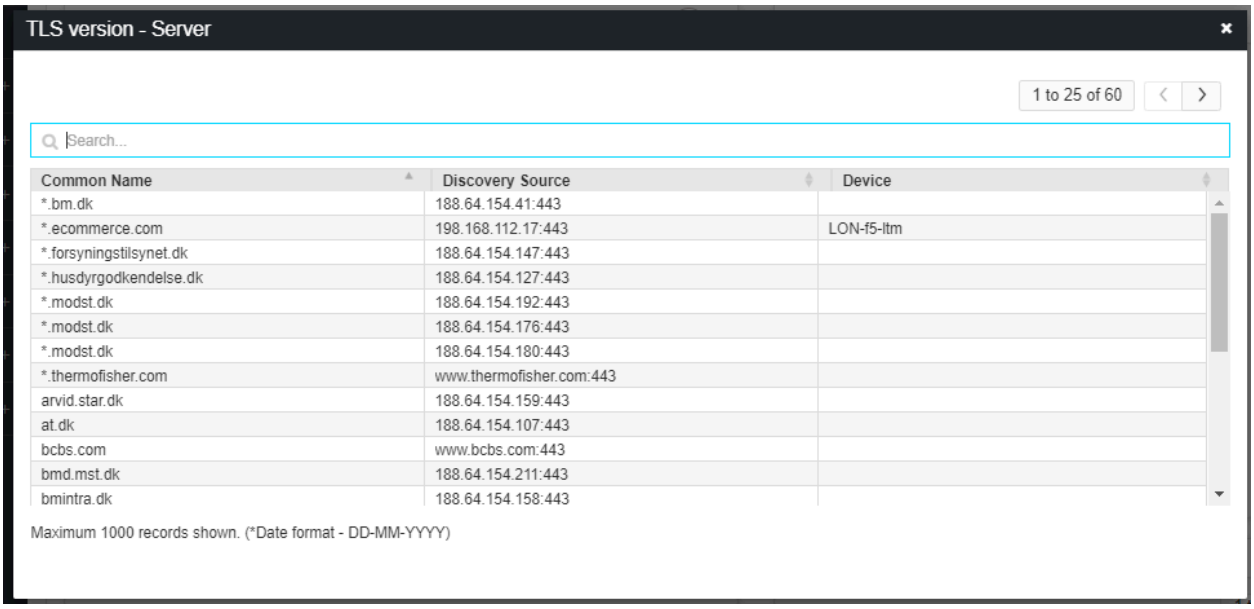
TLS version - Server

This report shows the count of certificates with respect to the TLS versions available in the server inventory.



On click of the Endpoint Count value in the report, the respective data of certificates will be shown as below:

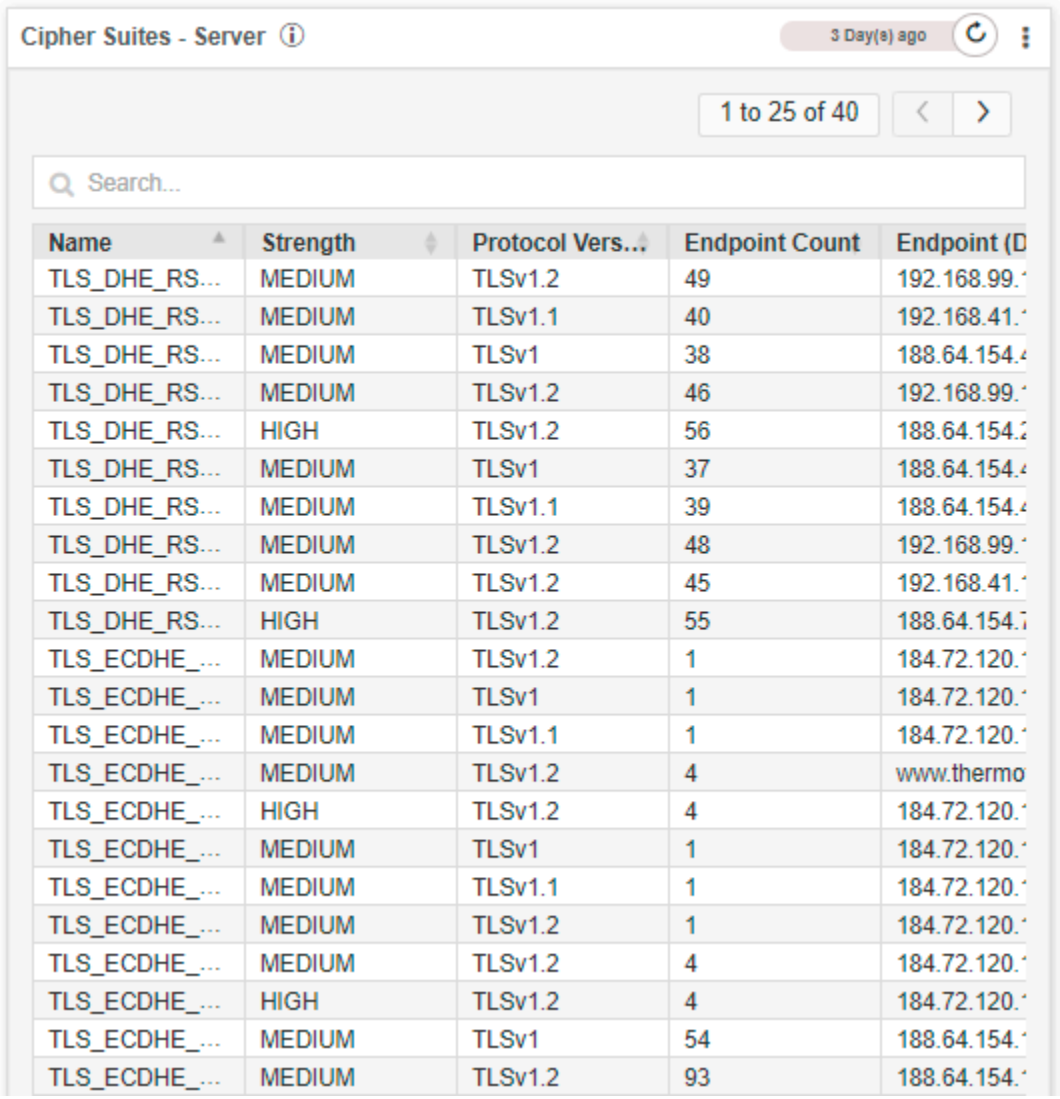
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Cipher suites - Server

This report shows the count of certificates with respect to the cipher suite details and the TLS versions. The cipher suites are shown based on the priority.

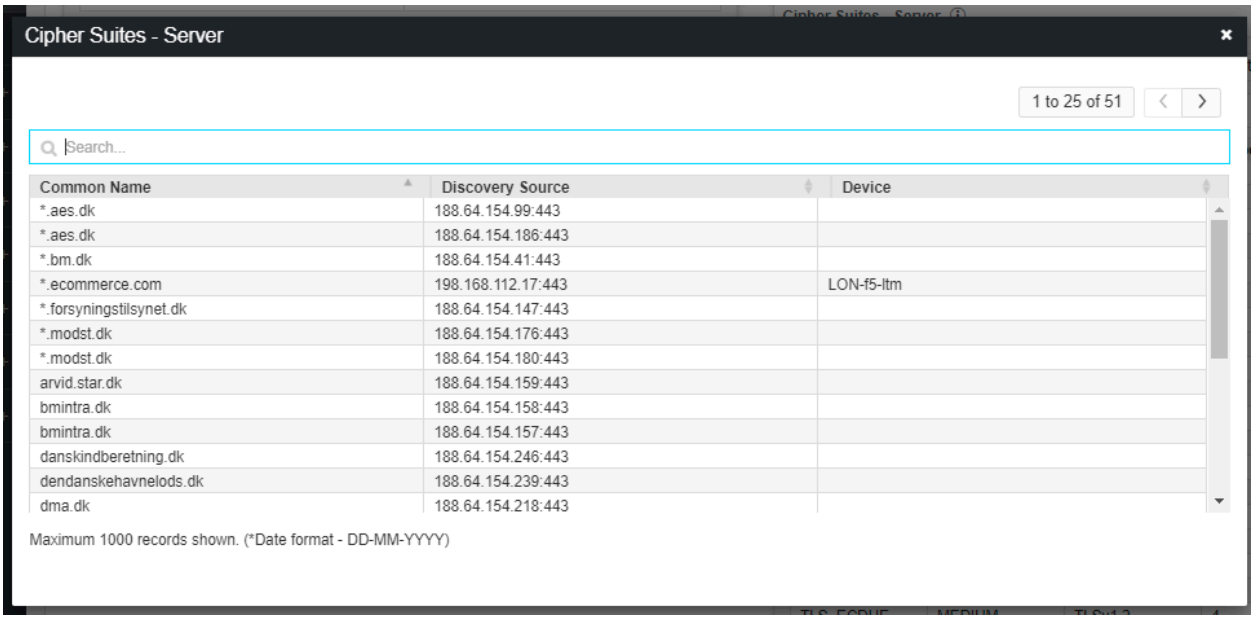
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Name	Strength	Protocol Vers...	Endpoint Count	Endpoint (D
TLS_DHE_RS...	MEDIUM	TLSv1.2	49	192.168.99.
TLS_DHE_RS...	MEDIUM	TLSv1.1	40	192.168.41.
TLS_DHE_RS...	MEDIUM	TLSv1	38	188.64.154.
TLS_DHE_RS...	MEDIUM	TLSv1.2	46	192.168.99.
TLS_DHE_RS...	HIGH	TLSv1.2	56	188.64.154.
TLS_DHE_RS...	MEDIUM	TLSv1	37	188.64.154.
TLS_DHE_RS...	MEDIUM	TLSv1.1	39	188.64.154.
TLS_DHE_RS...	MEDIUM	TLSv1.2	48	192.168.99.
TLS_DHE_RS...	MEDIUM	TLSv1.2	45	192.168.41.
TLS_DHE_RS...	HIGH	TLSv1.2	55	188.64.154.
TLS_ECDHE_...	MEDIUM	TLSv1.2	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1.1	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1.2	4	www.thermo
TLS_ECDHE_...	HIGH	TLSv1.2	4	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1.1	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1.2	1	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1.2	4	184.72.120.
TLS_ECDHE_...	HIGH	TLSv1.2	4	184.72.120.
TLS_ECDHE_...	MEDIUM	TLSv1	54	188.64.154.
TLS_ECDHE_...	MEDIUM	TLSv1.2	93	188.64.154.

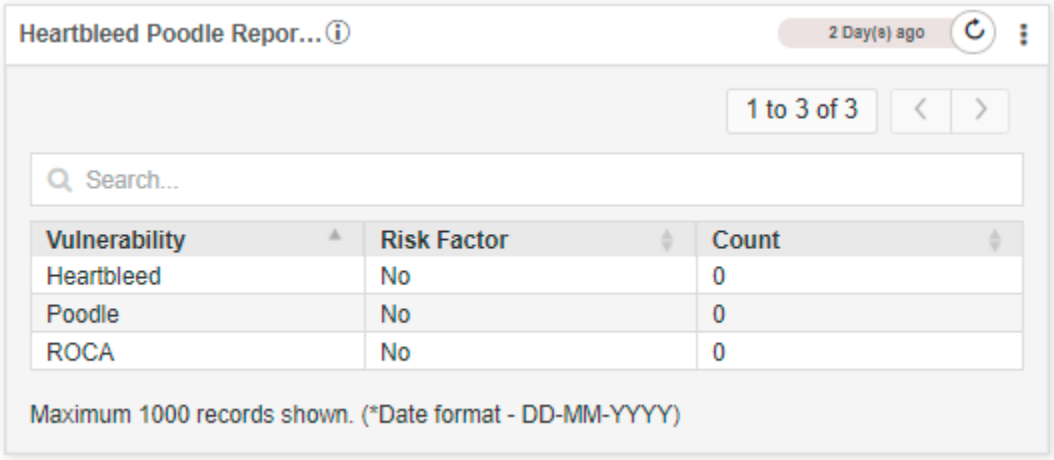
On click of the Endpoint count value in the report, the respective data of certificates will be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



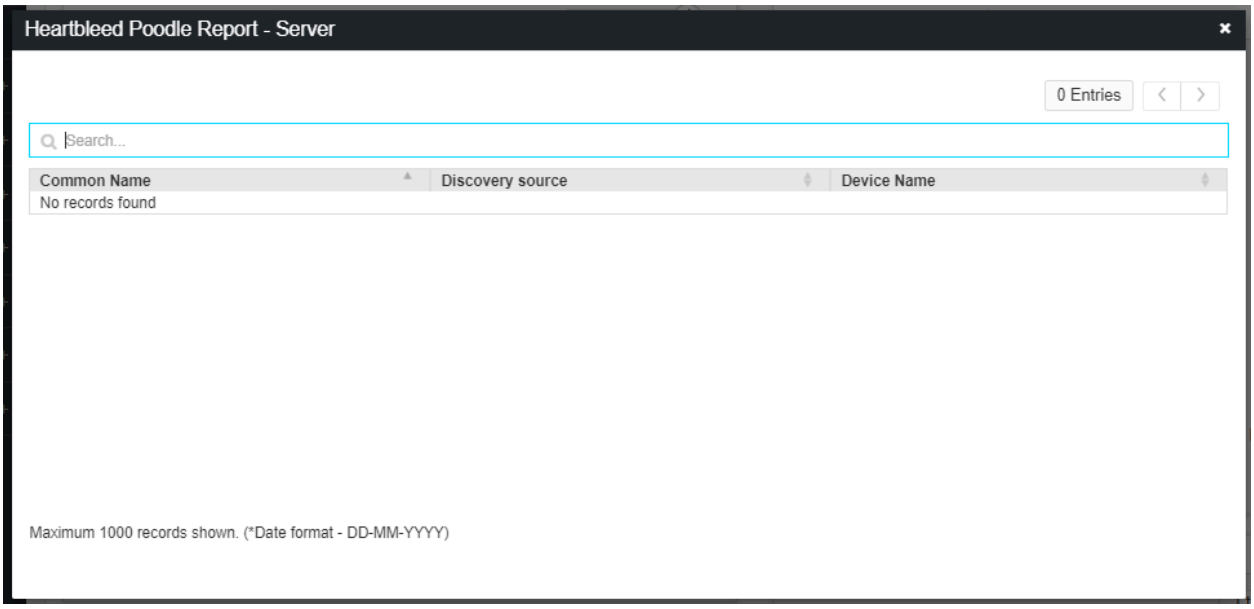
Heartbleed & Poodle report - Server

This report shows the count of device endpoints are exposed to Heartbleed, Poodle, and ROCA vulnerabilities.



On click of the Count value in the report, the respective data of certificates will be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

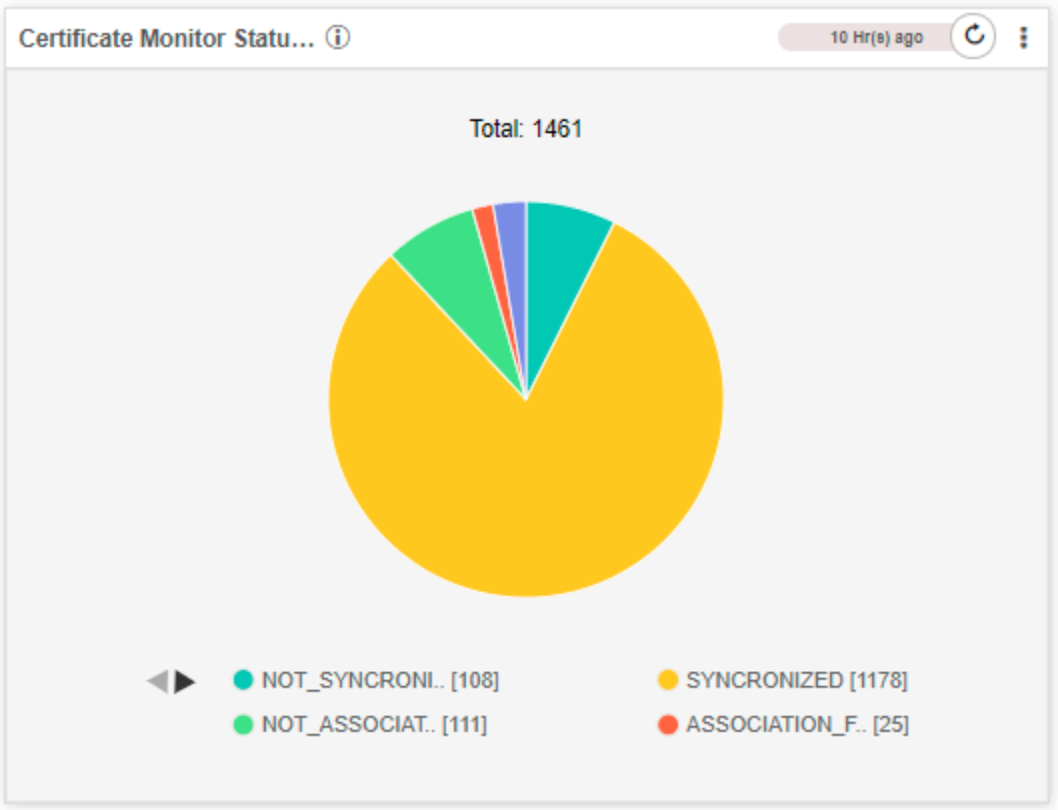


Note: Since there are no vulnerable data available in the product, this report is shown as No records found.

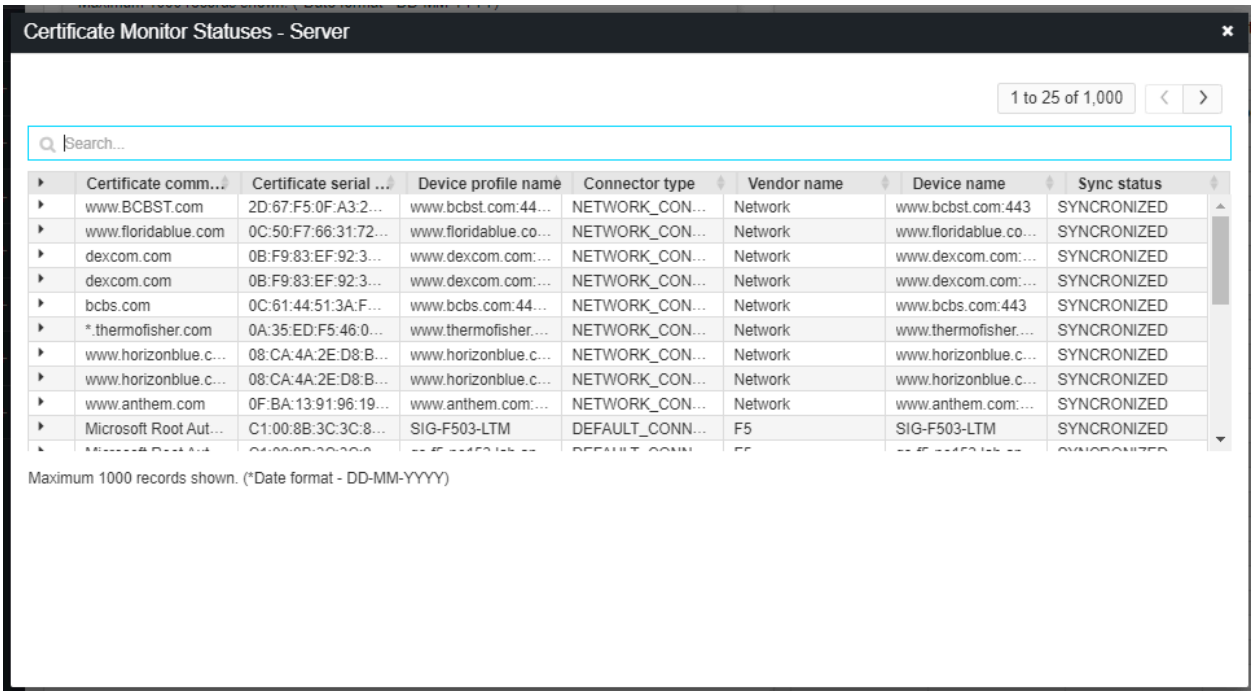
Certificate Monitor Statuses - Server

This report shows the count of domain names for which more certificates are available and only a few are managed/monitored in the Client certificate inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



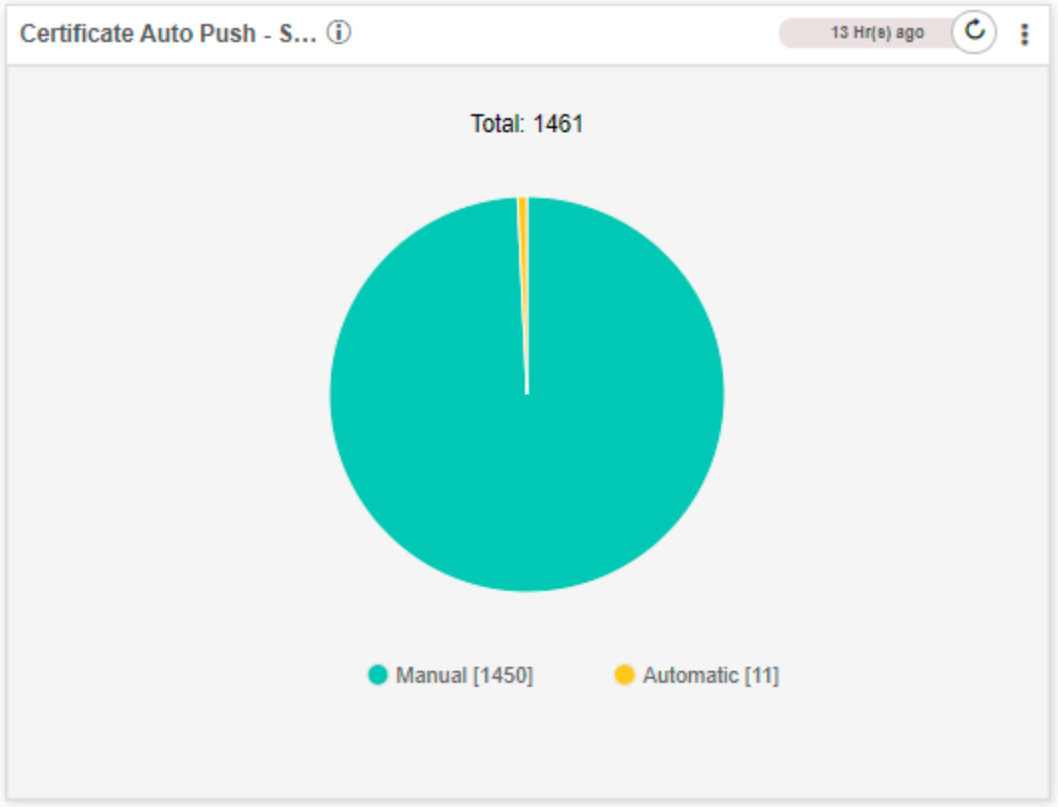
On click of the chart in the report, the respective data of certificates will be shown as below:



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Auto Push - Server

This report shows the count of certificates in the Server inventory which are enabled and not enabled with auto push feature.



If you click on the chart, the respective details will be shown.

Understanding the Client Endpoint Security Dashboard

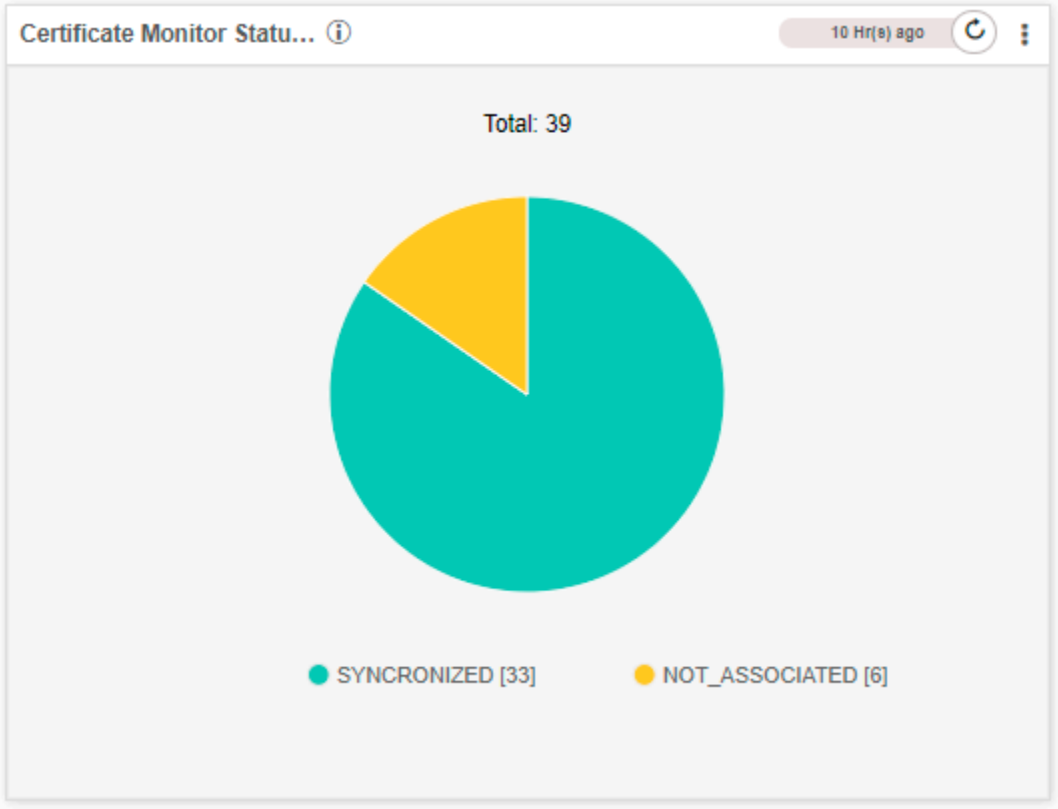
For the certificates in the Server inventory which are associated with the endpoints, from the security perspective, the following are the reports available:

- Certificate Monitor Statuses - Client
- Certificate Auto Push - Client
- Shared Client Report

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

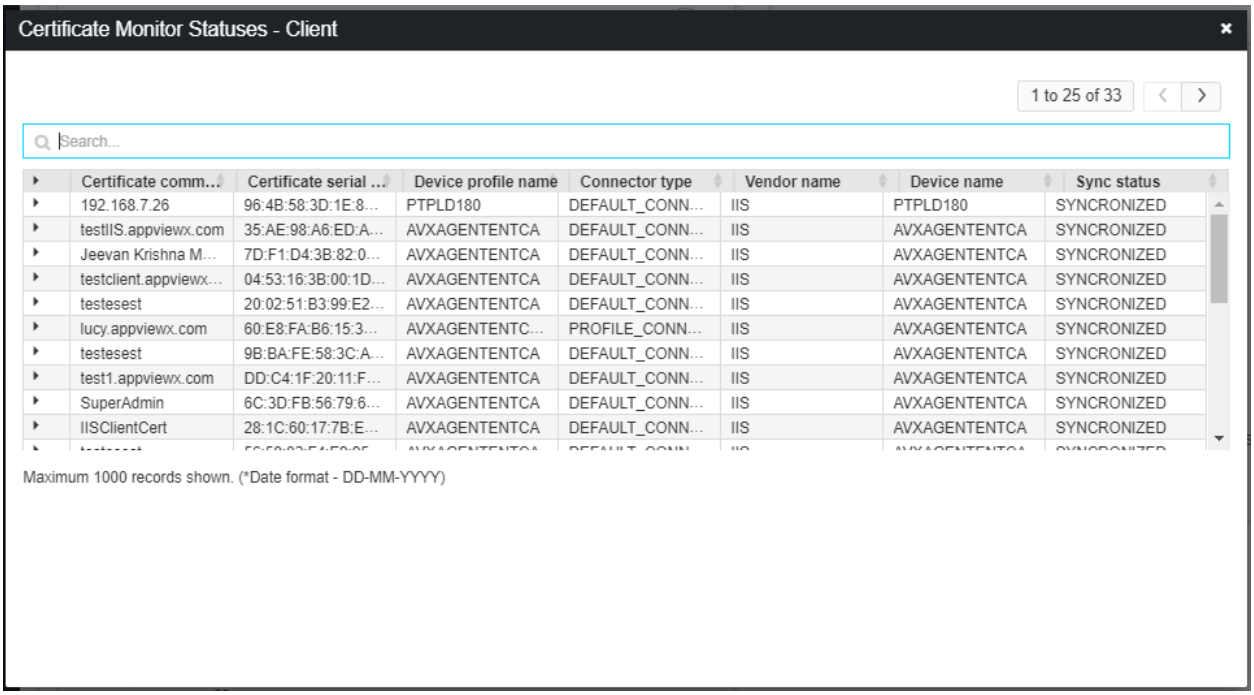
Certificate Monitor Statuses - Client

This report shows the count of endpoints with respect to their certificate monitor statuses available in the client inventory.



On click of this chart, the respective filtered data of certificates be shown as below:

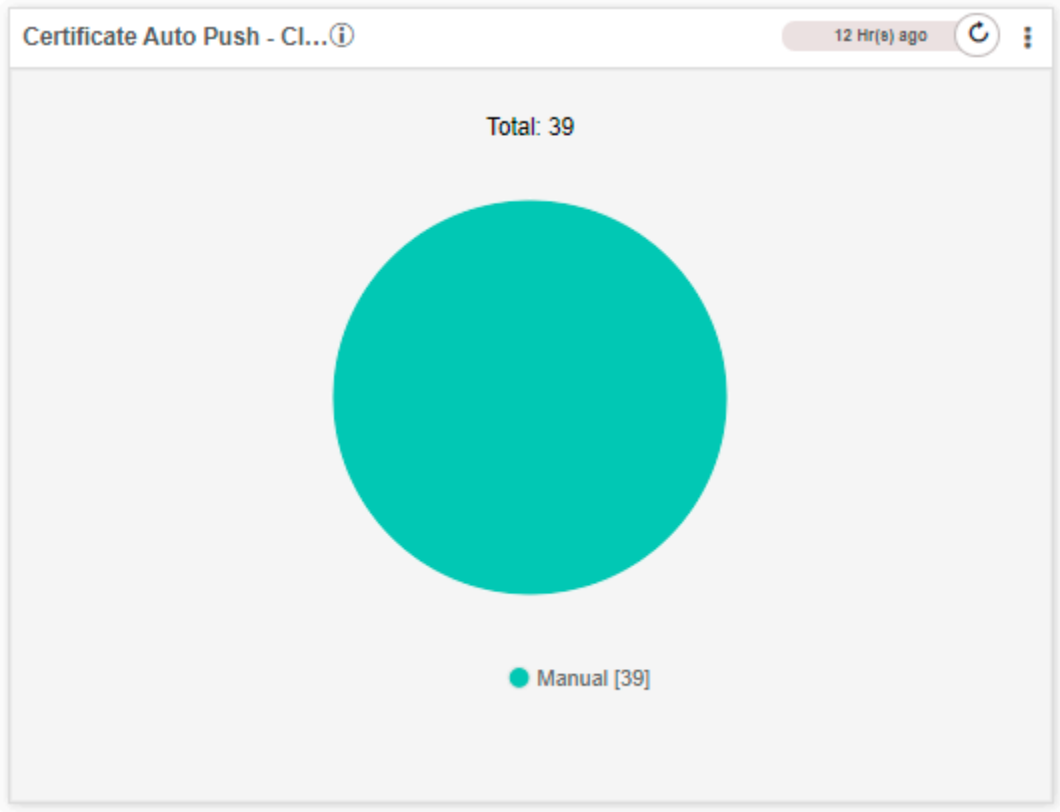
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



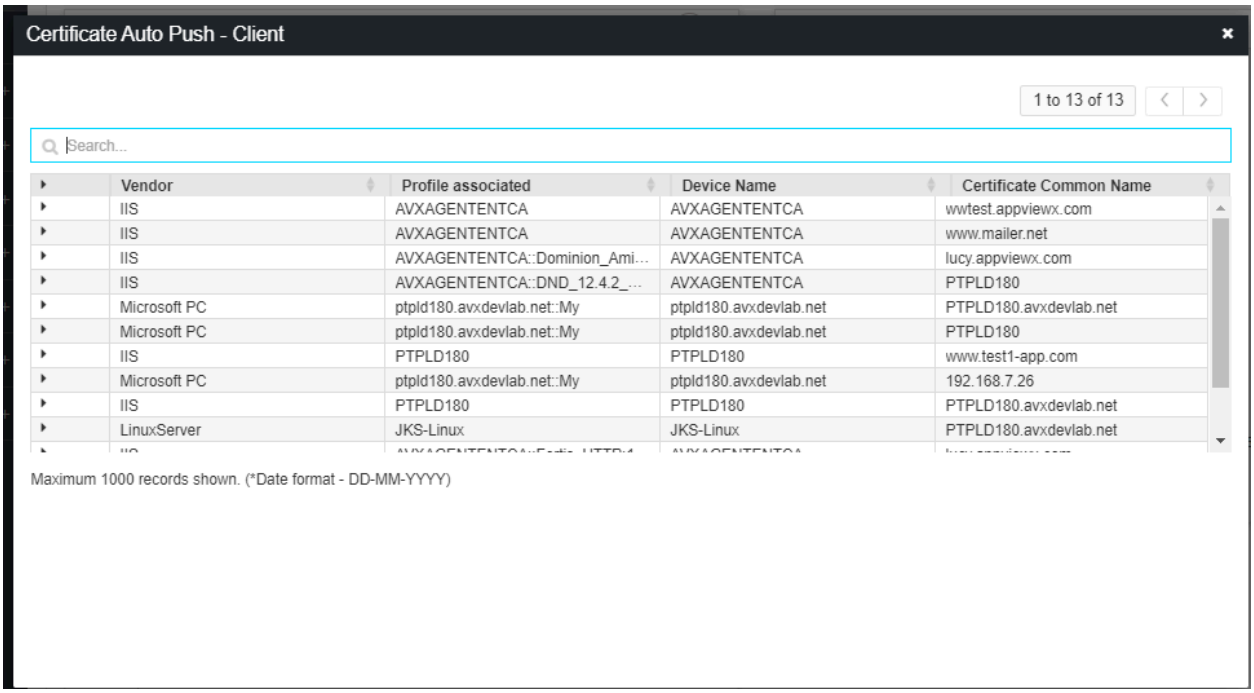
Certificate Auto Push - Client

This report shows the count of certificates in the client inventory which are enabled and not enabled with auto push feature.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



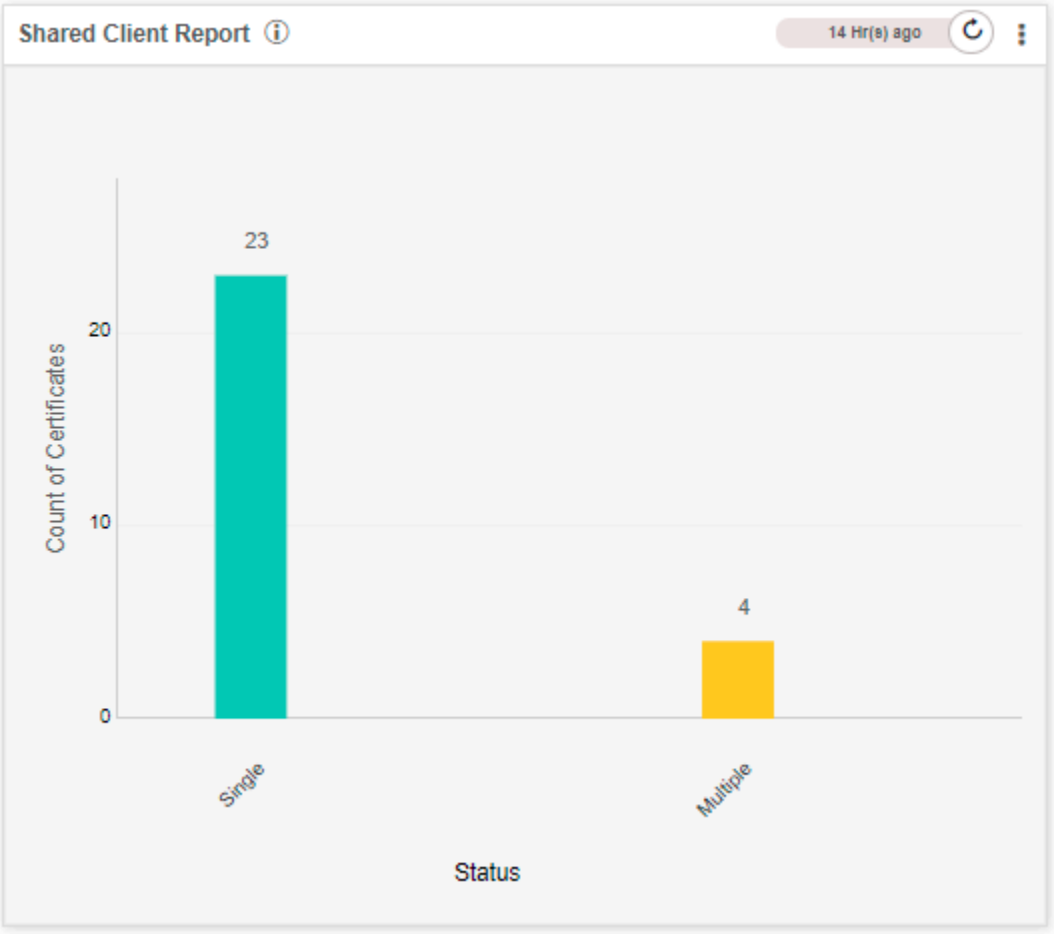
On click of this chart, the respective filtered data of certificates be shown as below:



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

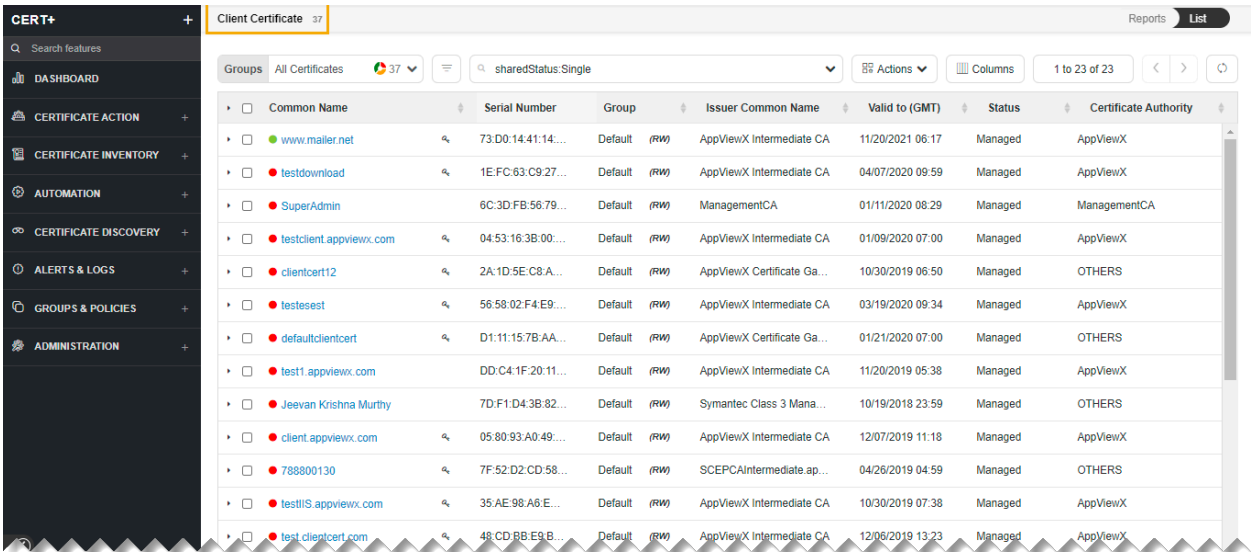
Shared Client Report

This report shows the count of certificates in the client inventory which are shared with a single endpoint or multiple endpoints.



On click of this chart, the respective filtered data of certificates be shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Understanding the Server Standard Dashboard

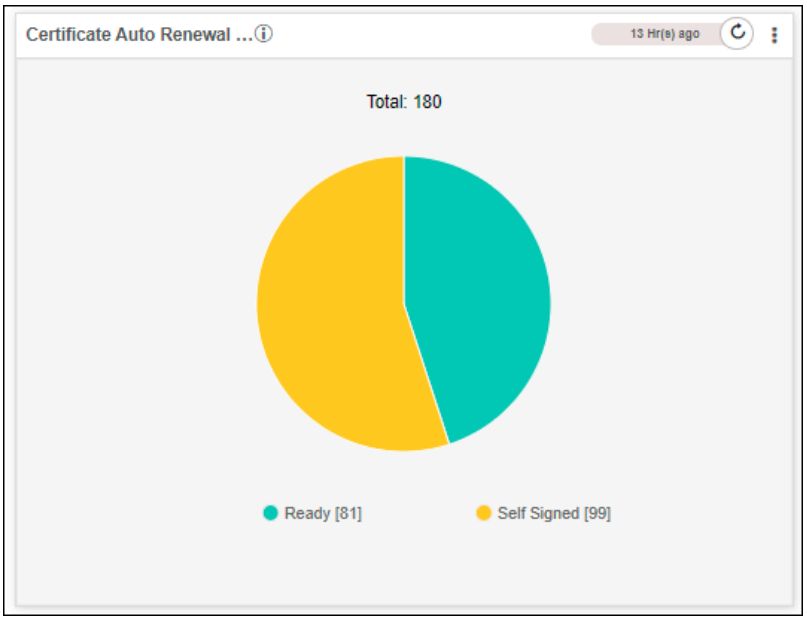
For the certificates in the Server inventory, from the standard perspective, the following are the reports available in this dashboard:

- Certificate Auto-Renewal Readiness - Server
- Certificate CA Actions - All Certificate Types
- Certificate Discovery Trend - All Certificate Types
- Report by Certificate Authority - Server

Certificate Auto-Renewal Readiness - Server

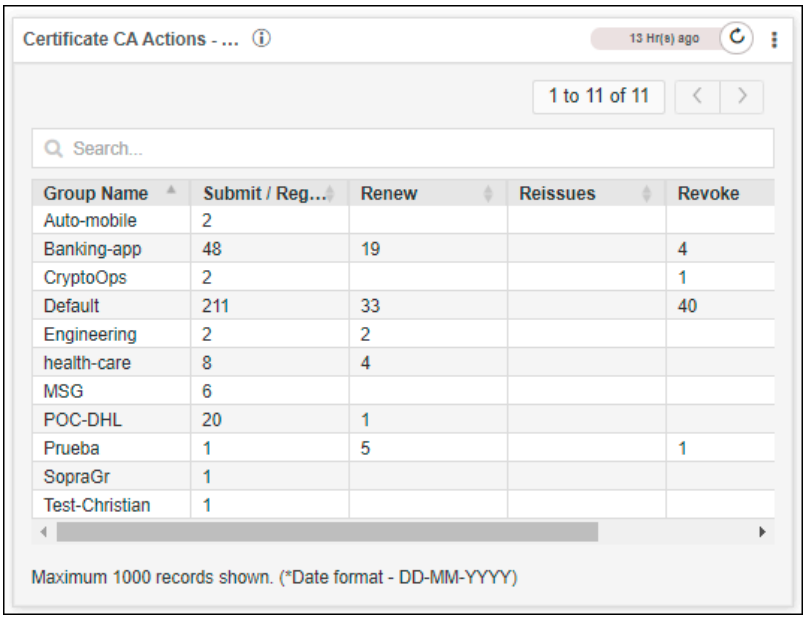
This report shows the count of certificates ready for the auto-renewal process available in the server inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate CA Actions - All Certificate Types

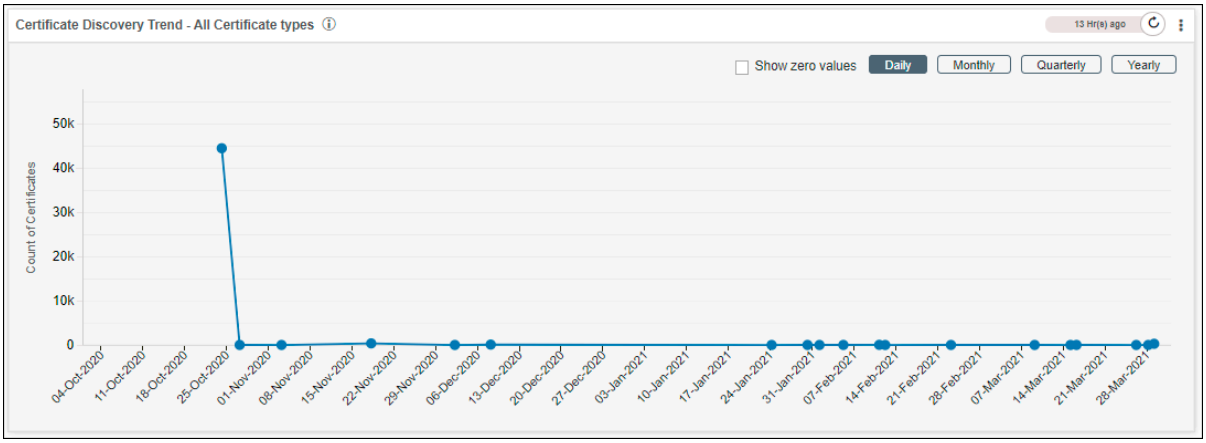
This report shows the count of CA actions performed with respect to the certificate groups available in the server inventory.



Certificate Discovery Trend - All Certificate Types

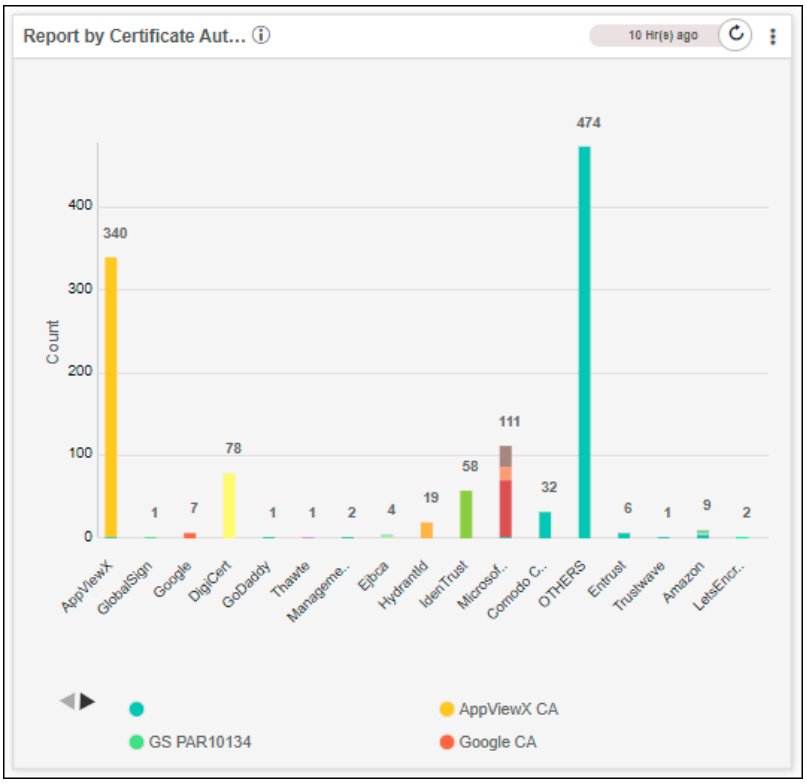
This report shows the trend of the count of certificates discovered into AppViewX in the last year.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



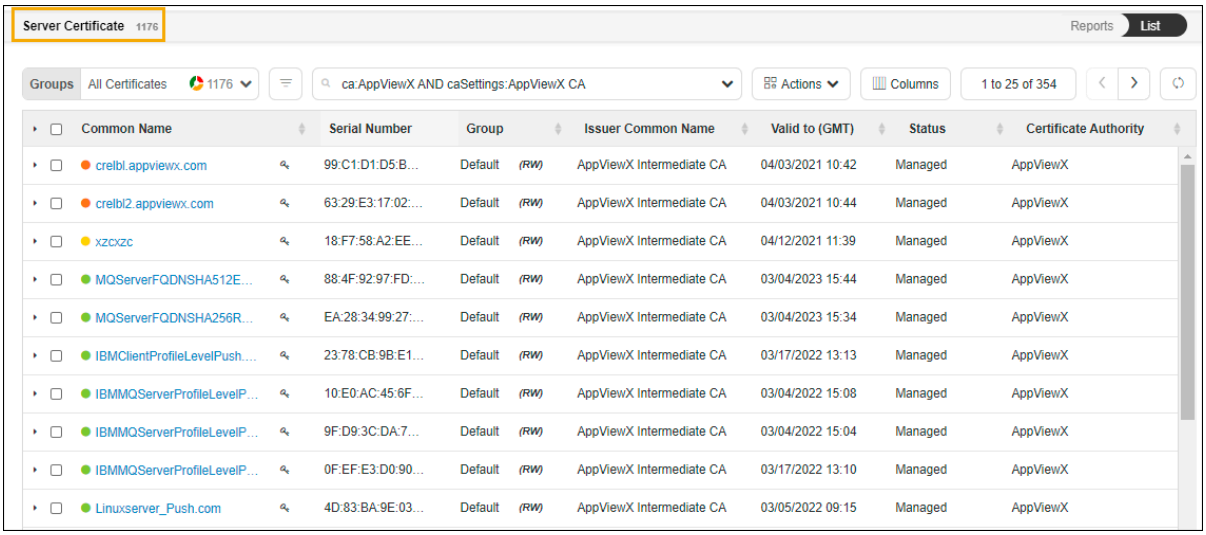
Report by Certificate Authority - Server

This report shows the count of certificates available in the server inventory with respect to the CA accounts.



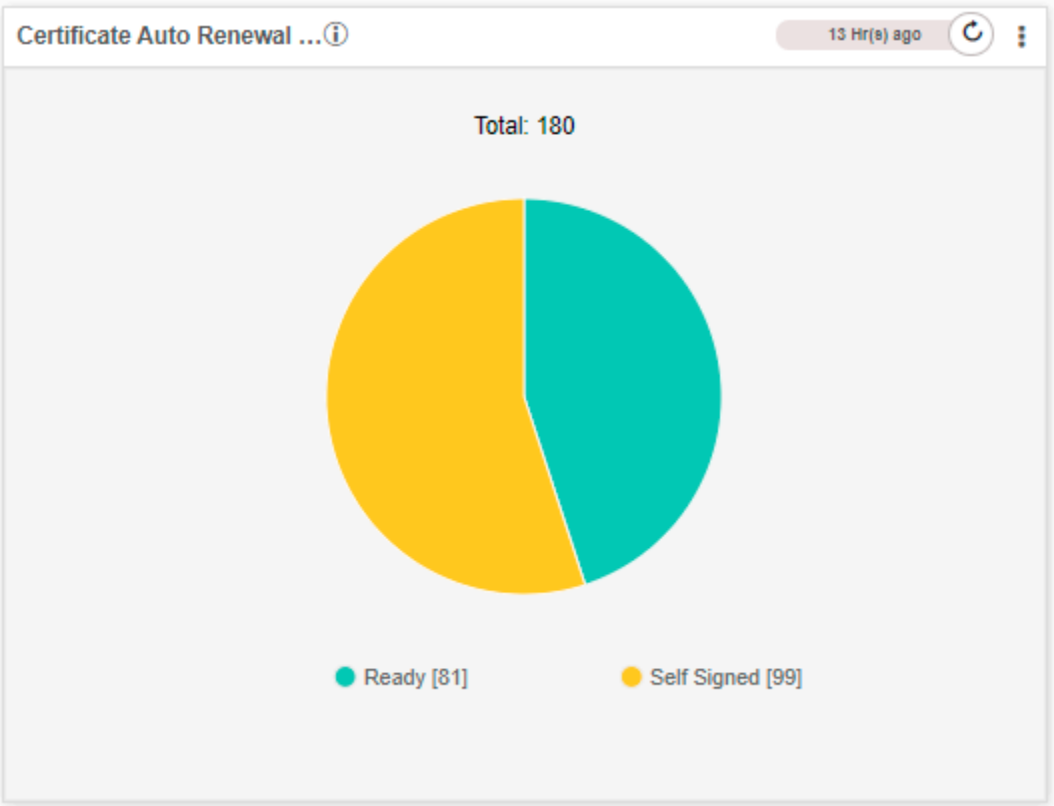
When you click of the chart, the filtered data of certificates are shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate Auto-Renewal Readiness - Server

This report shows the count of certificates ready for the auto-renewal process available in the server inventory.

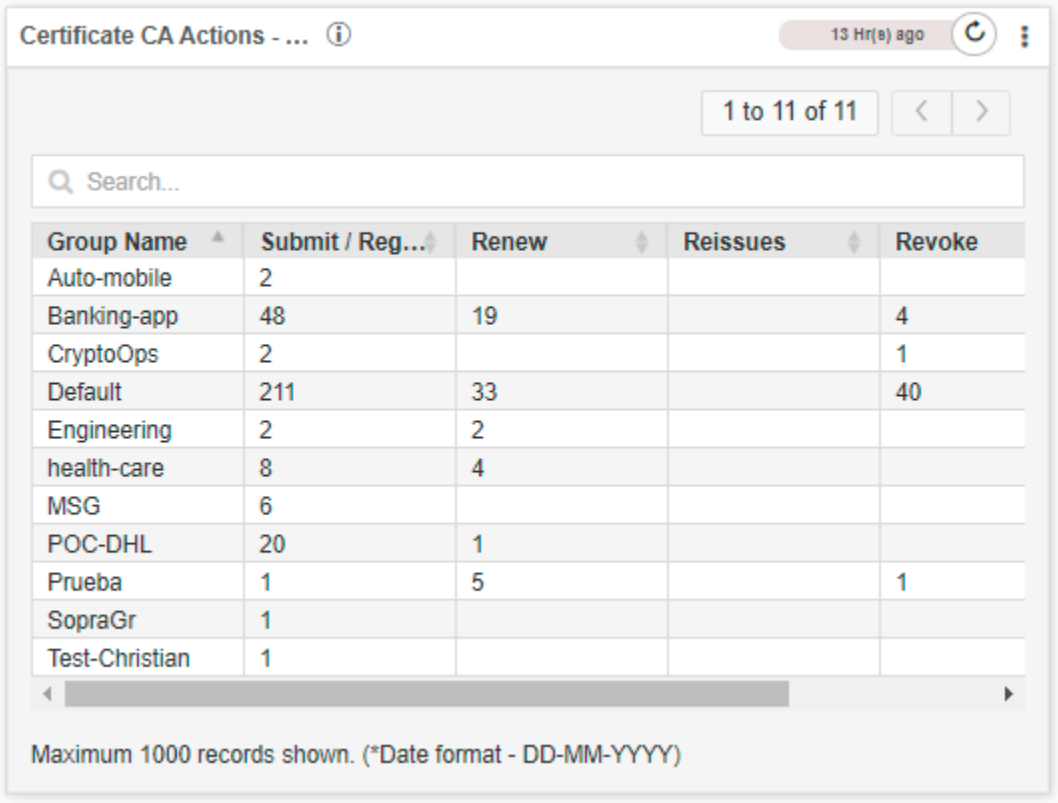


On click of the chart, the filtered data of certificates are shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

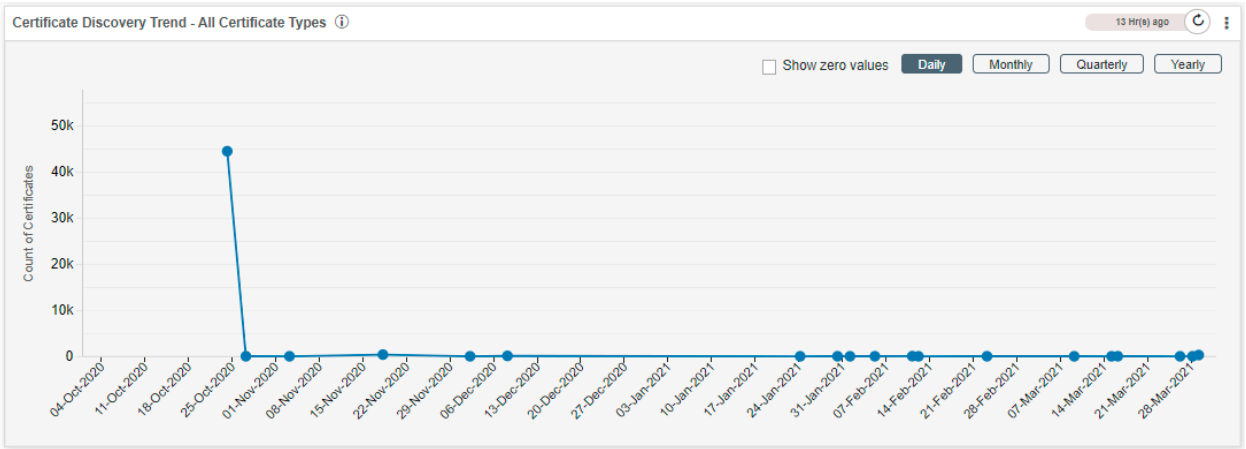
Certificate CA Actions - All Certificate Types

This report shows the count of CA actions performed with respect to the certificate groups available in the server inventory.



Certificate Discovery Trend - All Certificate Types

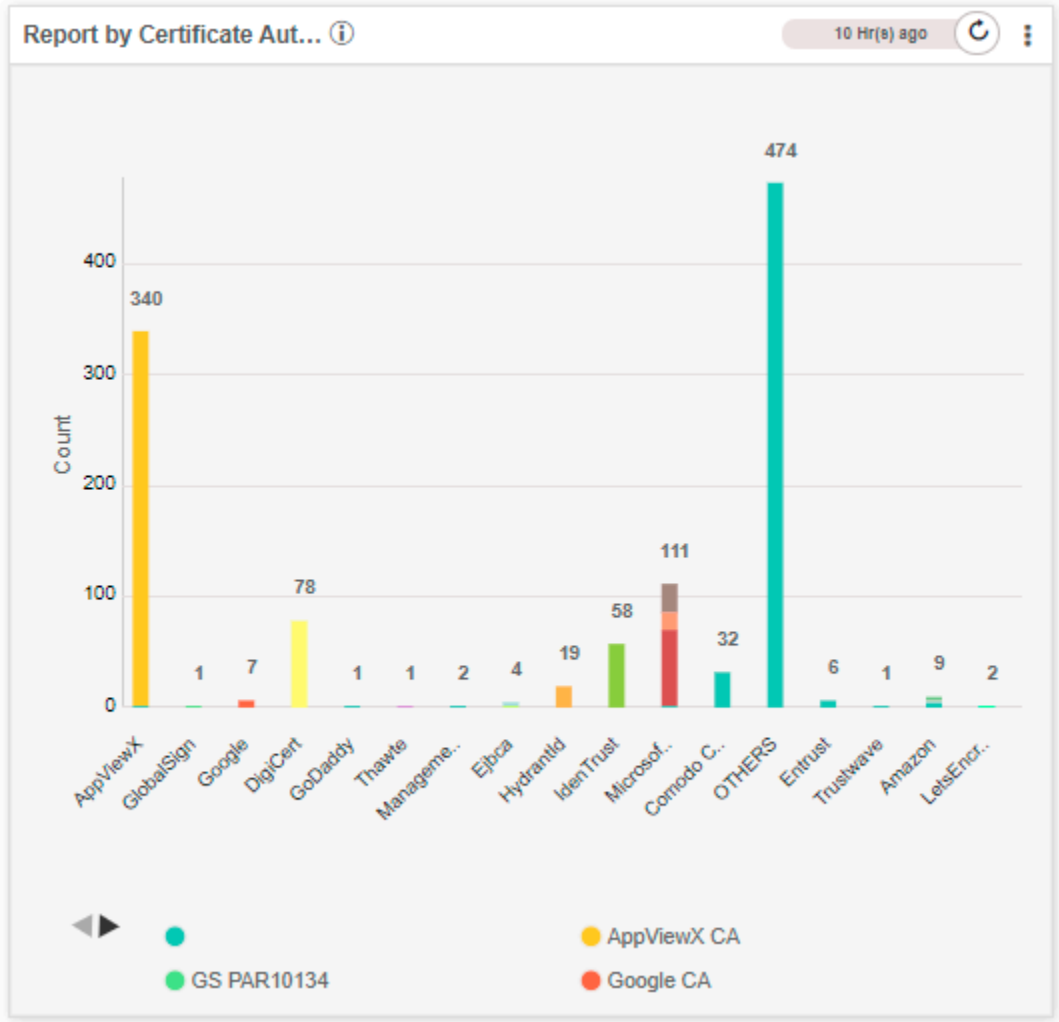
This report shows the trend of the count of certificates discovered into AppViewX in the last year.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

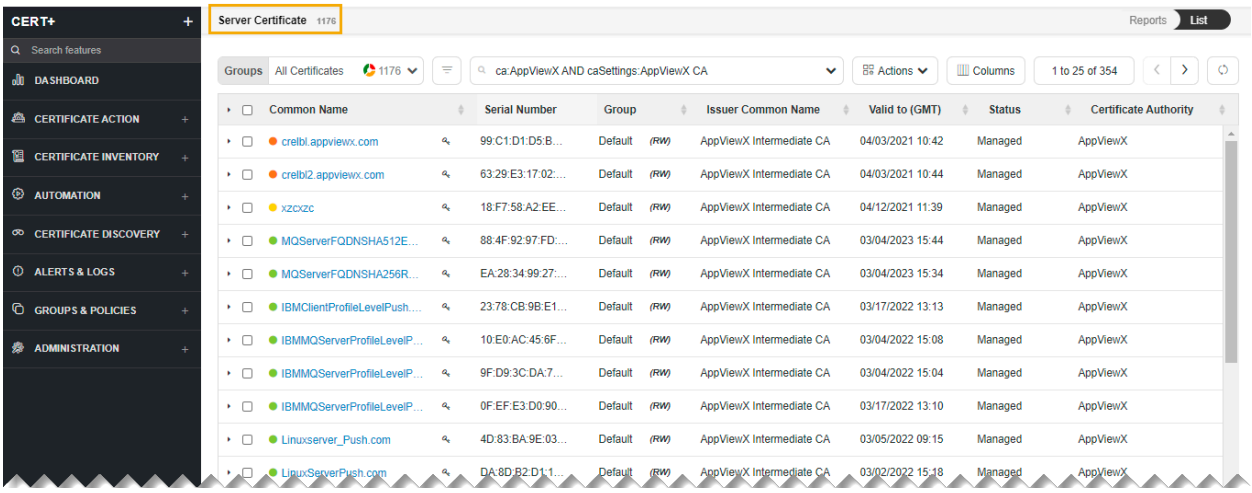
Report by Certificate Authority - Server

This report shows the count of certificates available in the server inventory with respect to the CA accounts.



When you click of the chart, the filtered data of certificates are shown as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Understanding the Client Standard Dashboard

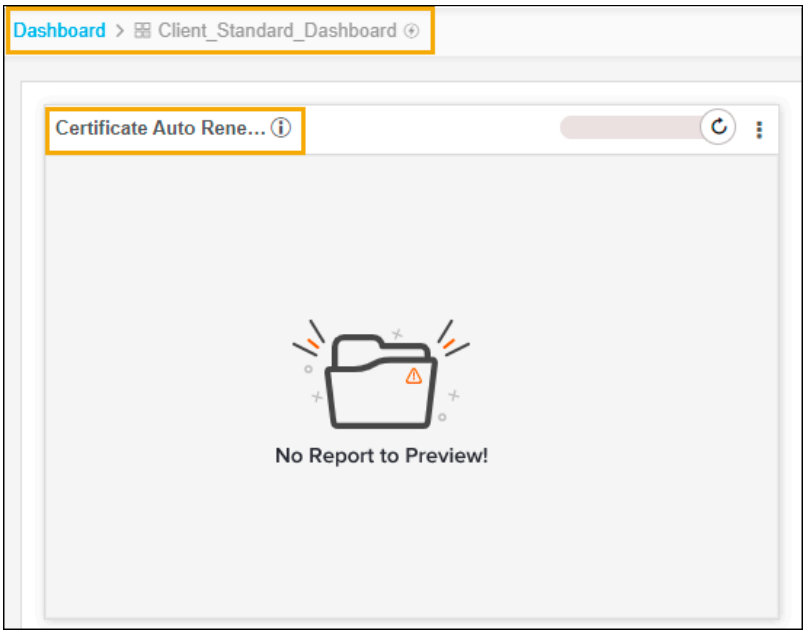
For the certificates in the Client inventory, from the standard perspective, the following are the reports available in this dashboard:

- Certificate Auto-Renewal Readiness - Client
- Certificate Discovery Trend - All Certificate Types
- Certificate CA Actions - All Certificate Types
- Report by Certificate Authority Accounts - Client

Certificate Auto-Renewal Readiness - Client

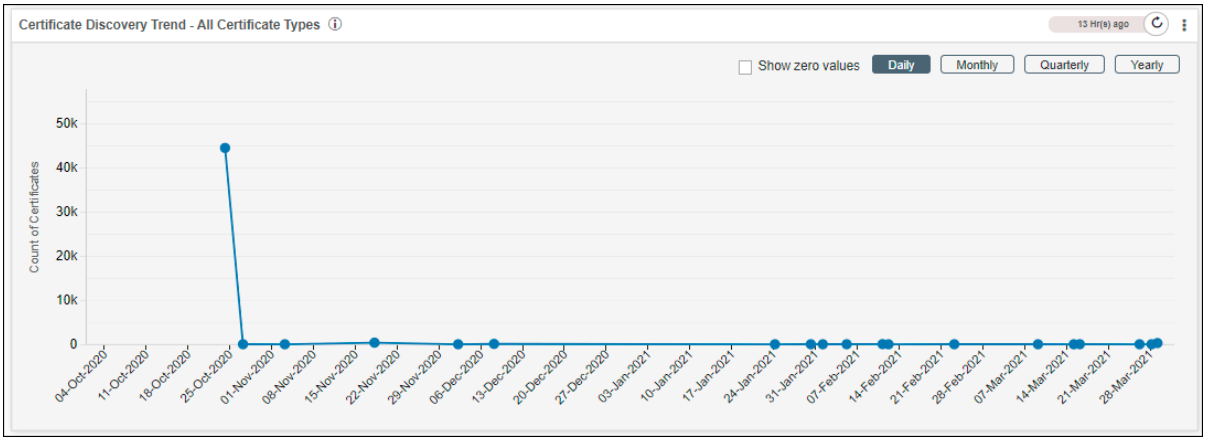
This report shows the count of certificates ready for the auto-renewal process available in the Client inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate Discovery Trend - All Certificate Types

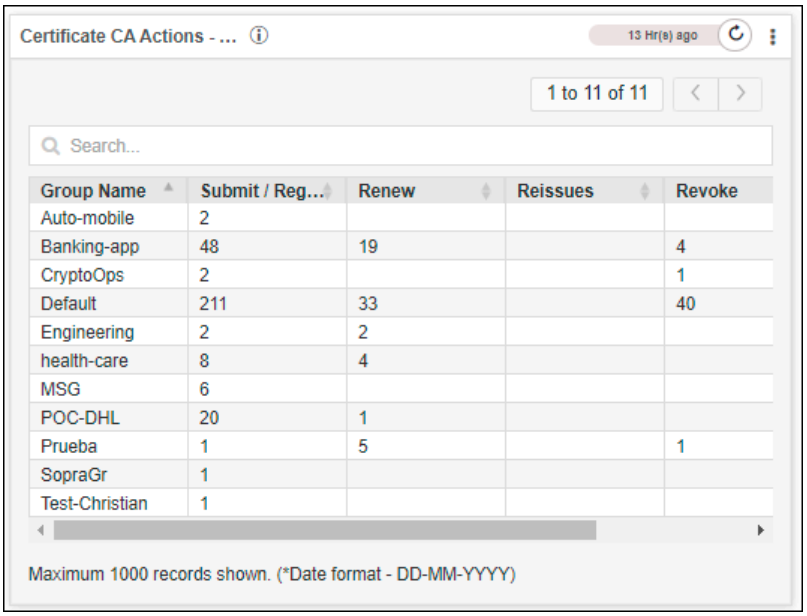
This report shows the trend of the count of certificates discovered in AppViewX in the last year.



Certificate CA Actions - All Certificate Types

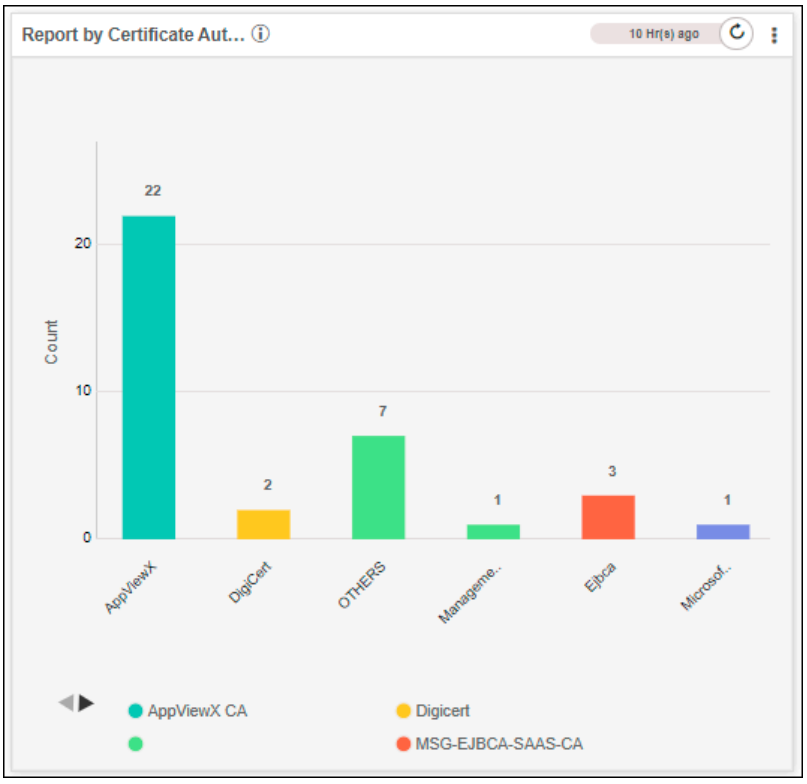
This report shows the count of CA actions performed with respect to the certificate groups available in the Client inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Report by Certificate Authority Accounts - Client

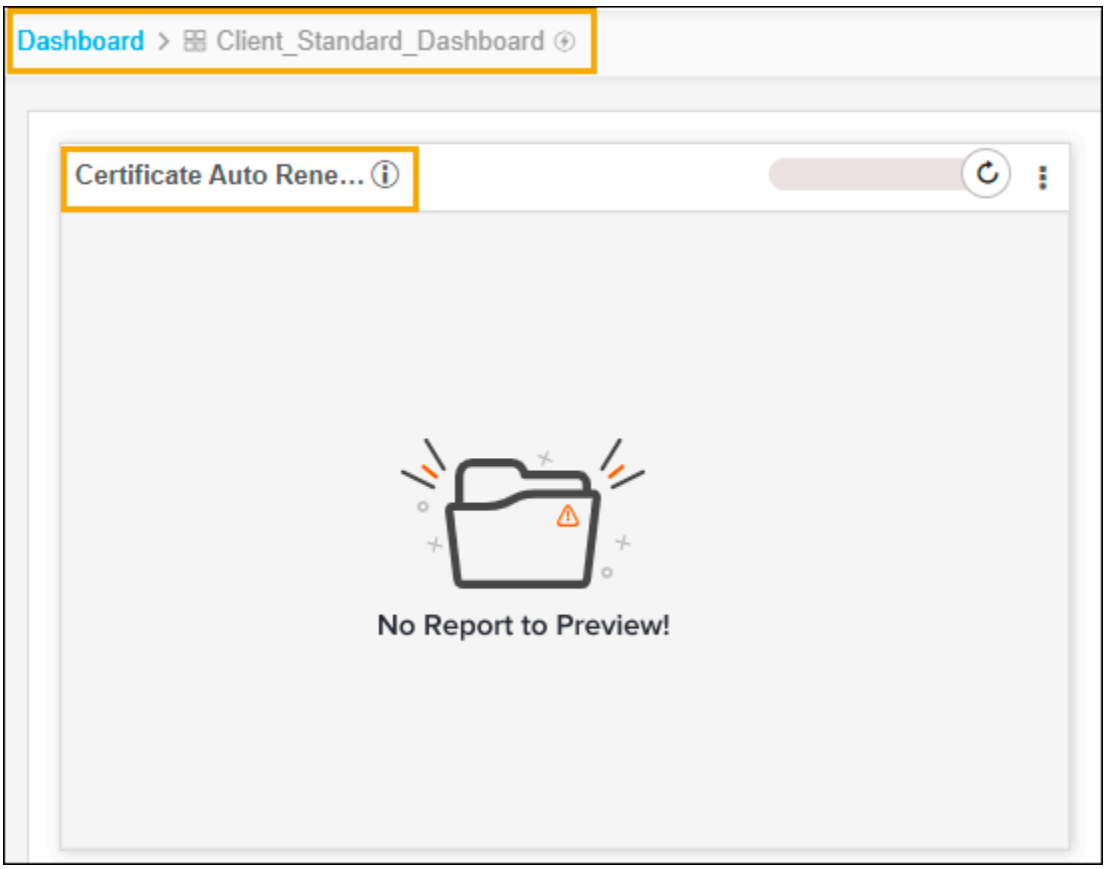
This report shows the count of certificates available in the client inventory with respect to the CA accounts.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Auto-Renewal Readiness - Client

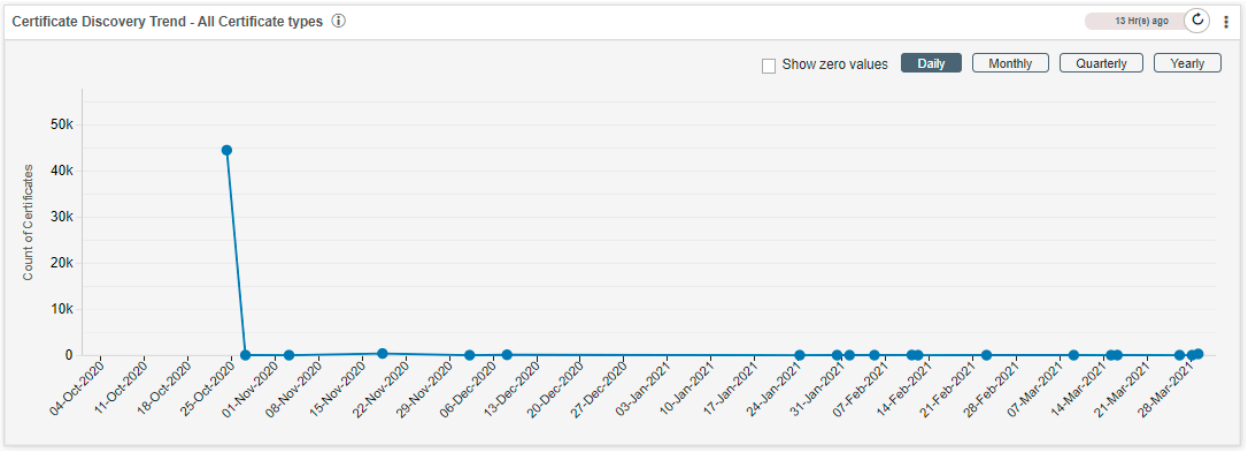
This report shows the count of certificates ready for the auto-renewal process available in the Client inventory.



Certificate Discovery Trend - All Certificate Types

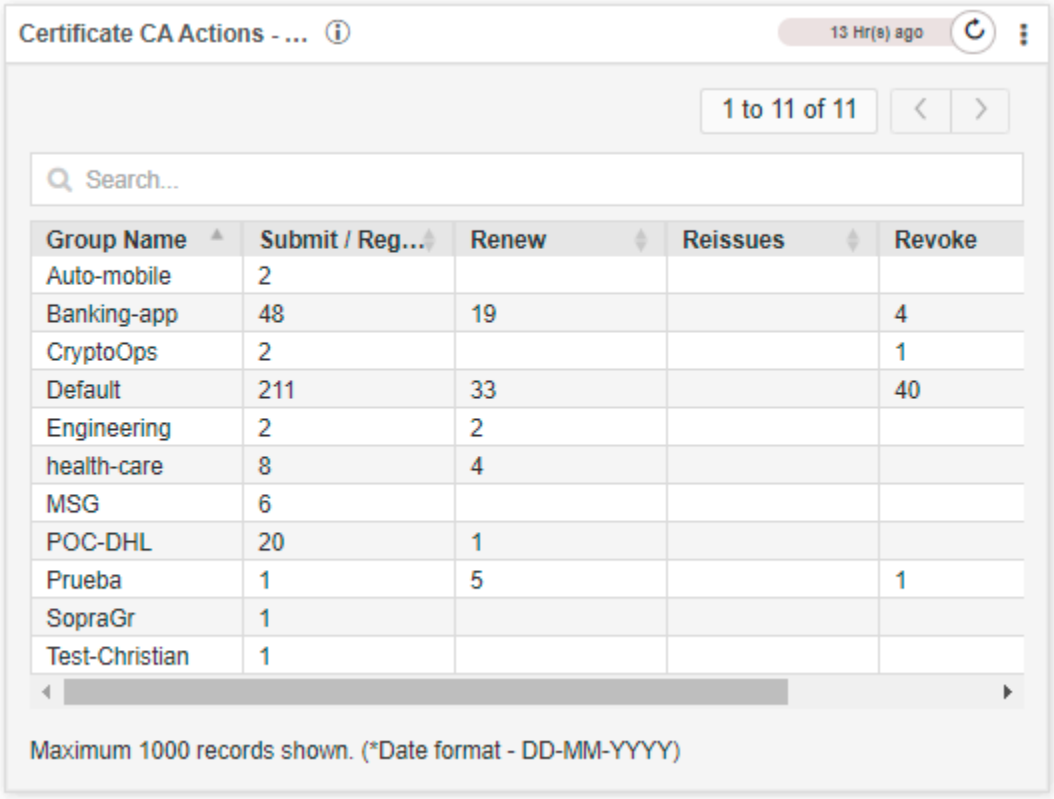
This report shows the trend of the count of certificates discovered in AppViewX in the last year.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate CA Actions - All Certificate Types

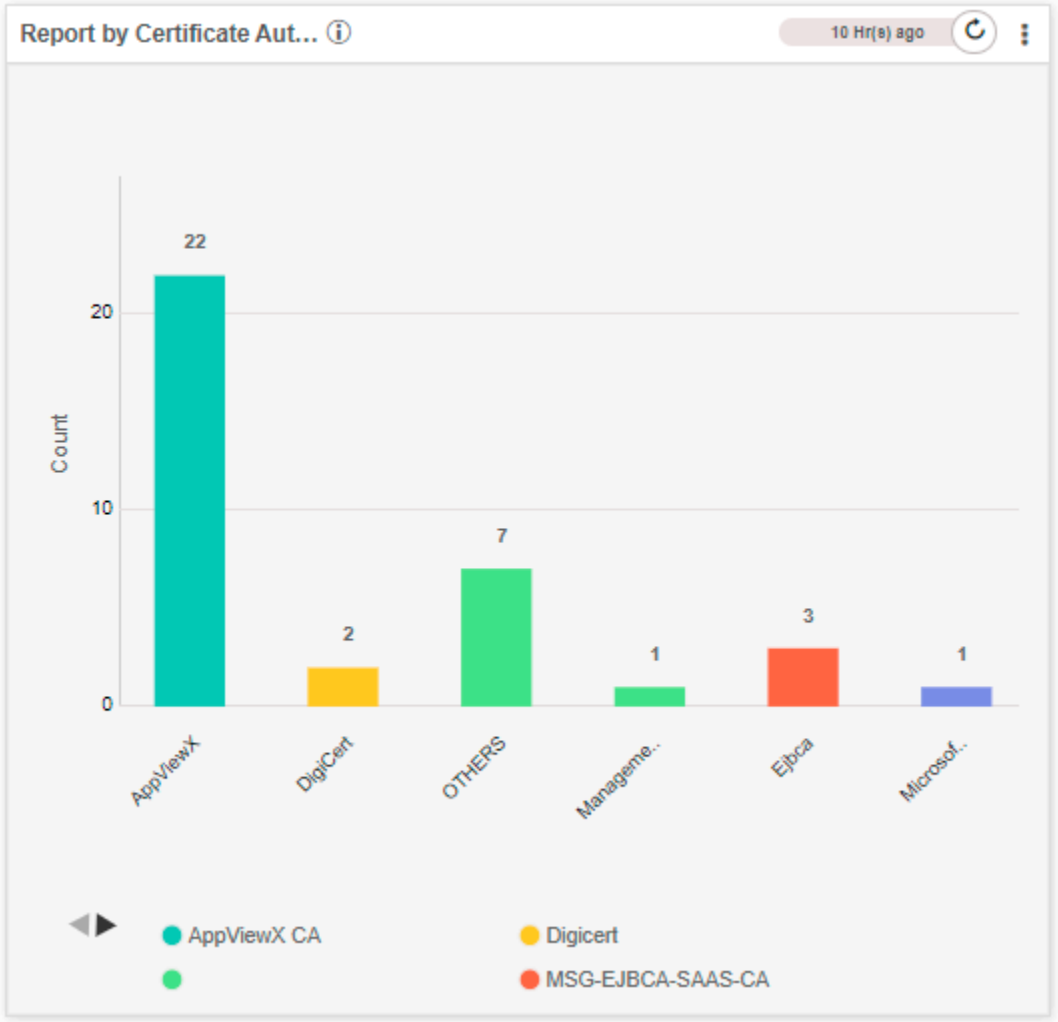
This report shows the count of CA actions performed with respect to the certificate groups available in the Client inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Report by Certificate Authority Accounts - Client

This report shows the count of certificates available in the client inventory with respect to the CA accounts.



On click of the chart, the respective filtered data of certificates will be shown.

Understanding the Trust Store Certificates Dashboard

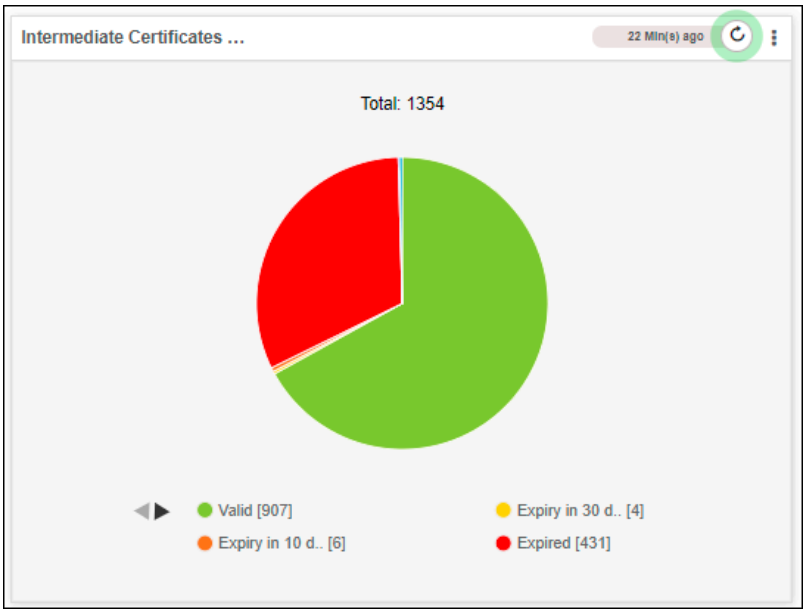
For the certificates in the Root and Intermediate inventories, the following are the reports available in this dashboard:

- Intermediate Certificates Expiry Statuses
- Root Certificates Expiry Statuses

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

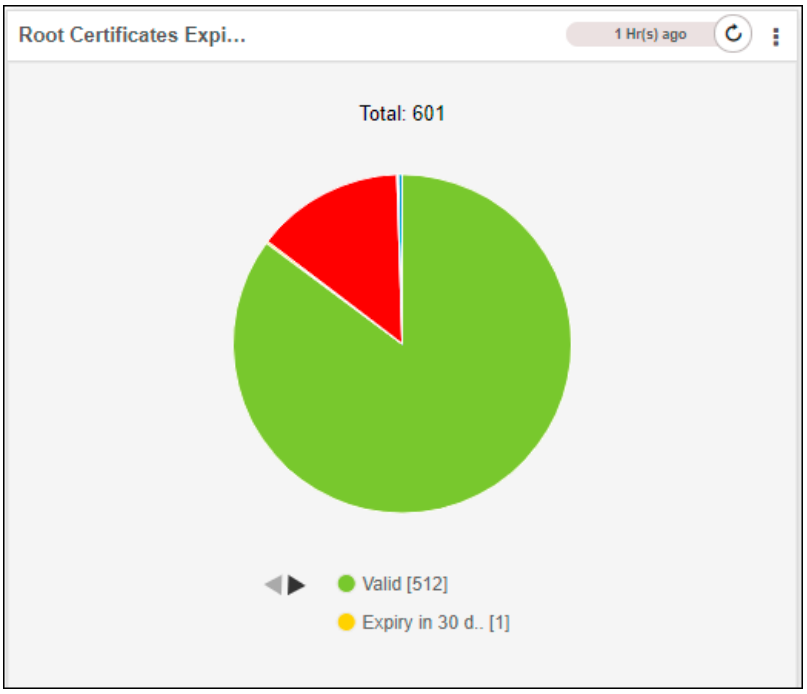
Intermediate Certificates Expiry Statuses

This report shows the count of certificates in the intermediate certificate inventory with respect to the valid and expiry status of the certificates.



Root Certificates Expiry Statuses

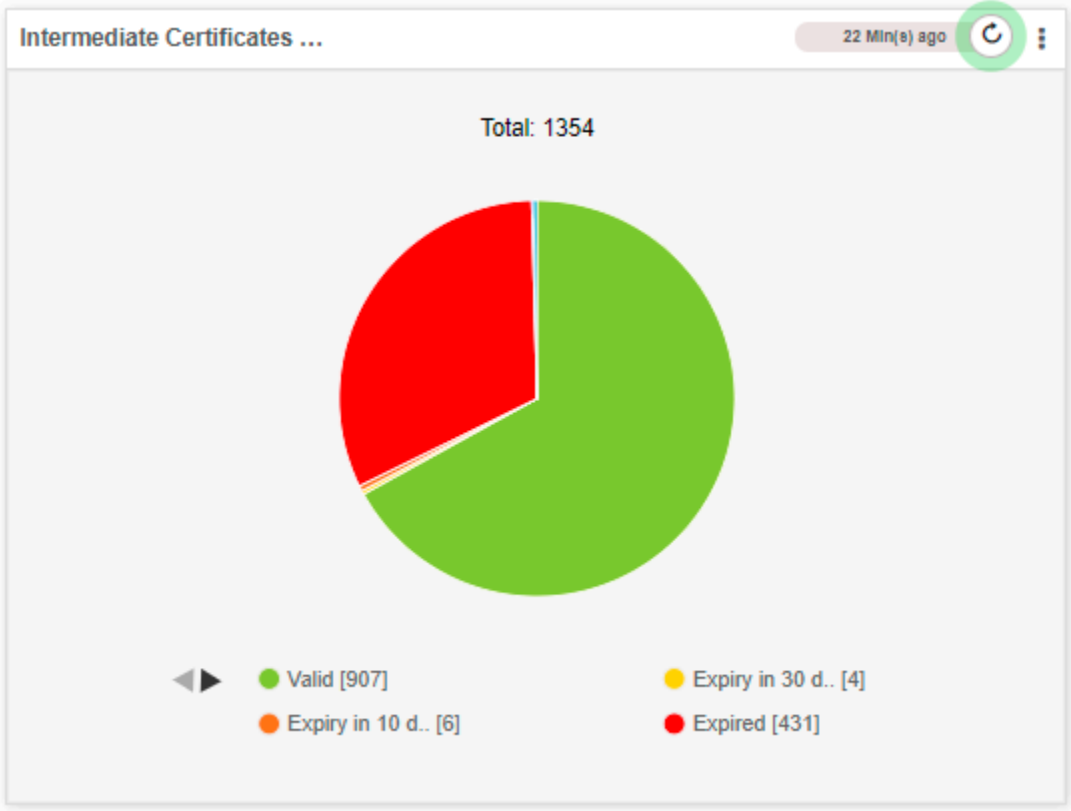
This report shows the count of certificates in the root certificate inventory with respect to the valid and expiry status of the certificates.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Intermediate Certificates Expiry Statuses

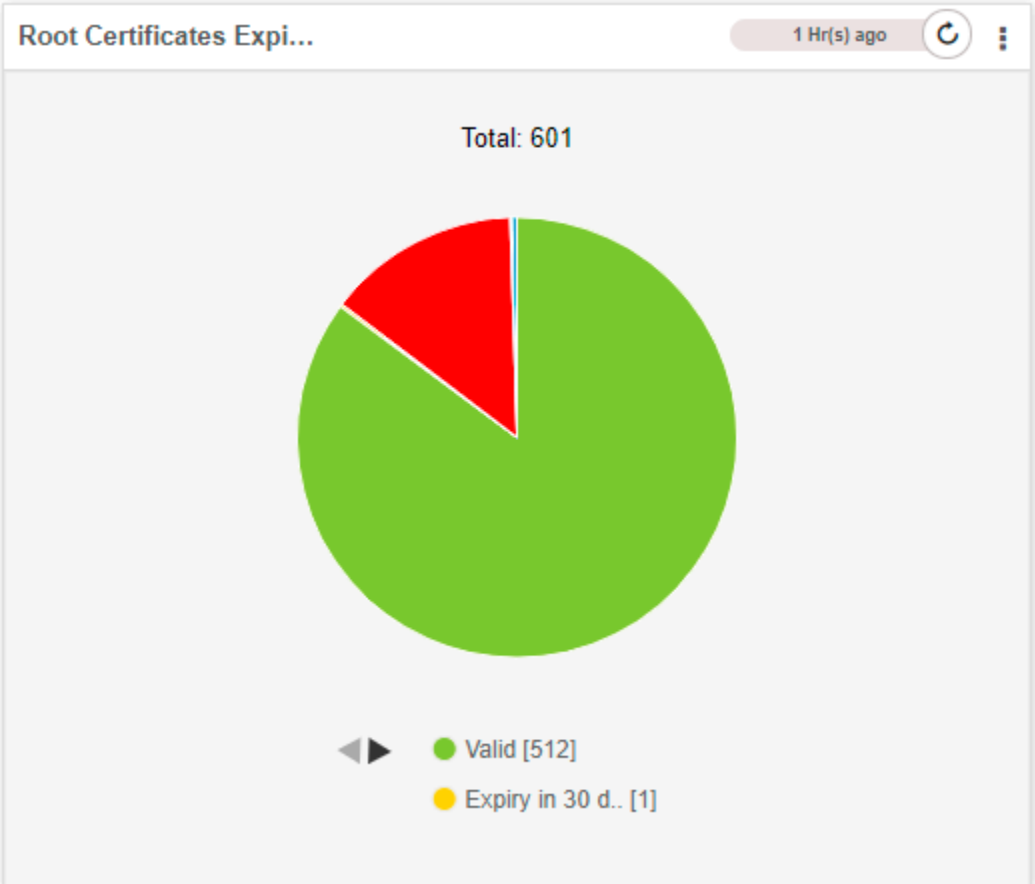
This report shows the count of certificates in the intermediate certificate inventory with respect to the valid and expiry status of the certificates.



Root Certificates Expiry Statuses

This report shows the count of certificates in the root certificate inventory with respect to the valid and expiry status of the certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Report Customization

AppViewX CERT+ allows you to customize your reports based on the organization's needs. Depending on the customization, reports are classified into:

- My Reports
- Store
- Widget

My Reports

Personalized reports can be generated based on a user account. This will be useful when an operator is assigned to do a specific task and has to generate reports on the same. To know more about **My Reports**, refer below.

- Creating a New Report
- Cloning a Report

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

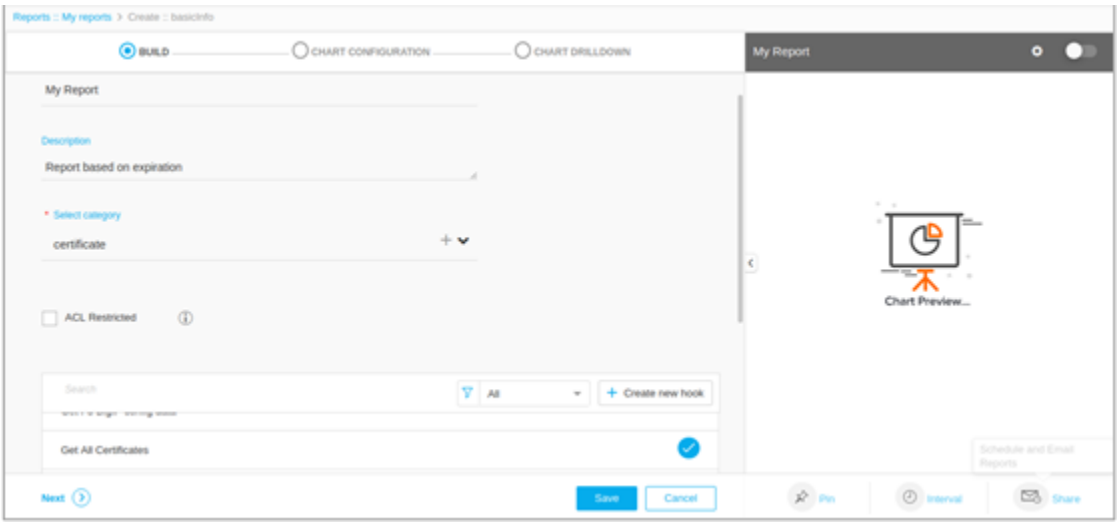
• Deleting a Report
• Pinning a Report
• Sharing a Report

Creating a New Report

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.
3. Click **Studio > Reports**.

   By default, **My Reports** page will be displayed.
4. Click **Create New Report** on the top-right.
5. On the **Create Report** page, enter the **Report Name**, **Description** and select a **Category** from the list.
6. Enable **ACL Restricted** option if you want the report to be visible based on the user's resource access.
7. Select a hook from the list of available hooks or click **Create New Hook**.
8. Click **Save** to save details.
9. Click **Next** at the bottom-left.



10. On the **Chart Configuration** page, select one of the following chart types:
    - Pie
    - Donut
    - Bar
    - Stacked Bar

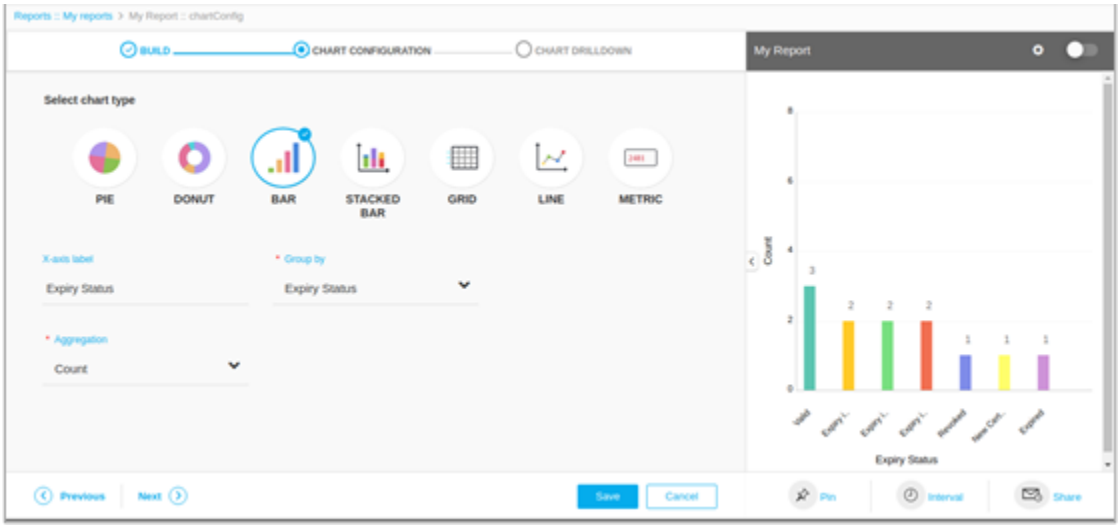
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Grid
- Line
- Metric

- If you have selected **Pie** chart type, choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Donut** chart type, choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected the **Bar chart** type, fill the **X-axis Label** field and choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Stacked Bar** chart type, fill the **X-axis Label** field and choose an option from the **Group By**, **Aggregation**, and **Stacked By** dropdown.
- If you have selected **Grid** chart type, enable the **Show Column Headers** option if required. Then, under **Columns**, select columns or click the **Select All** option.

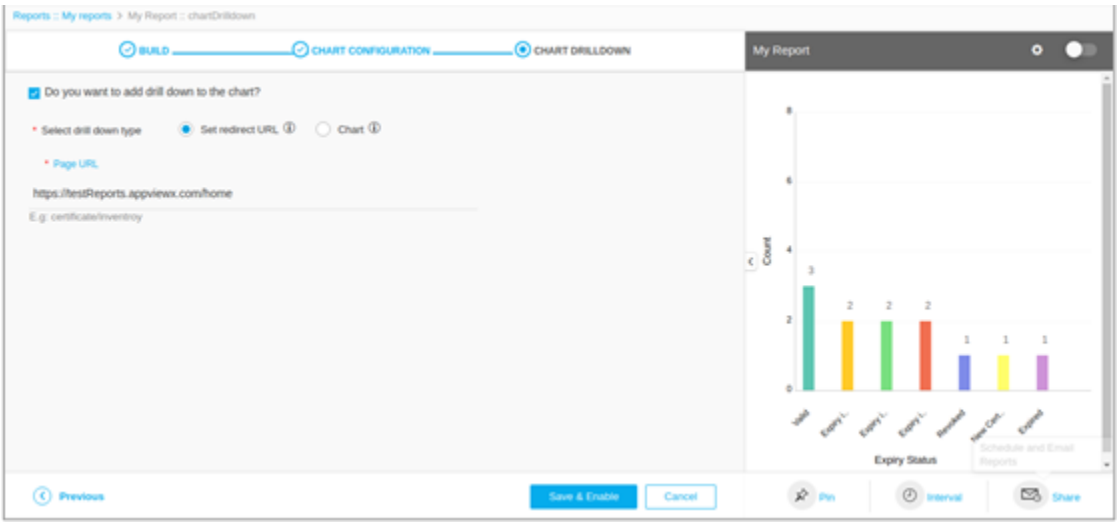
> **Note:** For the Select All option, only 10 columns can be selected.

- If you have selected **Grid** chart type, fill the **X-axis Label** field, choose a **Date Format**, and choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Metric** chart type, enter a **Chart Title** and choose an option from the **Aggregation** dropdown. Under **Chart Formatting**, select a chart size, alignment, font color, and icon.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

11. Click **Save**.
12. Click **Next** at the bottom-left.
13. On the **Chart Drilldown** page, enable the **Do you want to add drill down to the chart?** option to add drilldown.
14. Click **Save & Enable**.
    The graphical representation of the report will be displayed on the right.
15. To enable the generated report, click the enable icon on the top-right of the report window.
16. To pin the report to a dashboard page, click the **Pin** icon at the bottom right. Select Existing Dashboard or New Dashboard based on where it needs to be pinned.
17. To set the polling interval to collect data, click the **Interval** icon at the bottom right.
18. To share the report, click the **Share** icon at the bottom right.

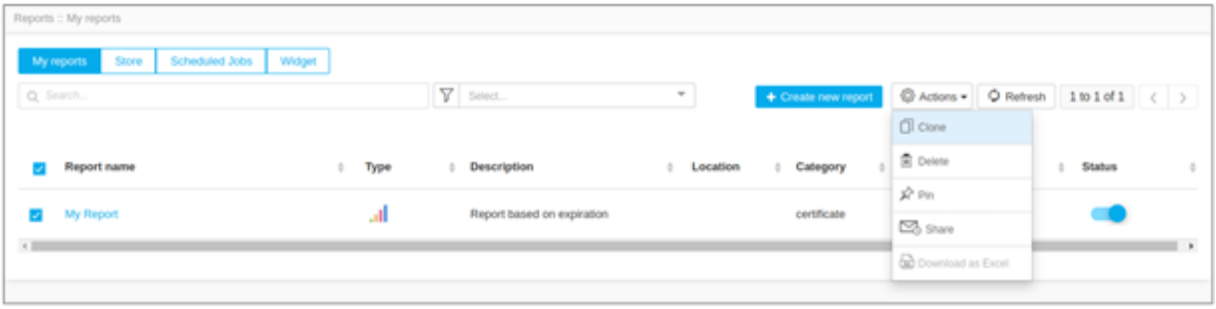


Cloning a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

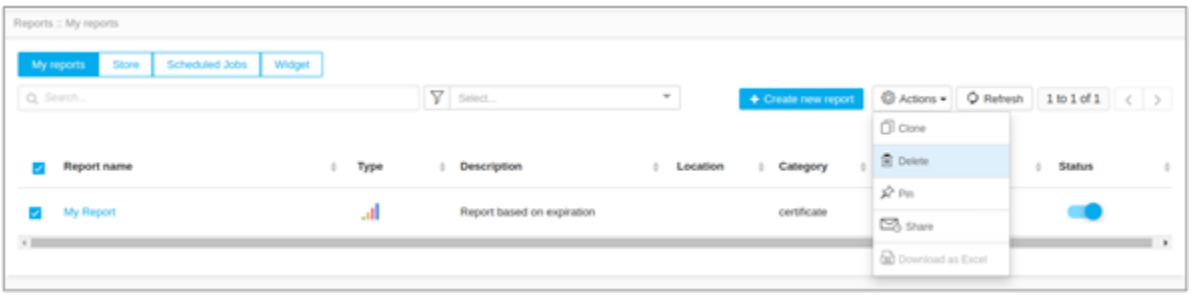
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The cloned reports will be displayed under the **My Reports** tab.



Deleting a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.

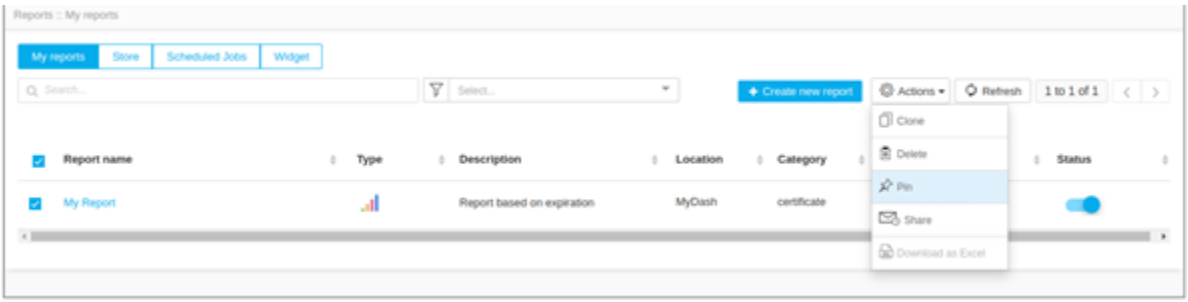


Pinning a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.

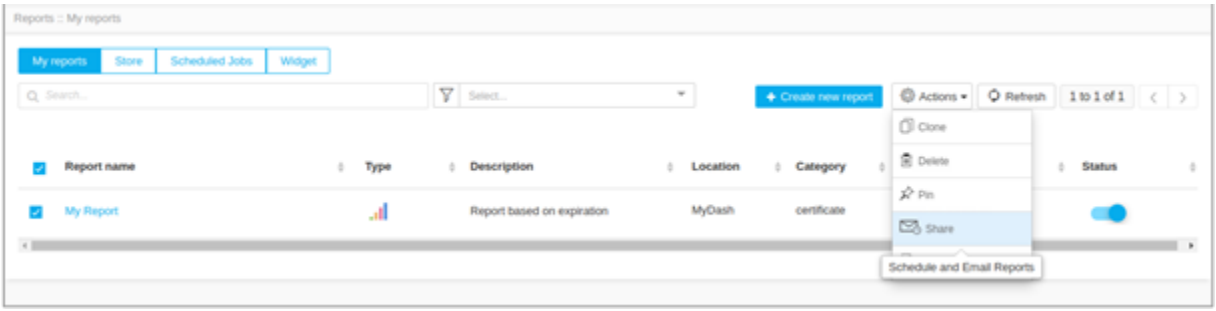
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.



Sharing a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share** to schedule and email reports.
5. On the **Schedule reports** window, fill the **General** section for mail content and **Schedule** section for scheduling emails.
6. Click **Save**.



Store

There are a few pre-defined reports available in the store. These reports can be cloned and customized to have personalized reports, but cannot be modified. To know more about **Store**, refer below.

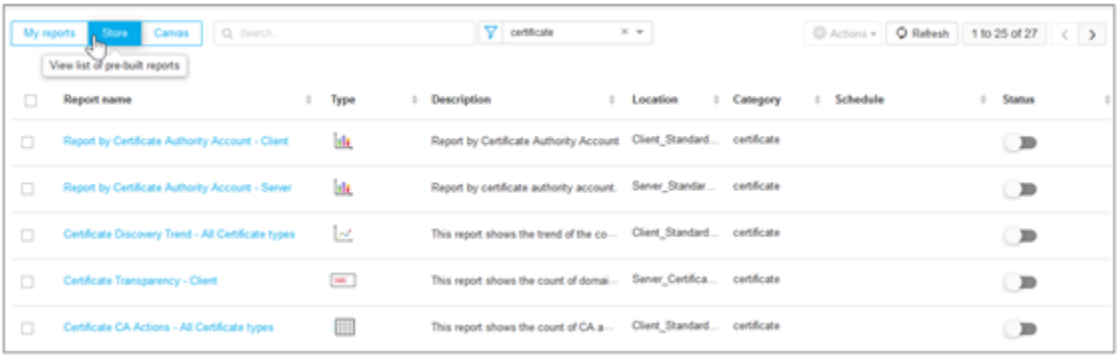
- Viewing Pre-built Reports
- Cloning a Pre-built Report

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Pinning a Pre-built Report
• Sharing a Pre-built Report

Viewing Pre-built Reports

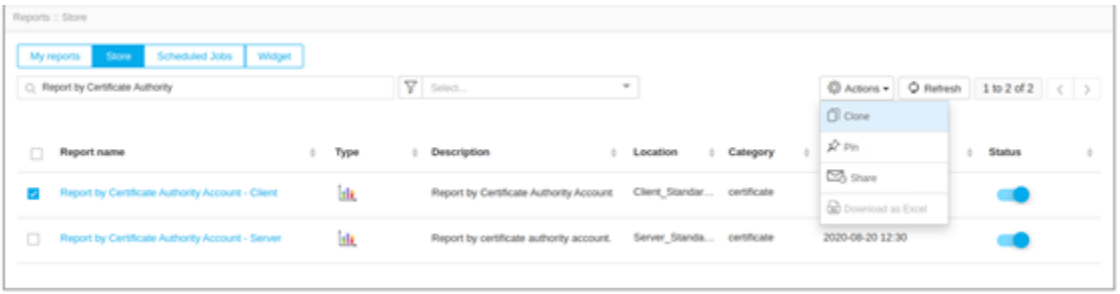
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **Studio > Reports**.
   By default, the My Reports page will be displayed.
4. Click **Store** on the top-left.
   list of pre-built reports will be displayed.
5. You can search for reports and filter reports by category.



Cloning a Pre-built Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

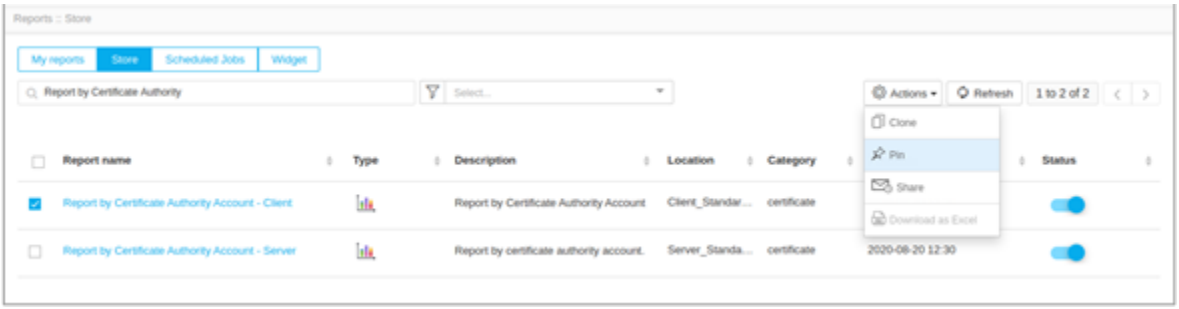


The cloned reports will be displayed under the **Store** tab.

Note: By default, store/pre-built reports are enabled. You cannot disable or delete it.

Pinning a Pre-built Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu >> Studio >> Reports**.
3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to the Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.



6. Click **Save**.

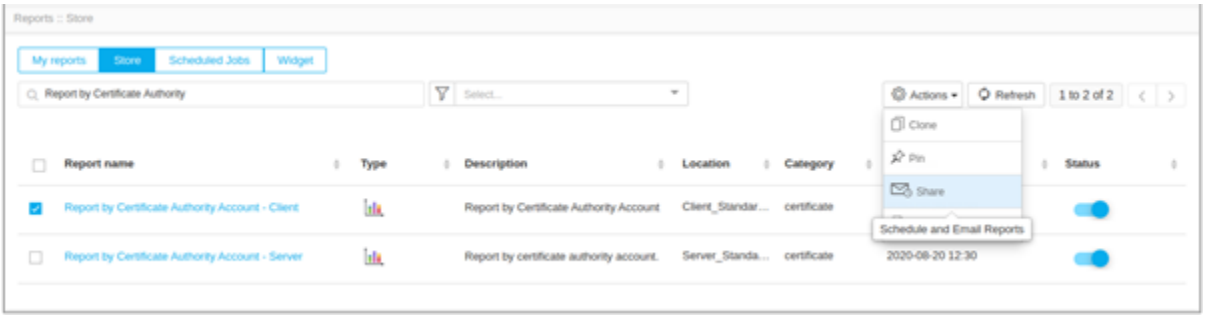
The pinned reports will be displayed in the dashboard.

Sharing a Pre-built Report

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

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Under the Store tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.
5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.
6. Click **Save**.



Widget

Widget reports are useful when an operator creates their widget based on the business needs. These widgets display the count of a specific operation that is executed and pending in the system. To know more about **Widget**, refer below.

- Viewing Custom Reports
- Creating a New Widget
- Cloning a Widget
- Deleting a Widget
- Pinning a Widget
- Sharing a Widget

Viewing Custom Reports

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.

3. Click **Studio > Reports**.

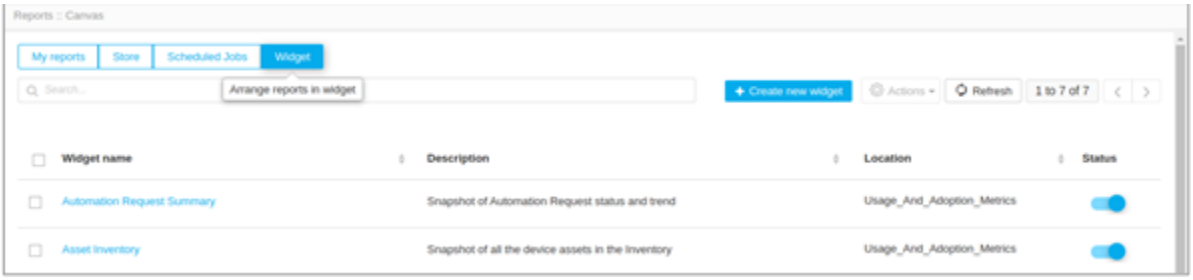
   By default, **the My Reports** page will be displayed.

4. Click **Widget** on the top-left.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

A list of custom reports with the Widget Name, Description, Location, and Status will be displayed.

5. You can search for reports and filter reports by category.



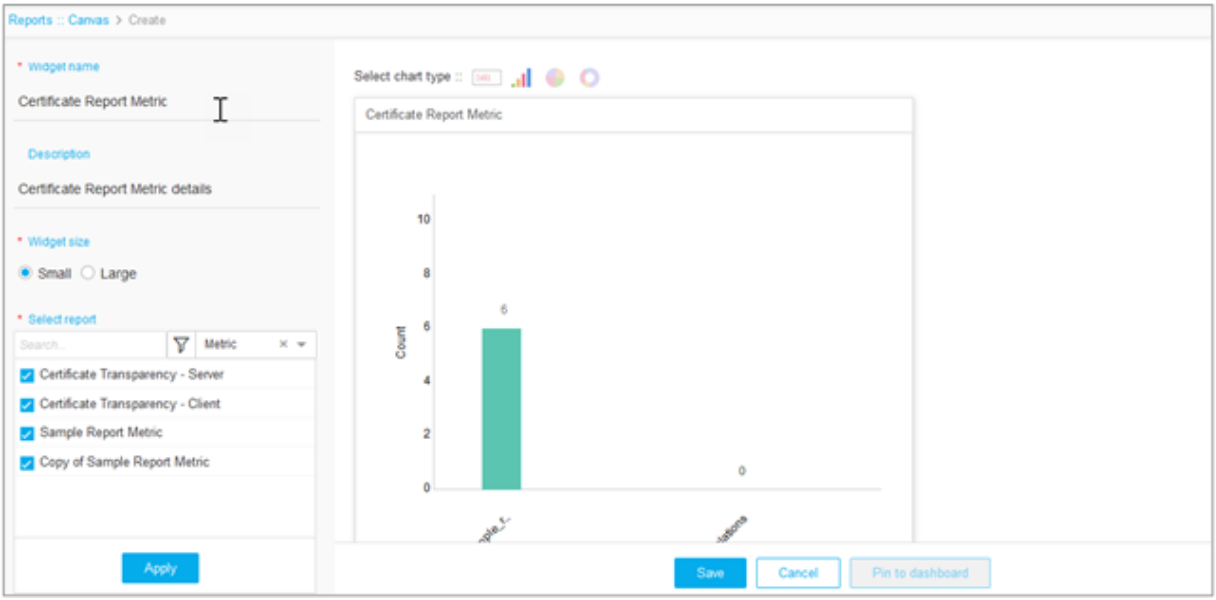
Creating a New Widget

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

   By default, **the My Reports** page will be displayed.
3. Click **Widget** on the top-left.
4. Click **+ Create New Widget** on the top-right.
5. On the **Create Widget** page, enter a **Widget Name** and **Description**.
6. Select the **Widget Size**: **Small** or **Large**.
7. Under **Select Report**, select a report from the list or search for specific reports.
8. Click **Apply**.
9. Select a **Chart Type**: **Metric**, **Bar**, **Pie** or **Donut**.
10. Click **Save**.
11. Click **Pin to Dashboard** to pin the widget to the existing or new dashboard.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

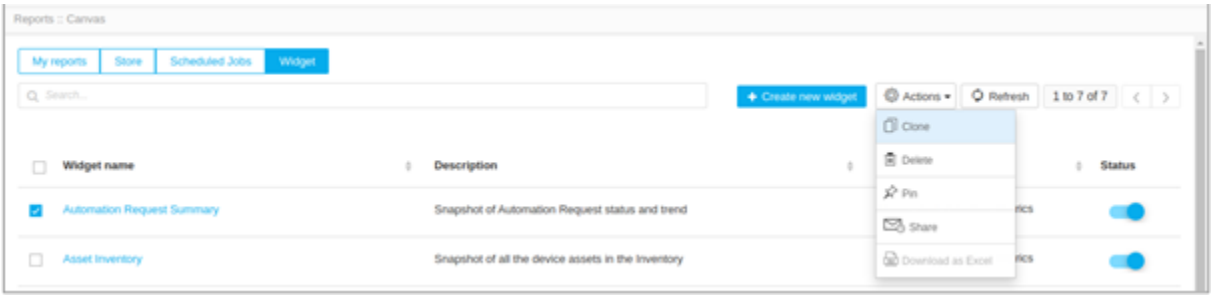
12. To enable the widget status, click the **Status** icon on the top-right.



Cloning a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

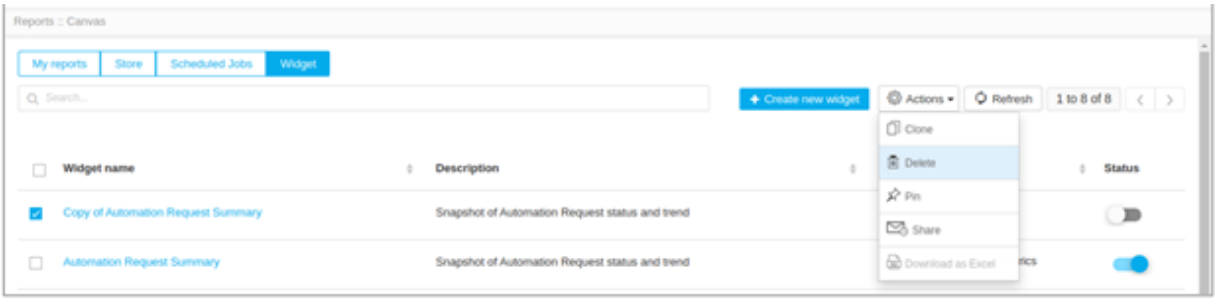
   The Cloned reports will be displayed under the **Widget** tab.



Deleting a Widget

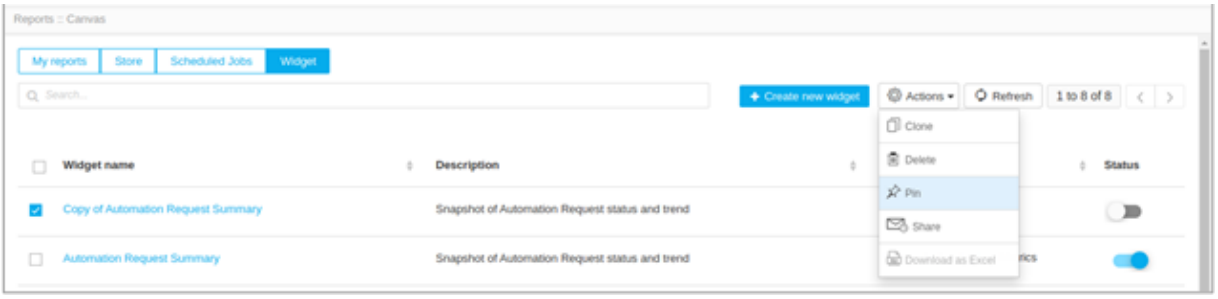
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.



Pinning a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.

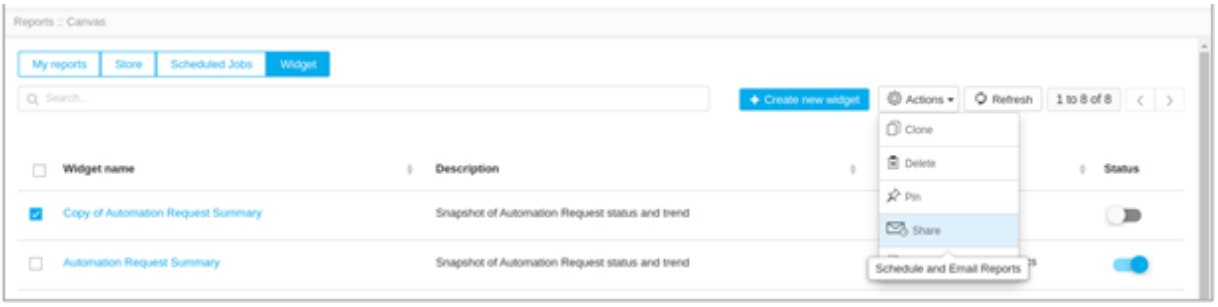


Sharing a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.
6. Click **Save.**



Security Posture Determination and Interpretation

Application security score reports, TLS, and Cipher suite reports allow you to identify the security level of service. To reduce security risks, change the application configuration to restrict the cipher suites and the TLS versions that are marked as LOW. Also for certain applications, OS upgrades will be applied to align with the security standard.

You can generate security reports through,

- TLS Report
- Cipher Suites Reports
- Generating Application Score Reports

TLS Report

TLS report fetches data from SSL sessions and generates the report. It makes it easy for customers to check the protocol version of their servers based on this data. This report will generate data to identify vulnerable protocol versions. For example, in your infrastructure, there may be endpoints that still support TLSv1.0 and TLSv1.1 versions.

The **TLS version - Server** report is available on the **Server Endpoint Security** dashboard.

Cipher Suites Reports

Some ciphers use SHA1 that is still supported by servers. Cipher Report will discover servers that support these ciphers and provide data as per security standards. This report will generate data to identify vulnerable ciphers.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

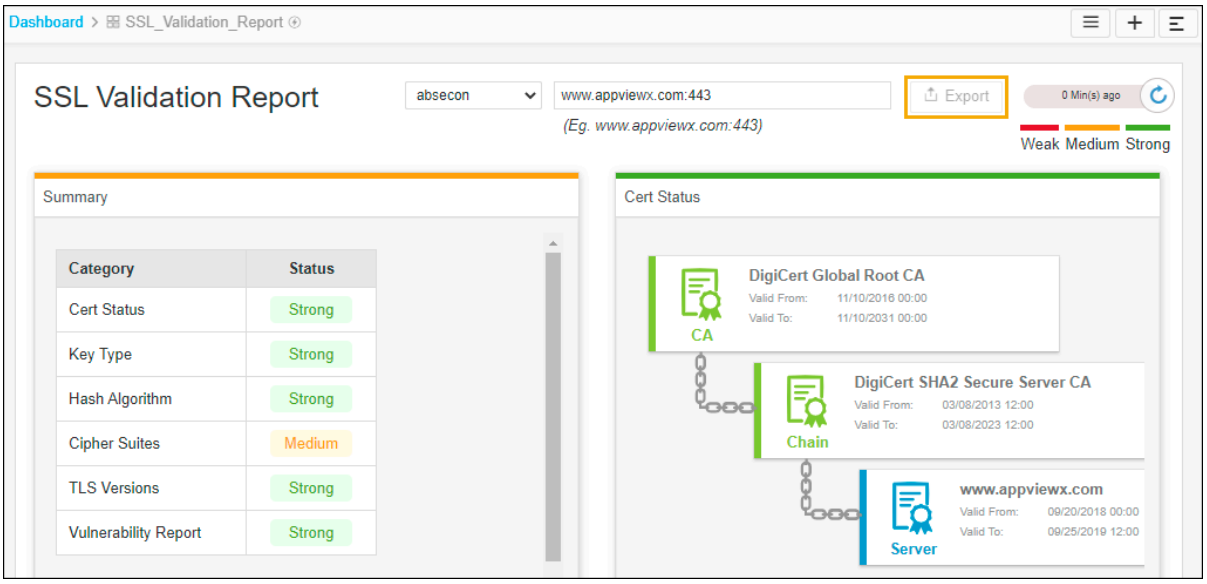
The **Cipher Suites - Server** report is available on the **Server Endpoint Security** dashboard.

Generating Application Score Reports

The application score report provides security scores of certificate parameters based on industry standards. You can get the score based on parameters such as Cert Status, Key Type, Hash Algorithm, CAA Record, TLS Version, and Vulnerability. Also, you can search for domains and check the security score. For example, you can check if the certificate name is valid through this report.

To generate application score reports:

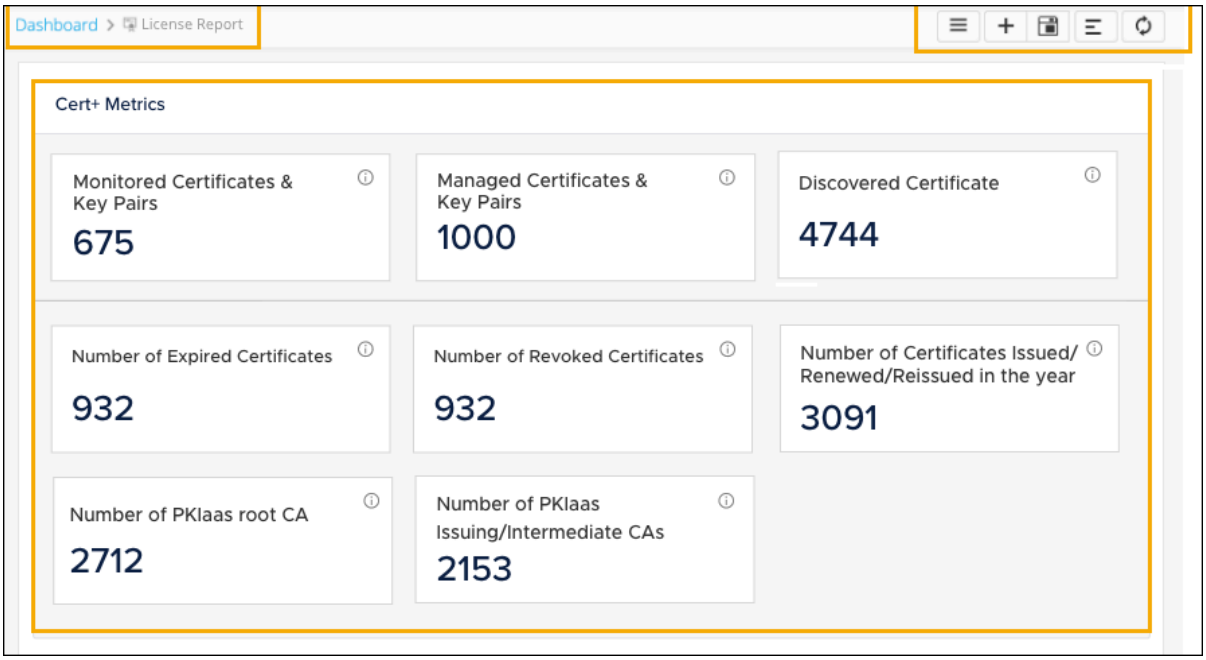
1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.
2. On the dashboard page, click **SSL Validation Report**.
3. Select a data center from the first dropdown.
4. In the search bar, enter a domain name (www.appviewx.com:443) and press **Enter**.
   The report is generated with the summary and all required parameters.
5. To export this report as a PDF, click **Export**.



License Report

The License Report dashboard displays the usage count of all the key metrics related to the license. It can be accessed from the Dashboard page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Options available on the License Report dashboard

Options	Descriptions
	Go to Dashboard page where all the Dashboards are listed.
	**Create** a dashboard/widget.
	**Save** the widget changes.
	**Align** the widgets within the dashboard.
	**Refresh** a dashboard.

Google 90 Day Dashboard

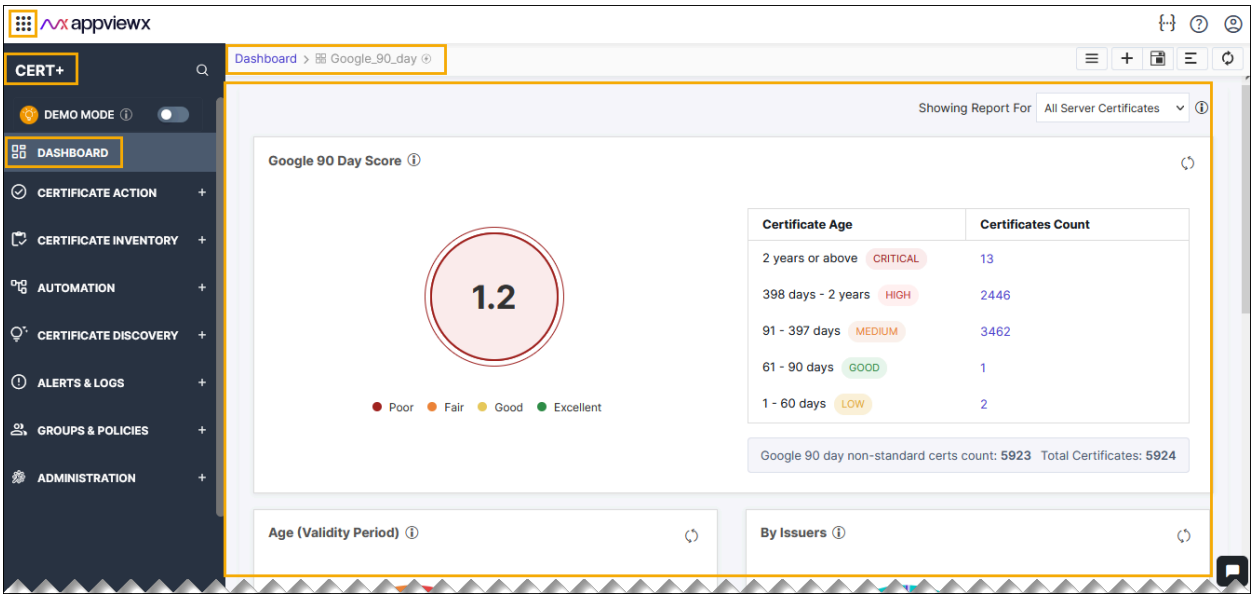
Overview

The Google 90-day certificate refers to Secure Sockets Layer (SSL) certificates issued by Certificate Authorities (CAs) in accordance with Google's guidelines on certificate validity periods. Certificates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

exceeding 398 days (approximately one year and one month) are considered insecure by Google. This policy encourages the adoption of shorter-lived SSL certificates, typically lasting 90 days, to enhance security and promote timely certificate renewal.

This dashboard displays the reports related to certificate scores, server certificate age, issuers, key algorithms, and key lengths, adhering to the guidelines set by Google for 90-day SSL certificates.



Benefits of Google 90 Day

- **Achieve Visibility**: Clear insight into certificates is crucial for effectively managing renewals and removals. Regular scanning aids in identifying existing certificates and uncovering new ones.
- **Monitor Expiry Dates**: Automation streamlines tracking and upkeep of certificate renewals by issuing timely alerts to relevant personnel. It also ensures proper provisioning and configuration of certificates, along with accurate binding to endpoints.
- **Enforce Encryption Standards**: Encryption forms the cornerstone of certificates, making it imperative to determine the appropriate encryption level to uphold infrastructure security. Analyzing certificates for indicators like key size, strength, or signing algorithms helps identify those utilizing insecure or outdated cryptographic standards.
- **Establish Governance**: While automation aids certificate management, it necessitates a foundational policy for enforcing Public Key Infrastructure (PKI) governance. This governance framework oversees data protection, user identity provisioning, and the security of end-to-end communications.
- **Secure Key Management**: Private keys serve as the ultimate safeguard for sensitive data, yet storing them in unprotected text files exposes them to exploitation. Utilizing encrypted software vaults or certified Hardware Security Modules (HSMs) offers superior protection, particularly if automated key rotation is enabled to periodically replace them.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

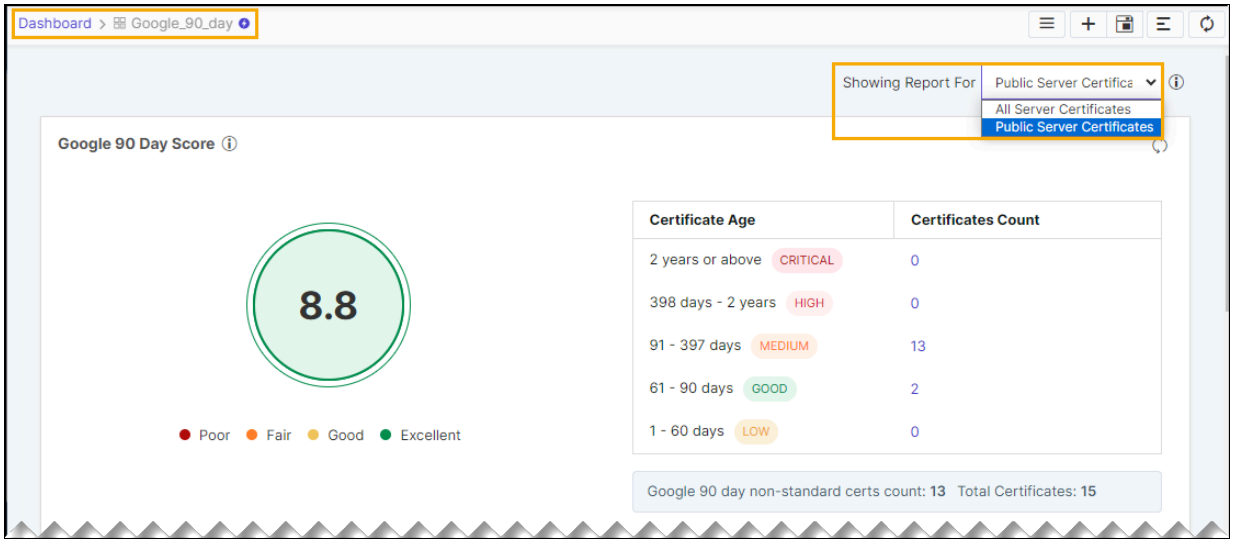
Showing Report For

The Google 90-day dashboard showcases two types of reports along with specific widgets:

- **All Server Certificates**: All Server Certificates refers to a category or group that includes all types of server certificates, regardless of their specific characteristics or attributes.

> **Note:** To access the report for the entire system, users must belong to the admin group with super access.

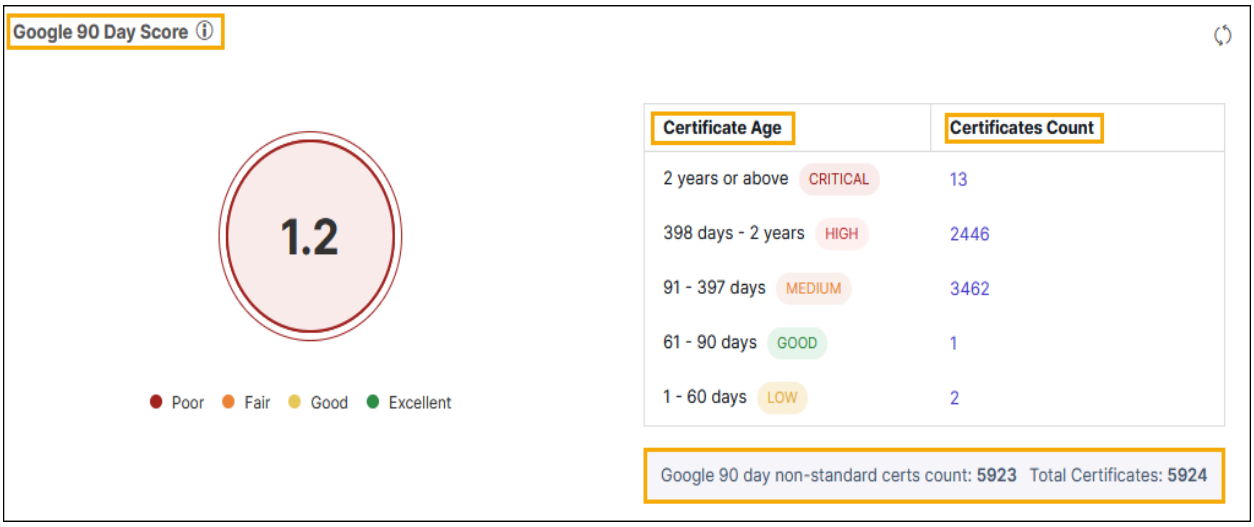
- **Public Server Certificates**: Certificates that have a trust chain consisting of a public root certificate and intermediate certificates are categorized as public certificates.



Google 90 Day Score

This report displays the score of certificate based on the certificate age and certificate count categorization on the single certificate validation time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Certificate Age: This report presents the severity status of certificates. A certificate includes a created date and an expiry date, and the number of days between these dates is referred to as the certificate age. The terms Validity Period and Certificate Age share the same definition. Following are the status based on age limit:

- 2 years or above - CRITICAL
- 398 days - 2 years - HIGH
- 91 - 397 days - MEDIUM
- 61 - 90 days - GOOD
- 1 - 60 days - LOW.

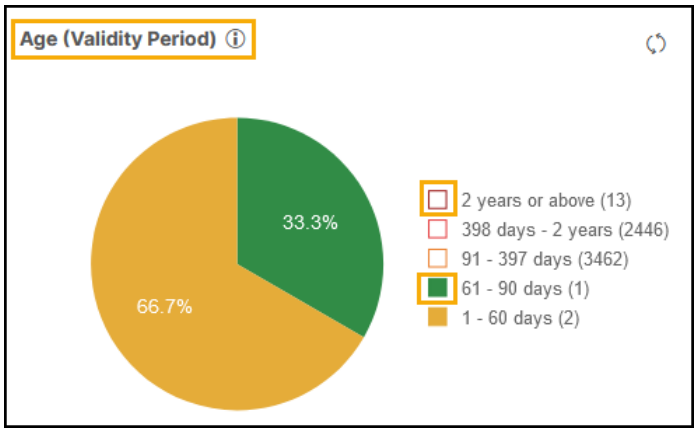
Certificates Count: The certificate count report displays the number of non-standard certificates. You can click on the count, which will redirect to the server certificate inventory.

Age (Validity Period)

The server certificates are grouped by validity in the Age (Validity Period) report, displays the different validity periods as shown on the image. The pie chart's colored sections represent the count and validity status of the certificates. You have the following options:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

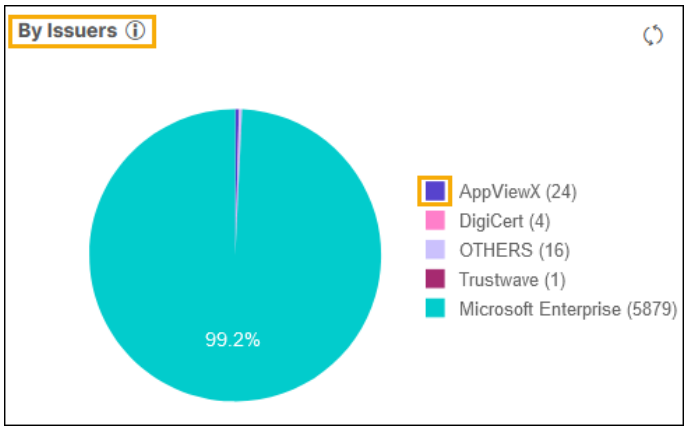
- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.



By Issuers

The server certificates are categorized by issuing vendors. The By Issuers report displays all the server certificates that are currently managed or monitored, excluding expired and revoked. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.

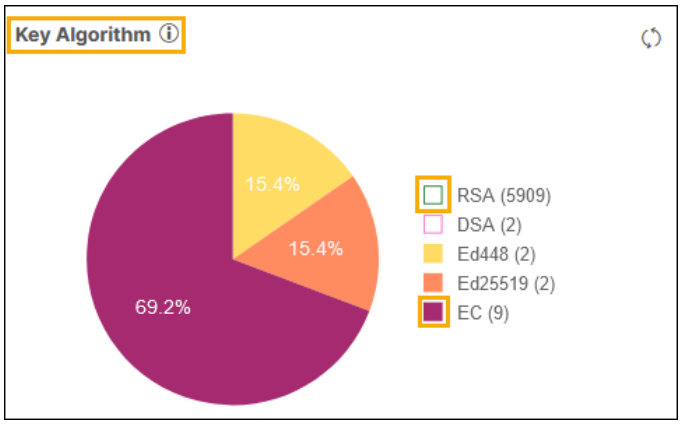


Key Algorithm

This report displays the count of server certificates by key algorithm. Different colored sections of the pie chart represent the count of server certificates based on the key algorithm. For instance, RSA (59), DSA (10), and so on. You have the following options:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

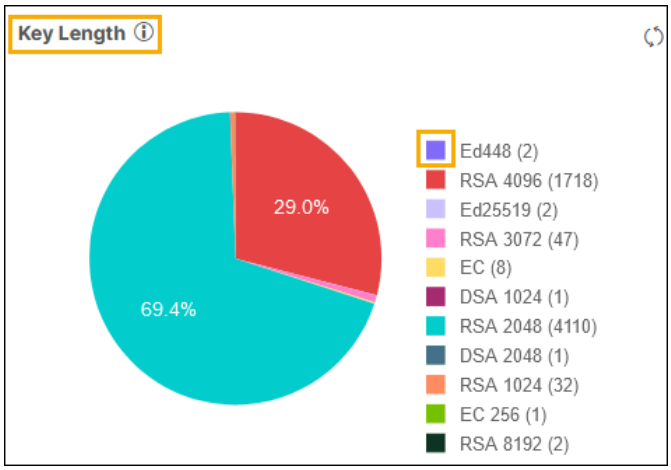
- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.



Key Length

This report displays the count of server certificates by key length. Different colored sections of the pie chart represent the count of server certificates based on the key length. For instance, RSA (59), DSA (10), and so on. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.



Searching for Dashboard, Object, or Widget

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Enter the search keyword in the search field, and then press **Enter**.
   The dashboards, objects, or widgets that match with the specified keyword are displayed.

Deleting a Dashboard

The default dashboard cannot be deleted from the AppViewX platform. Only the customized dashboard can be deleted and deleting the dashboard includes the deletion of all the widgets on the dashboard also.

To delete a dashboard,

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.
2. Select the checkbox corresponding to the dashboard you want to delete.
3. From the command bar, click  .
4. In the **Confirmation** dialog box, click **Yes**.

> **Important:** Deleting a dashboard will delete all the widgets displayed for the dashboard.

Alerts and Logs

- Overview
- Certificate Alerts
- Configuring Expiry Alerts
- Configuring a Certificate Expiry Alert
- Configuring a Certificate Sync Alert
- Configuring a Certificate Validation Alert
- Configuring a Connection Failure Alert
- Certificate Logs
- Export Certificates Logs

Overview

CERT+ allows you to monitor the AppViewX component level and certificate-related alerts in a dashboard with predefined filters. Also, you can configure alerts based on your business needs. With these alerts,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

you can trigger an email with the necessary information. To run a custom logic based on the alert condition, you can configure it through a visual workflow in AppViewX. Alerts and logs help you to ensure the system performance is monitored.

You can view logs and receive certificate alerts through,

- Certificate Logs
- Certificate Alerts

Certificate Alerts

Certificate Alerts helps you with alerts that are related to certificates. You can configure these alerts based on certificate events such as sync, validation, or expiry. Any certificate-related actions performed in your application are captured as logs. Also, you can notify users of a specific certificate action through these alerts.

To verify certificate alerts,

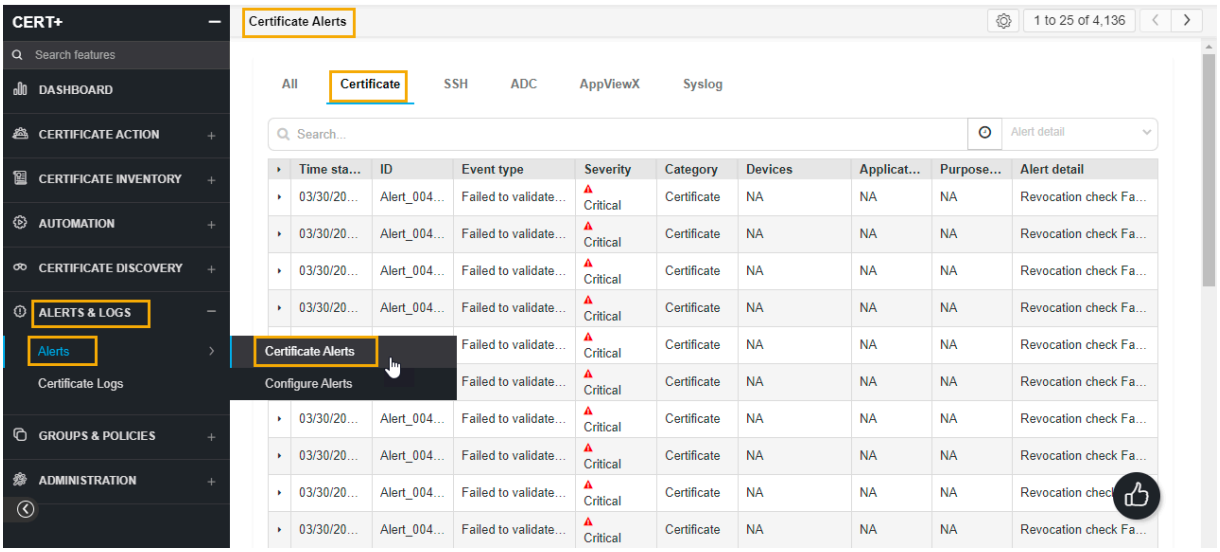
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **ALERTS & LOGS**.
5. Click **Alerts**, and then select **Certificate Alerts**.

   The **Certificate Alerts** screen appears.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. On the Certificate Alerts list view page, you can find the list of alerts related to the certificates. Any actions performed on the certificates are captured under this list view.
7. You can search for alerts based on the Alert ID, Alert Event type, Severity, Category, Devices, Applications, and Alert detail.
8. On the alert screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

Configuring Expiry Alerts

Digital certificates are issued with a validity period predefined by the certificate authorities. When a certificate outgrows this validity period, it is no longer trusted and the services consuming the certificate are considered broken.

AppViewX lets you create certificate expiry alerts, which are proactive notifications to customers to renew the certificates that are due for expiry.

The alerts are primarily created based on the period of certificate expiry (certificates expiring on a specific date, certificates expiring after x number of days, and so on). The emails also include a certificate renewal link, thus simplifying the CLM process.

The following sections list the prerequisites for configuring the expiry alerts and the configuration steps.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Configuring Certificate Expiry Alerts over Email
• Configuring Certificate Expiry Alerts over ITSM
• Disabling Expiry Alerts Manually

Configuring Certificate Expiry Alerts over Email

Before configuring certificate expiry alerts over emails, **ensure that permissions to create and modify the expiry alerts are assigned to the required role(s)**.

Note: Certificate renewal is allowed only for users having read and write permission to the certificate group. Ensure that you assign permissions accordingly.

1. To do this, follow the instructions given here and enable **Expiry Alerts** under **Authorized Functions** > **CERT+**.
2. Modify the resource mapped to this role to assign the following workflow requests (**Access Control** > **Workflow Requests**) to the resource:
   - **Cert_Expiry_Mail_Individual**
   - **Cert_Expiry_Mail_Bulk**

To configure certificate expiry alerts over email:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Expiry Alerts**.
   The expiry alerts inventory is displayed.
2. To create a new email expiry alert, click **+ Create**.
   The **ExpiryAlert > Expiry Alert Add** page is displayed.

   Tip: This page has a list of best practices you are advised to follow when creating a new expiry alert.

3. For the new alert, enter a unique **Alert Name** (mandatory) and a description (optional) with additional details about the alert.
4. In the **Alert Configuration** section, click **+ Add**.
   The **Add Configuration** pane is displayed.
5. Select the **Certificate Type** for which you want to configure the expiry alert.
   - **End Certificate**
   - **CA Certificate**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Enter/Select the **Filter Configuration** details.

Field descriptions for the Filter Configuration section

Field	Description
Certificate Expiry Period*	To filter certificates based on their expiry, • Range in days: Select this option to send an expiry alert email for certificates that will expire in the range of number days specified. For example, to set an alert for certificates that will expire between 10 to 40 days from today, enter **10** in the field before **to** and enter **40** in the field after **to**. • **On specified days**: Select this option to send an expiry alert email for certificates that will expire after x number of days from today. For example, to send an alert for certificates expiring on the 50th day days from today, enter **50**. • **Range in dates**: Select this option to send an expiry alert for all certificates expiring in a specific duration. Use the calendar widget to select the **Start date** and **End date** of this duration.
Additional Filters	To add a filter in addition to the certificate expiry period: a. Select the required filter from the **Select option** dropdown list. b. Enter/select the corresponding value in the **Type to enter value** field. c. Click **Add**. The selected filter option and its value are displayed.
***Notification Method**	To send an expiry alert over email, select **Email**. **Note:** For instructions on sending an expiry alert over an ITSM tool (ServiceNow/JIRA), click here.
Allow certificate renewal	**Note:** This field is displayed only when **Notification Method** = **Email**. To trigger individual emails for each certificate that matches the filter criteria along with a renewal and unsubscribe link for the certificate, enable this button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Ignore renewed certificate	To stop alerts for certificates that have already been renewed, enable this button.
***ITSM Tool**	**Note:** This field is displayed only when **Notification Method** = **Others**. From the following options in the dropdown list, select a tool to raise a ticket for the alert: • **ServiceNow** • **JIRA**
Notification Format*	**NOTE**: This field is displayed when **Allow certificate renewal** is disabled. (Instead of emails for individual certificates, you will now receive a notification with a bulk of certificates in your chosen format.) • **Attachment**: A CSV file with details of all certificates due to expire will be attached to the alert email. • **Email Body**: A table with details of all certificates due to expire will be included in the body of the alert email.
Ignore renewed certificate	When this field is enabled, results returned after the alert is triggered will not include certificates that have already been renewed, even though they match the filter criteria.

7. Enter/Select the **Email Configuration** details.

Field descriptions for the Email Configuration section

Field	Description
To*	
Recipient(s)	Enter the recipient(s) email address. You can enter a maximum of 20 email addresses, separated by a comma.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Parameter(s)	To add more recipients for the alert email, you can retrieve email addresses from the following certificate parameters: • Subject Email • SAN (rfc822) • Certificate Group From the dropdown list, select the required parameter(s).
Certificate Attribute(s)	To add more recipients for the alert email, you can retrieve email addresses from any certificate attribute that has the email ID as its value, for example, **Cert Owner**. From the dropdown list, select the certificate attribute.
CC	
Recipient(s)*	Enter the email address of stakeholders who are to receive a copy of the expiry alert email.
Certificate Parameter(s)	To add more recipients to the CC field in the alert email, you can retrieve email addresses from the following certificate parameters: • Subject Email • SAN (rfc822) • Certificate Group From the dropdown list, select the required parameter(s).
Certificate Attribute(s)	To add more recipients to the CC field in the alert email, you can retrieve email addresses from any certificate attribute that has the email ID as its value, for example, **Cert Owner**. From the dropdown list, select the certificate attribute.
Email Subject	
Subject*	Enter the subject line for the expiry alert email using the following (recommended) format: **Expiry Alert :: |Common Name| certificate| expiring on |Valid Until|**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The full list of placeholders and their corresponding values is given here.
Email Body	
Body*	Enter the body text for the email using the following (recommended) format: The list of placeholder that can be used in the Subject <list and it's value> **Certificate with Common Name |Common Name|** **Serial number |Serial Number|** **issued by |Issuer Common Name|** **is about to expire on |Valid Until|** **Note:** The full list of placeholders and their corresponding values is given here.

8. Click **Add**.
   The created alert is listed in the table below the **+ Create** button.

   Tip: To edit/delete an alert, use the **Edit**/**Delete** button, as required.

9. Under **Alert Execution Type**:

   Note: The settings configured here will be applicable to all expiry alerts listed in the above table.

   a. To trigger the alert immediately, select **Run Now** and click **Save**.

   OR

   a. To trigger the alert at a scheduled time, select **Schedule** and enter/select the following details:
      - **Time Zone***
      - **Frequency** (daily/weekly/monthly/yearly)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Starts On***
- **Ends**
  - For ends **ON**, use the calendar widget to select the date on which the last expiry alert email will be sent.
  - For ends **After**, enter the number of **Occurrences** after which the expiry alert will be discontinued.

10. Click **Save**.

    Once the expiry alerts are configured with **Allow certificate renewal option**, the individual certificate renewal email will be sent to the stakeholders with two links:

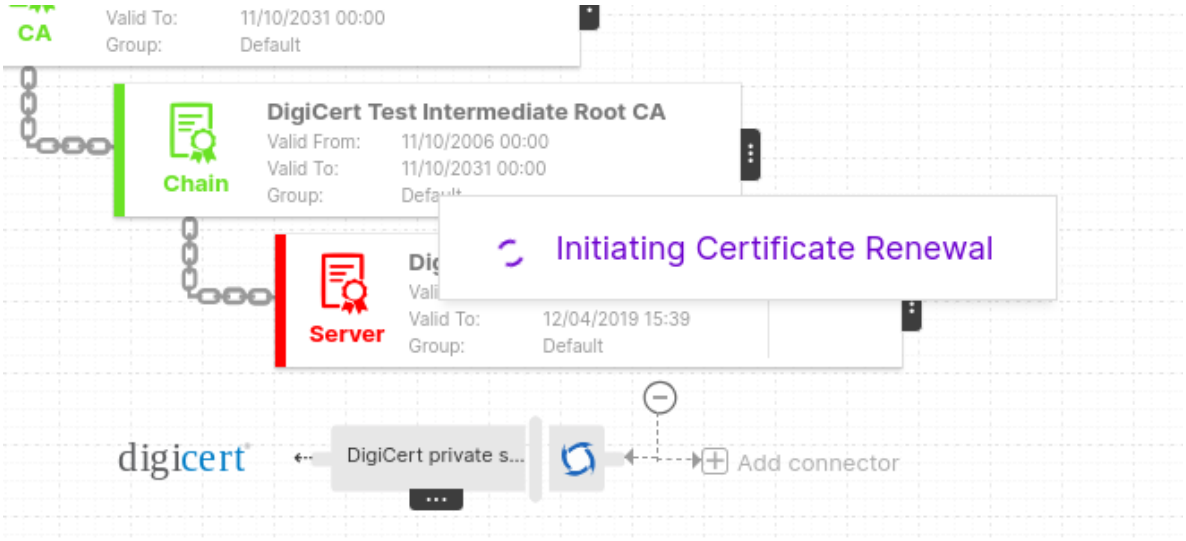
    - Link for certificate renewal
    - Link for unsubscribing from the alerts for that specific certificate

> **Tip:** You can repeat steps **4** to **9** to add more than one **Alert Configuration** under a **Alert Name**.

11. To renew the certificate:

    a. Click on the renewal link and login to AppViewX.

    You will be redirected to the holistic view for the certificate and the following renewal alert will be displayed:



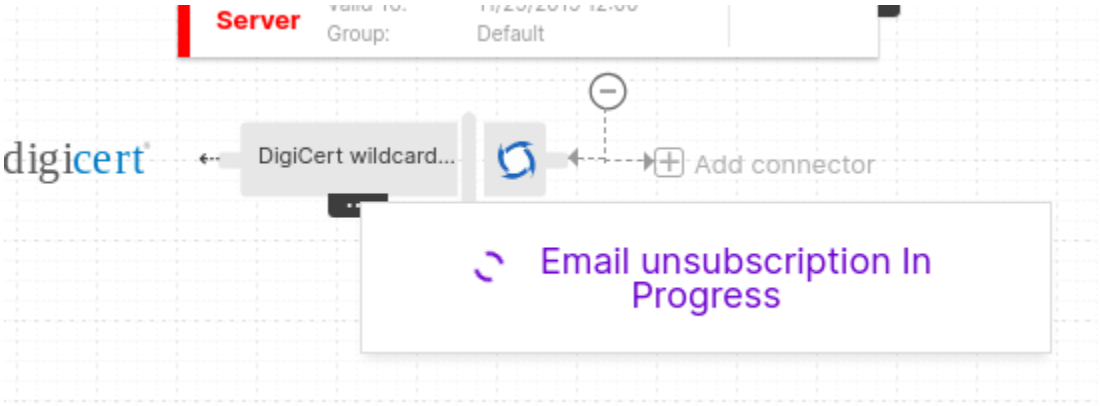
    b. For instructions on how to renew a certificate, refer to the documentation for renewing a certificate.

    To unsubscribe from the alerts for the certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. Click the unsubscribe link from the alert email.

You will be redirected to the certificate inventory page and the following unsubscribe alert will be displayed:



- Placeholders for Email Subject and Body
- Use Cases for Configuring Expiry Alerts

Placeholders for Email Subject and Body

To retrieve the parameter value (on the left) in the email body/subject, you can use the following corresponding placeholders (on the right):

```
"common name" : "commonName",
    "country" : "country",
    "state" : "state",
    "location" : "location",
    "division" : "division",
    "organization" : "organization",
    "subject" : "subject",
    "mail address" : "mailAddress",
    "serial number" : "serialNumber",
    "valid from" : "validFrom",
    "valid until" : "validUntil",
    "directory names" : "enhancedSANTypes.directoryNames",
    "rfc822 names" : "enhancedSANTypes.rfc822Names",
    "registered IDs" : "enhancedSANTypes.registeredIDs",
    "uniform resource identifiers" : "enhancedSANTypes.uniformResourceIdentifiers",
    "dns names" : "enhancedSANTypes.dnsnames",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"ip addresses" : "enhancedSANTypes.ipaddresses",
"ucc" : "enhancedSANTypes.ucc",
"fqdn" : "enhancedSANTypes.fqdn",
"other names" : "enhancedSANTypes.otherNames",
"upn" : "enhancedSANTypes.upn",
"issuer common name" : "issuer.commonName",
"issuer certificate authority" : "issuer.certificateAuthority",
"issuer setting name" : "issuer.settingName",
"issuer serial number" : "chainIdentifier.issuerSerialNumber",
"certificate group name" : "certificateGroup.name",
"vendor" : "certAssociations.vendor",
"device name" : "deviceDetails.deviceName",
"source" : "certAssociations.source",
"applications" : "certAssociations.applications",
```


Use Cases for Configuring Expiry Alerts

- Use Case 1
- Use Case 2
- Use Case 3

Use Case 1

Objective: Application owners want to configure alerts specific to their application.

Alert Criteria 1: Bulk notification

Instructions to configure an expiry alert for alert criteria 1

Alert Criteria 2: Individual certificate notification (recommended)

Instructions to configure an expiry alert for alert criteria 2

- Configuring an Expiry Alert for Alert Criteria 1
- Configuring an Expiry Alert for Alert Criteria 2

Configuring an Expiry Alert for Alert Criteria 1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 1 configuration

Alert parameter	Value
Range in days	20 - 30
Filter	Certificate group < select the application group>
Notification Format	Attachment
To	< Recipient as application group email ID > Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid From , Valid Until

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 1 configuration

Alert parameter	Value
Range in days	0 - 10
Subject	Expiry Alert :: Certificates Expiring in 10 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring an Expiry Alert for Alert Criteria 2

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 2 configuration

Alert parameter	Value
Range in days	20 - 30
Allow Users Renewal	Enabled
Filter	Certificate group < select the application group>
To	< Recipient as application group email ID > Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 2 configuration

Alert parameter	Value
Range in days	0 - 10
Subject	Expiry Alert : Critical : |Common Name| certificate is expiring on |Valid Until|
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Use Case 2

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Objective: The PKI team will receive the alerts and take remediation action, following up with the application owners. The PKI team will get a list of certificates expiring on the 30th day from the day of alert configuration and must then consult with the application owners. Reminders for certificates missing from remediation for 20 days should be part of a critical alert condition.

Alert Criteria 1: Bulk notification (recommended)

Instructions to configure an expiry alert for alert criteria 1

Alert Criteria 2: Individual certificate notification

Instructions to configure an expiry alert for alert criteria 2

- Configuring an Expiry Alert for Alert Criteria 1
- Configuring an Expiry Alert for Alert Criteria 2

Configuring an Expiry Alert for Alert Criteria 1

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 1 configuration

Alert parameter	Value
On specified days	30
Filter	Certificate group < select the application group>
Notification format	Attachment
To	< PKI Admin > Certificate group : <select the application group>
CC	<Certificate group>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid from , Valid Until, Issuer Common Name

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 1 configuration

Alert parameter	Value
On specified days	10
Subject	Expiry Alert :: Certificates Expiring in 10 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring an Expiry Alert for Alert Criteria 2

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 2 configuration

Alert parameter	Value
On specified days	30
Allow Users Renewal	Enabled
Filter	Certificate group < select the application group>
To	< Recipient PKI Admin > Certificate group : <select the application group>
CC	<Certificate group>
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until| for the group |Certificate Group|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 2 configuration

Alert parameter	Value
On specified days	10
Subject	Expiry Alert : Critical : |Common Name| certificate is expiring on |Valid Until| for the group |Certificate Group Name|
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Use Case 3

Objective: The administrator wants to send expiry alerts for certificates expiring in the next 30 days to all the application owners (who will take remedial action on their respective certificates). The administrator also wants to send a critical reminder to the application owners if an action has not been taken in the next 15 days.

Alert Criteria 1: Bulk notification

Instructions to configure an expiry alert for alert criteria 1

Alert Criteria 2: Individual certificate notification

Instructions to configure an expiry alert for alert criteria 2

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Configuring an Expiry Alert for Alert Criteria 1
• Configuring an Expiry Alert for Alert Criteria 2

Configuring an Expiry Alert for Alert Criteria 1

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 1 configuration

Alert parameter	Value
Range in days	0 - 30
Allow user Renewal	Enabled
To	Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|
Alert execution type	Scheduled; everyday from the day of alert configuration

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 1 configuration

Alert parameter	Value
Range in days	0 - 15
Subject	Expiry Alert :: Certificates not taken action for past 15 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring an Expiry Alert for Alert Criteria 2

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert critera 2 configuration

Alert parameter	Value
Range in days	0 - 30
Notification Format	Attachment
To	Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid From , Valid Until, Issuer Common Name
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert critera 2 configuration

Alert parameter	Value
Range in days	0 - 15
Subject	Expiry Alert :: Certificates not taken action for past 15 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Certificate Expiry Alerts over ITSM

Important: Expiry alerts over email can be configured for end certificates as well as CA certificates. Expiry alerts over ITSM channels can be configured only for end certificates.

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Expiry Alerts**.
   The expiry alerts inventory is displayed.
2. To create a new ITSM expiry alert, click **+ Create**.
   The **ExpiryAlert > Expiry Alert Add** page is displayed.

   Tip: This page has a list of best practices you are advised to follow when creating a new expiry alert.

3. For the new alert, enter a unique **Alert Name** (mandatory) and a description (optional) with additional details about the alert.
4. In the **Alert Configuration** section, click **+ Add**.
   The **Add Configuration** pane is displayed.
5. From the **Certificate Type** field, select **End Certificate**.
6. Enter/Select the **Filter Configuration** details.

Field descriptions for the Filter Configuration section

Field	Description
Certificate Expiry Period*	To filter certificates based on their expiry, • Range in days: Select this option to send an expiry alert email for certificates that will expire in the range of number days specified. For example, to set an alert for certificates that will expire between 10 to 40 days from today, enter **10** in the field before **to** and enter **40** in the field after **to**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **On specified days**: Select this option to send an expiry alert email for certificates that will expire after x number of days from today. For example, to send an alert for certificates expiring on the 50th day days from today, enter **50**. • **Range in dates**: Select this option to send an expiry alert for all certificates expiring in a specific duration. Use the calendar widget to select the **Start date** and **End date** of this duration.
Additional Filters	To add a filter in addition to the certificate expiry period: a. Select the required filter from the **Select option** dropdown list. b. Enter/select the corresponding value in the **Type to enter value** field. c. Click **Add**. The selected filter option and its value are displayed.
***Notification Method**	To send an expiry alert over ITSM, select **Others**.
Ignore renewed certificate	When this field is enabled, results returned after the alert is triggered will not include certificates that have already been renewed, even though they match the filter criteria.
***ITSM Tool**	**Note:** This field is displayed only when **Notification Method** = **Others**. From the following options in the dropdown list, select an ITSM tool to raise a ticket for the alert: • **ServiceNow** • **JIRA**

7. To receive expiry alerts on **ServiceNow**:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. From the following options, select the **Configuration Type**:
   - **Basic**: Create a ticket by specifying the minimum details in the **Configuration** section.
   - **Advanced**: Based on the organization policy, fill the required values for a ticket using a JSON. In this case, a JSON editor will replace the **Configuration** section. The JSON is editable and can be customized as per requirement.

b. From the following options, select the **Issue Type**:
   - **Incident** (Tickets will be listed on the **Incidents** page)
   - **Service Request** (Tickets will be listed on the **My requests** page)

c. Enter/select the **Configuration** details.

Field description for Incident requests

Field	Description
Short Description*	Enter a title/short description for the ticket.
Description*	Enter a detailed description of the incident event here (for example, certificate details and operation links).
Urgency*	From the dropdown list, select the urgency level of the incident.
Impact*	From the dropdown list, select the impact level of the incident.
Assignment Group*	Enter the name of the group this incident will be assigned to.

Field description for Service Requests

Field	Description
Short Description*	Enter a title/short description for the ticket.
Description*	Enter a detailed description of the incident event here (for example, certificate details and operation links).
Priority*	From the dropdown list, select the priority assigned to the incident.
Assigned to*	Enter the name of the user this incident will be assigned to.
Due Date*	Using the calendar widget, select a due date for the ticket.

d. Click **Validate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

OR

To receive expiry alerts on **JIRA**:

a. From the following options, select the **Configuration Type**:
- **Basic**: Create a ticket by specifying the minimum details in the **Configuration** section.
- **Advanced**: Based on the organization policy, fill the required values for a ticket using a JSON. In this case, a JSON editor will replace the **Configuration** section. The JSON is editable and can be customized as per requirement.

b. Enter/Select the **Configuration** details.

Field descriptions for the Configuration details

Field	Description
Project Id*	Enter the unique identifier of the project in JIRA under which the JIRA ticket will be created.
Issue Type*	From the dropdown list, select the type of JIRA issue.
Summary*	Enter a title/short description for the JIRA ticket.
Description	Enter additional details related to the ticket here.
Priority*	From the dropdown list, assign a priority to the ticket.
Reporter	Enter the name of the user who reported the issue.
Assignee*	Enter the name of the user to whom this JIRA ticket will be assigned.

c. Click **Validate**.

8. Click **Add**.
The created alert is listed in the table below the **+ Create** button.

Tip: To edit/delete an alert, use the **Edit**/**Delete** button, as required.

9. Under **Alert Execution Type**:

Note: The settings configured here will be applicable to all expiry alerts listed in the above table.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. To trigger the alert immediately, select **Run Now** and click **Save**.

OR

a. To trigger the alert at a scheduled time, select **Schedule** and enter/select the following details:
   - **Time Zone***
   - **Frequency** (daily/weekly/monthly/yearly)
   - **Starts On***
   - **Ends**
     - For ends **ON**, use the calendar widget to select the date on which the last expiry alert email will be sent.
     - For ends **After**, enter the number of **Occurrences** after which the expiry alert will be discontinued.

10. Click **Save**.

    Once the expiry alerts are configured with **Allow certificate renewal option**, the individual certificate renewal email will be sent to the stakeholders with two links:
    - Link for certificate renewal
    - Link for unsubscribing from the alerts for that specific certificate

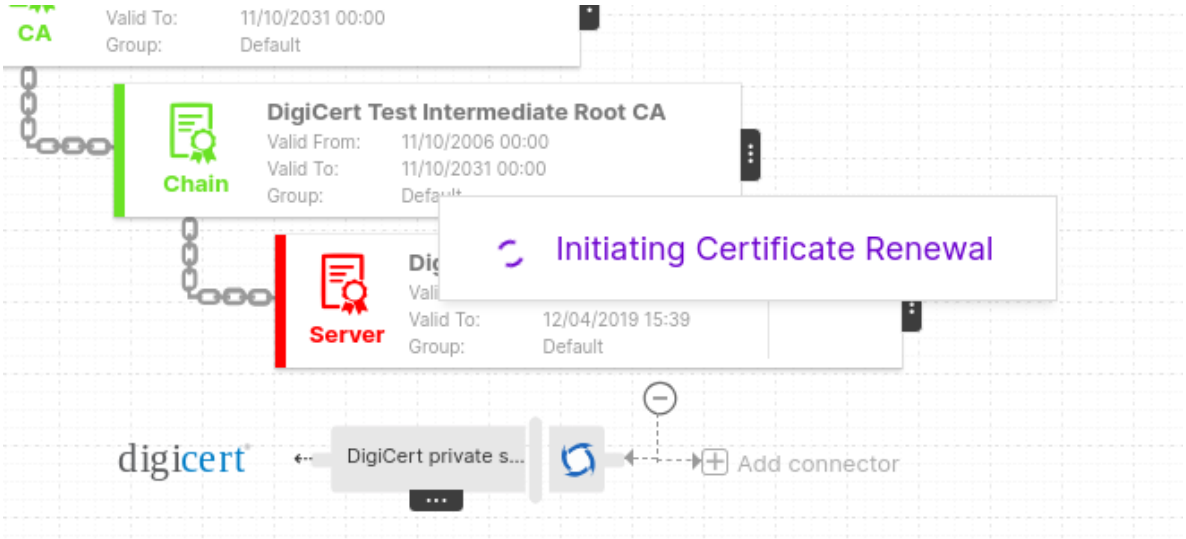
> **Tip:** You can repeat steps **4** to **9** to add more than one **Alert Configuration** under a **Alert Name**.

11. To renew the certificate:

    a. Click on the renewal link and login to AppViewX.

    You will be redirected to the holistic view for the certificate and the following renewal alert will be displayed:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



b. For instructions on how to renew a certificate, refer to the documentation for renewing a certificate.

Disabling Expiry Alerts Manually

1. Go to the certificate inventory and click the common name of the certificate that you want to disable the alerts for.
2. Set the **Expiry Alert** field to **False**.

Configuring a Certificate Expiry Alert

Certificate expiry alerts are sent to designated recipients for all certificates that are set to expire on the date specified on the Settings: Certificate expiry alert screen.

To configure a certificate expiry alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. Hover on **Alerts**, and then select **Configure Alerts**.
3. Enter a name for the certificate alert.
4. In the Event Type field, select Certificate Expiry Alert.
5. Select Critical as the severity of the alert.
6. Select the Certificate Category from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. In the Expires in (days) field, enter the number of days before a certificate expires. An alert will be sent out.
8. To use Email Configuration to send the alert, complete the following steps:
   - Select the Email Configuration checkbox.
   - In the Email Address field, enter the email addresses you want to send the alert to. Use commas to separate the addresses.
   - In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.
9. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
   - Enter the Destination IP for the alert.
   - Select the version of SNMP you want to use: V1 or V2.
   - Enter the port that should be used for the alert.
10. Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
11. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Sync Alert

AppViewX maintains a record of what certificate is mapped to which Server:Application service, which can be seen on the certificate's holistic view. This information is used by AppViewX to monitor continued existence of the certificate on Server:Application. AppViewX establishes connectivity to the Server and validates if the Application is still configured with the Certificate. Any change in the status is flagged out as a Certificate Sync Alert. This can also be visualized through the change of Application Connector status color. The Application Connectors on the Certificate's holistic view will turn Red in such circumstances.

To configure a certificate sync alert:

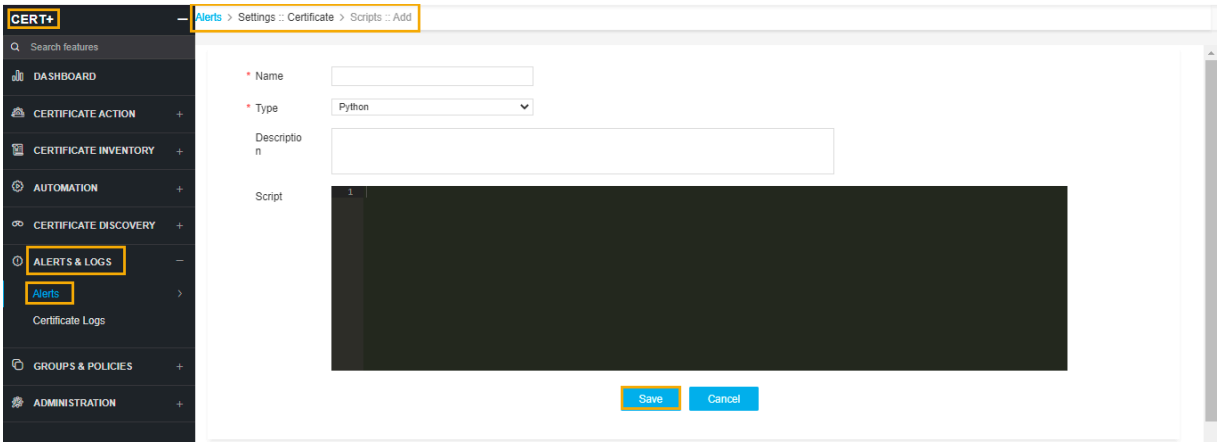
1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. In the **Event Type** field, select Certificate Sync Alert.
3. Enter/Select the alert details.

Field	Decription
***Alert name**	Enter a unique name for the alert.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Decription
***Event type**	From the dropdown list, select **Certificate Sync Alert**.
***Vendor**	From the dropdown list, select the vendor for the alert criteria.

4. Enter a name for the certificate alert.
5. Select the Alert severity of the alert: Critical, Major, and Notification.
6. In the Alert Message field, enter the text that users see when the alert appears on the screen.
7. Select the Vendor whose device or application you are creating an alert for.
8. Select the Certificate Category from the dropdown list.
9. In the Device Name field, select the device associated with the certificate you are creating an alert for.
10. In the Application field, select the application associated with the certificate you are creating an alert for.
11. Select the Execute Script checkbox.
12. In the Execute Script dropdown list, select the script to trigger the alert. To create a script, click the (Add new script) icon. The below page appears.



- Provide value in the Name field.
- Type by default is selected as Python.
- Provide description value in the Description field.
- Enter the script to be executed in the Script field and click **Save**.

13. To use the Email Configuration to send the alert, complete the following steps:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Select the Email Configuration checkbox.
- In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.
- In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.

14. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
    - Enter the Destination IP for the alert.
    - Select the version of SNMP you want to use: V1 or V2.
    - Enter the port that should be used for the alert.
    - Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
15. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Validation Alert

AppViewX acts as a repository of all the known certificates in the organization. A certificate identifies a application via its Subject Common Name. In many a circumstance it observed that the organizations faces certificate related outages even if the certificate is valid. This is because of an error while setting up the application configuration or invalid certificate selected for the application. To identify such a misconfiguration AppViewX periodically validates the identity of application but trying and establishing connectivity to the Subject Common Name of server certificates in the Inventory. If the certificate is exchanged as part of SSL handshake is found to be invalid through expiry, revocation or through misconfiguration, AppViewX triggers a Certificate Validation Alert to notify administrators about a SSL handshake issue that users could be facing.

To configure a certificate validation alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. In the **Event Type** field, select **Certificate Validation** Alert.
3. Enter a name for the certificate alert.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Select the severity of the alert: Critical, Major, or Notification.
5. In the Alert Message field, enter the text that users see when the alert appears on the screen.
6. Select the Vendor whose device or application you are creating an alert for.
7. Select the Certificate Category from the dropdown list.
8. In the Device Name field, select the device associated with the certificate you are creating an alert for.
9. In the Application field, select the application associated with the certificate you are creating an alert for.
10. To use the Email Configuration to send the alert, complete the following steps:
    - Select the Email Configuration checkbox.
    - In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.
    - In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.
11. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
    - Enter the Destination IP for the alert.
    - Select the **version** of SNMP you want to use: V1 or V2.
    - Enter the port that should be used for the alert.
    - Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
12. Click **Add** to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Connection Failure Alert

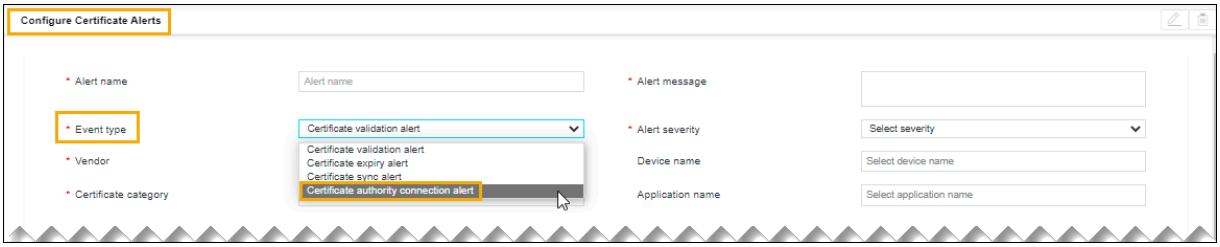
When a certificate is enrolled with AppViewX, a connection is established between the Certificate Authority (CA) signing the certificate. This connection is vital to perform CLM actions and certificate discovery tasks seamlessly.

When you can check manually if the connection is successfully established between AppViewX and certificate authority, and continues to stay so, starting version 2021.1.0, AppViewX allows you to configure automatic alerts when this connection fails. These alerts will be recorded in AppViewX logs as well as sent as email notifications.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To configure a connection failure alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. Enter an **Alert name**.
3. From the **Event type** dropdown list, select **Certificate authority connection alert**.





4. From the **Certificate Authority Settings** dropdown list, select the CA Account
5. Set the **Alert severity** to critical.
6. To configure email alerts, in the **Email configuration** section, enter the **Email address** that will receive the email notifications in the event of a connection failure.
7. Enter the relevant subject in the **Subject** field.
8. To use the Simple Network Management Protocol (SNMP) for sending the alerts:
   a. Enter the **Destination IP** address for the alert.
   b. Select the SNMP **version** to be used.
   c. Enter the **Port** number to be used for the alert.
   d. Enter the **Community string** for the alert.

      The string is similar to a user ID or password and allows users to access the requested information on the device.
9. Click **Add** to create the alert.
   The new alert is now listed in the **Certificate Alerts** page.
10. Click **Reset** if you want to re-enter the details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Logs

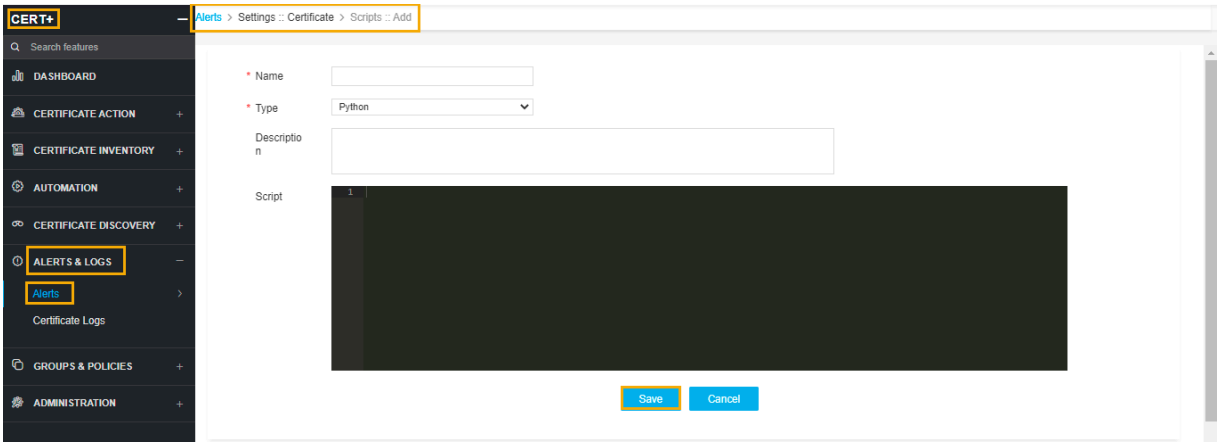
Logs keep track of all activities that take place within AppViewX or any external entity that is connected to the AppViewX system. The Logging functionality in AppViewX tracks user activities and creates the device and object-level event logs. Certificate Logs helps you with logs that are related to certificates. Any system or certificate-related actions performed in the application are captured as logs. With these logs, you can check the system performance and it helps you with audit purposes to meet industry standards.

To check logs,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

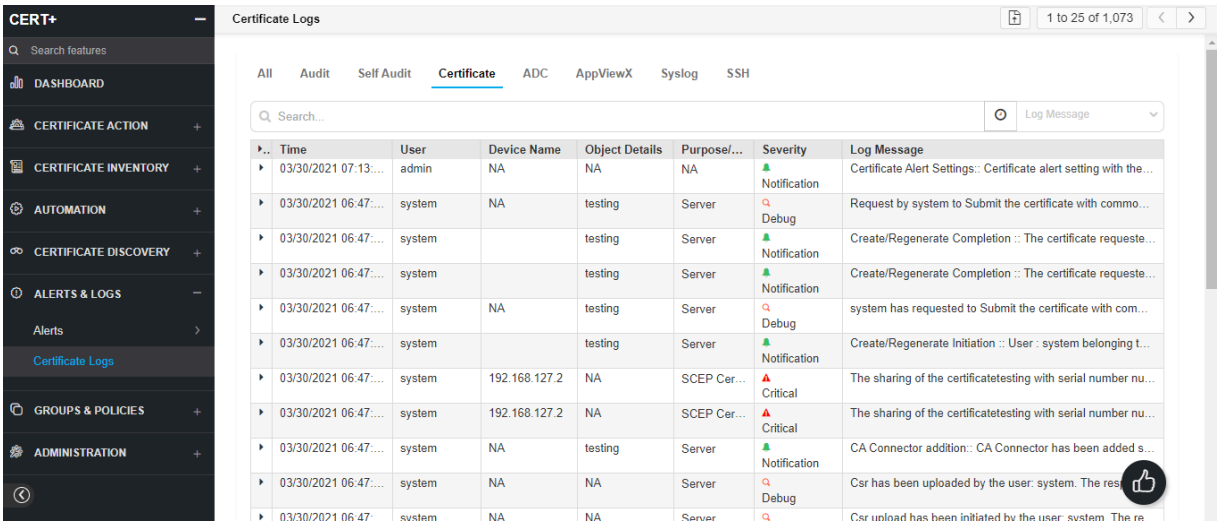
   The left navigation pane appears.
3. Click **CERT+**.

   The CERT+ left navigation pane appears Logging



4. Under the section Alerts & Logs, select Certificate Logs.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. On the Certificate logs list view page, you can find the list of logs related to the certificates. Any actions performed on the certificates are captured under this list view.
6. You can search for logs based on the time, user, device name, object details, and severity.
7. You can also filter logs based on the date and time and through the Log Message filter.
8. On the log screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

Export Certificates Logs

When exporting logs in AppViewX, you can export all of the logs of a given type-for example, all Configure files or all Audit files-or you can search for specific logs or filter the default log list using the Date Range and Log Detail fields and then export only the logs that remain.

To export a logging report:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Certificate Logs**.
   The **Certificate Logs** page is displayed.
2. At the top of the Logging screen, click the tab for the type of logs you want to export: Certificate (in this case).
3. (Optional) Run a search for specific logs or filter the default list using the Date Range and/or Log Detail fields in the Search bar.
4. Click the export button in the Command bar in the top-right corner of the page.
5. The log report is then downloaded as a tar.gz file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Standard Practices

- PKI Standard Practices
- CLM - Best Practices
- Standard Practices followed in the Certificate Inventory Management
- Securing CERT+

PKI Standard Practices

Offline Root CA

- The root CA should never be connected to the network or to the domain and no fingerprint of the server should ever be recorded since the root key compromise will impact the entire PKI hierarchy.
- Root CAs should always stay offline and shut down except when signing the Issuing CA certificates and during root CRL publish.
- Access to the Root CA to sign the Issuing CA request should be initiated in an agreed and controlled workflow so as to not compromise the Root CA in any means.
- Once the Issuing CA certificate has been issued and Root CRL published the Root CA should be turned off.
- Ensure to publish a reasonably short-lived Root CA CRL, the recommendations from NIST is to have the Root CA CRL published for 1 year and ensure to renew the CRL before expiry.
- We strongly recommend that all your CA keys be stored securely in a FIPS 140-2 Hardware Security Module (HSM).
- Protect the server during boot using Bitlocker or any other encryption system of choice and ensure to backup CA private key, CA registry Key, the CA database, and the CA certificate.
- Ensure to enable an audit event to track all actions performed on the Root CA.

Inline with Compliance

- Ensure to have a CP and CPS created to suit the organization's needs and ensure the PKI infrastructure meets all standards and requirements with respect to the CP and CPS.
- Any changes or addition of features ensure to capture in the CP and CPS documents.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Ensure to renew the CA certificates(Root and Subordinate) within half its lifecycle.
- Enterprise key and certificate security policies should align with the latest regulatory, industry-standard recommendations, and guidelines such as key storage, secure communication protocols (TLSv1.2), cryptographic algorithms (RSA-2048), and hashing algorithms (SHA-2).
- Enterprise security architects should constantly monitor security standard recommendations and periodically update the enterprise's security policy.
- Ensure all security events are audited and a periodic security audit is performed to validate the security adherences and metrics.
- Encourage short-lived certificates for all key usages.

CSR Generation Standardization

- A process must be defined across the enterprise to generate CSR that aligns with the security standards and to store keys securely.
- Harden parameters such as Country and Organisation in accordance with organizational requirements.
- Access to keys should be restricted to authorized personnel.
- Key Generation, Certificate Request, and Approval processes should be well defined.

Archival

Signing keys do not require archival. We can always generate new keys for signing since the signed data is not encrypted. But encryption keys have to be archived so that the encrypted files during the certificate validity can be decrypted even after the certificate expiry. Also, this is recommended for security audits.

Secure Storage of Keys

- It is recommended to store private keys in HSM.
- Ensure respective certificate owners or certificate authorized administrators are granted access to private keys using the RBAC solution.
- Best practices training can be provided to certificate users and administrators to keep private keys secure.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Compromised CA/CA keys

- Ensure to discover a compromise as quickly as possible by implementing tracking and detection mechanisms and performing regular manual operational sanity checks.
- Establish well-defined communications plans for informing subjects, relying parties, and other stakeholders with sufficient details about the type of compromise so these parties can implement the appropriate remedial actions.
- If a CA system or signing key compromise occurs, the organization should perform the following steps:
  - Ensure that certificates issued to the organization’s systems or users from the compromised CA are revoked.
  - Notify all owners of the affected certificates about the CA compromise and establish a point of contact for responding to questions and providing guidance and instructions.
  - Replace all certificates from the compromised CA with new certificates from a different CA effective immediately.
  - Ensure that all relying parties have the certificate trust chains required to validate certificates from the new CA.
  - Ensure that revocation checking is enabled on all relying party systems.
- If the compromised CA is a root CA, the root certificate must be removed from all trust stores and relying on party systems.

Compromised Certificate Handling

- Ensured to be prepared to respond in a timely manner in case of a CA or end-entity certificate compromise and have a plan or workflow to replace all affected certificates or the trust chain.
- In the event of a key or certificate compromise, a fresh key pair should be generated on a secured system. The compromised item should be revoked and taken out of the service as soon as the systems are secured.
- If you are not sure of your private key possession, report it to your CA and suspend the key immediately. Once you find the key is secure, reinstate the certificate.

CA Compromise and Remediation Matrix

S/No.	Issue Type	Revoke compromised/ counterfeit certificates	Revoke CA certificate	Replace all certs issued	Remove/Revoke Root certificate
1	Impersonation	Yes	NA	NA	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

S/No.	Issue Type	Revoke compromised/ counterfeit certificates	Revoke CA certificate	Replace all certs issued	Remove/Revoke Root certificate
2	RA compromise	Yes	NA	NA	NA
3	CA system compromise	NA	Yes	Yes	Yes
4	CA key compromise	NA	Yes	Yes	NA
5	Root CA compromise	NA	NA	Yes	Yes

CLM - Best Practices

Risks Involved in an Enterprise without CLM and their Solutions

S/No	Risks Involved in an Enterprise without CLM	Solutions
1	No centralized management for all certificates in an enterprise and to know the certificate's location.	Different modes to discover existing certificates along with the discovery source.
2	Enforcing teams to follow the enterprise security standards.	• Get information about all certificates within an enterprise. • Run a validation for the existing certificate against the organization's security standard.
3	Poor monitoring of certificate validity causes outages due to expired certificates.	• Continuous monitoring of the certificate status and notifications. • Automated renewals and provisioning should be available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

S/No	Risks Involved in an Enterprise without CLM	Solutions
4	Control over the generation of keys.	Provide a mode of access to teams to access and generate certificates for their requirements.

- Create a certificate lifecycle management action plan
- Start automating the certificate management process wherever feasible.
- Identify and expose all the neglected certificates, these are the certificates that will cause more damage during expiry.
- Ensure proper RBAC controls and avoid using direct user accounts and instead use identified admin accounts for access and control.
- Enable notifications and alerts to ensure timely renewal.
- Schedule scans to run overnight or after business hours.

Standard Practices followed in the Certificate Inventory Management

- Certificate Group
- Access Control
- Recommended Columns to View in the Default Inventory

Certificate Group

- Group similar certificates into logical groups
- Groups can be based on business units or teams using certificates
- Provide group owner details during configuration for easy tracking
- Create hierarchy-based grouping to leverage alert escalation on OOB workflow.
- Try and maintain the same policy across a hierarchy of groups. It is also allowed to set a different policy for each hierarchy.

The best way to manage certificates is to group certificates based on the following:

- AD Security Group vs Department
- Test vs Production

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Internal vs External Hierarchy
- Auto-renew vs Approved CSRs
- Auto Push Updated Certificate vs Controlled Push Updated Certificate

Access Control

Based on certificate groups, you can create resources and map devices/applications.

Identify various authorization roles that have to be created. Find the list of roles below:

- Certificate Administrator Team
- CERT Owner/Requester
- Approver
- Certificate Manager
- Inventory View

The certificate admin team should be granted access to view the entire certificate inventory and end-users should be able to view their respective certificates.

All managed/monitored certificates should be available on a single window for tracking and visibility. The product provides various columns that have rich information that might not be needed in all scenarios.

Recommended Columns to View in the Default Inventory

- Subject Distinguished Name (DN)
- Subject Alternative Names (SANs)
- Issue Date (not Before date)
- Expiry Date (not After date)
- Issuing Certificate Authority
- Key Length
- Key Algorithm (RSA, ECDSA)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Signing Algorithm
- Validity Period (From the not Before date/time to the not After date/time)
- Installed location(s) of a certificate (IP or DNS address and file path)
- Certificate Owner (The group responsible for the certificate)
- Contacts (The group of individuals is notified of issues)
- Approver(s) (parties responsible for reviewing issuance and renewal requests)

As the inventory is a RegEx-based search engine, users can search for a certificate based on any parameter with various filters.

Securing CERT+

CERT+ Certificate Lifecycle Management (CLM) offers capabilities to discover and manage certificates on devices and self-service certificate enrollment for users. CERT+ also acts as a Key Escrow for keys discovered and enrolled.

Typically, the private keys are stored by the devices handling SSL termination, and an SSL management tool retrieves them during certificate renewal. The tools and devices store them in their storage in the original format, which can be reused. If there is an attack on the device or tool storage, the private keys will be given away, which can be used to host an array of attacks.

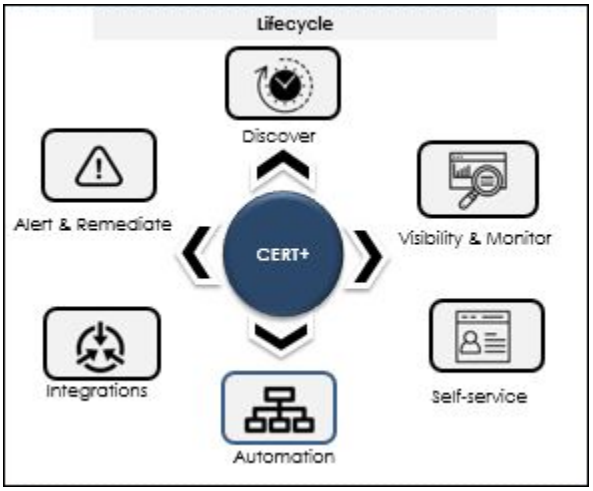
AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using the AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key.

Thus, even if the hackers get the database, they will not be able to get the private keys. Only a maze of jumbled up characters will be visible to them, which does not make any sense and hence, rendering the attack useless.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 2: CERT+ Admin Guide

AppViewX's CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CERT+, security teams can manage the certificate lifecycle from an intuitive single-pane management Interface. It enables the Certificate Lifecycle Management and Automation solution which helps enterprise IT manage and automate the entire lifecycle of their internal and external PKI. The key stages of the certificate lifecycle can be broken into the following stages:



- Getting Started
- CERT+ Setup

Getting Started

About AppViewX

AppViewX is advanced cybersecurity and network management, automation, and orchestration platform for Enterprise IT. AppViewX Lifecycle Management Solution for Certificates on ADC or Load Balancers, Servers, Firewall, Cloud, Web Application Firewall (WAF), and enterprise mobility solution aims to avoid network outages due to unplanned certificate expiration and improve organization security posture. This remote monitoring and management platform helps network operations move faster, enforce compliance, eliminate errors, and reduce costs in the organization.

CERT+ Overview

AppViewX's CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CERT+, security teams can manage the certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

lifecycle from an intuitive single-pane management Interface. It enables the Certificate Lifecycle Management and Automation solution which helps enterprise IT manage and automate the entire lifecycle of their internal and external PKI. The key stages of the certificate lifecycle can be broken into the following stages:

- **Certificate Discovery & Inventory Management** - Allows users to discover certificates across the network and manage inventory of all certificates in one place.
- **Visibility and Monitoring** - Enables the user to monitor certificate expiry and usage. The monitored data is represented as a detailed report on the web portal along with options to trigger email alerts. Allows users to gain insights into certificates; monitor and take remedial action.
- **Certificate Enrollment** - Allows users to request certificates from a certificate authority (CA) that confirms their identity and generates a certificate.
- **Certificate Renewal** - Allows users to either manually or automatically renew a certificate before the expiry date by retaining the old private key.
- **Certificate Regeneration** - Allows users to enroll new certificates with similar parameters to an old certificate. When a user generates a new private key, the user can modify the parameters if required.
- **Certificate Reissuance** - Allows users to enroll new certificates with similar parameters to an old certificate. But the newly issued certificate comes with the same validity as the older certificate and can modify the parameters.
- **Certificate Revocation** - Allows users to revoke a certificate in the event of certificate loss, compromise, or any other reason when the certificate is no more necessary for business.
- **Certificate Audit** - Track and audit the usage, creation, expiration, and revocation of certificates. Track user interaction with the platform.

What is Certificate Lifecycle Management (CLM)?

There is a growing need for organizations to allow and control only specific individuals, devices, machines to gain access to the network. The need for digital certificates to authenticate, identify and control who can access and operate on an organization’s network. Managing digital certificates across complex networks to ensure protection and prevent failures is a must for all businesses. CLM ensures continuous monitoring of digital certificates, with the ability to audit and keep track of expirations and renewals to avoid any service disruption. The digital certificate is a mechanism by which machines and individuals are identified and authenticated.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

What is x.509 Digital Certificate?

The digital certificate is a mechanism by which machines and individuals are identified and authenticated. Digital certificates (x.509 certificates) are essential to establish trust and authenticate the identity of machines, people, and so on.

It helps to verify the identity between users in operation, servers, and other entities in a network. Also, identifies servers from whom the encrypted data is received, the signer of information, and helps to establish authenticity and integrity. The x.509 digital certificate protects information belonging to enterprises and their customers.

A digital certificate contains:

- Name of the certificate holder.
- Serial Number that is used to uniquely identify the service, individual, or entity identified by the certificate.
- Expiry date.
- Copy of the certificate holder's public key (used for decrypting messages and digital signatures).
- Digital Signature of the certificate-issuing authority.

Certificate Authority

A Certificate Authority (CA) is also known as a certification authority or certificate issuer and is an establishment that validates the identities of certificate requesters and associates them to a cryptographic key through the issuance of electronic documents known as digital certificates.

- CERT Administration
- Prerequisites
- Accessing the CERT+
- CERT+ Home Page
- RBAC Configuration

CERT Administration

Using the tools on the Admin tab, you can perform the following tasks:

- Deploy and manage CERT+ hosts and licenses.
- Configuring user accounts, authorization, and authentication.
- Monitor the system health of managed hosts and the application.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Prerequisites

Supported Web Browsers

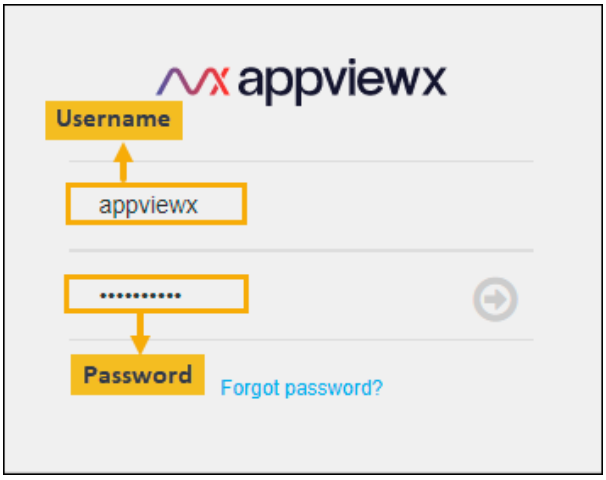
Web Browser	Version
Firefox	118.0.1 (64-bit) or later
Google Chrome	117.0.5938.134 (Official Build) (64-bit) or later

Related Documentation:

- License Management
- Logging & Alert Management.

Accessing the CERT+

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



2. Click (**Menu**) button located in the upper left corner of the screen.
3. Click **CERT+** on the left navigation bar.

CERT+ Home Page

The CERT+ home page contains necessary features for the certificate lifecycle management. The following table describes the options available in the CERT+ home page:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Options	Description
Menu button	Displays the left navigation pane of the AppViewX.
Expand/ Collapse	Expands/Collapses all the options, which are on the left navigation pane.
Search Field	Searches for the given key word(s) in the field and results the feature that matches the search key word(s).
Left Navigation Pane	Displays all the features available in the CERT+.
Collapse/ Expand	Hides/Displays the left navigation pane.
Help Tool Bar	Use the tool-bars for the additional options: • **Date** - plays Today Date • **Time** - Displays the time based on the locale

RBAC Configuration

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

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

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

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

- Benefits of RBAC
- Simplified RBAC Configuration in AppViewX

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Benefits of RBAC

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

Simplified RBAC Configuration in AppViewX

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

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

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

CERT+ Setup

Every individual certificate is associated with several variables which are different for each one, such as:

- Varying expiration dates (and hence, renewal necessities)
- Issued by multiple certificate authorities
- Consisting of unique system vulnerabilities that need to be individually monitored and addressed.

Certificates need to be constantly monitored to ensure that they’re effective. Administrators also require control over who gets to request and approve certificates, to ensure that unwanted certificates are not added to the system. All these processes are impossible to handle on manual systems like spreadsheets, prompting the need for a specialized certificate management process. The topics in this section lets you configure the various certificate authorities, policies along other configuration of devices and credentials that are important to the certificate management lifecycle.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Configuring CA Settings
- CA Policy
- Certificate Group
- Configuring Certificates
- Managing Devices
- Certificate Reports
- Auto Enrollment Protocols

Configuring CA Settings

- Amazon and Amazon Private CA
- Custom CA
- DigiCert CA
- DigiCert MPKI
- EJBCA CA
- Entrust CA
- Entrust MPKI
- GlobalSign MSSL CA
- GlobalSign Atlas CA
- GlobalSign SSL CA
- GoDaddy CA
- Google CA
- HashiCorp Vault CA
- HydrantID CA
- IDnomic CA
- InCommon CA
- Let’s Encrypt CA
- Microsoft Enterprise CA
- Microsoft Standalone CA
- Nexus CA
- Sectigo CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Symantec CA
- Trustwave CA

Amazon and Amazon Private CA

- Before you Begin
- Configuring Amazon CA
- Configuring Amazon Private CA
- Validating Amazon

Before you Begin

The prerequisites for configuring Amazon CA or Amazon Private CA account in AppViewX are as follows:

- An Amazon account for a user having necessary access for enrolling the certificates and other CLM operations.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.
- Policy JSON for AWS Ec2 Instance Certificate Management.
- Prerequisite for Amazon CA:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ssm:SendCommand",
"ssm:DescribeDocument",
"ec2:DescribeInstances",
"ec2:DescribeRegions",
"s3:ListBucket",
"ssm:CreateDocument",
"ssm:GetCommandInvocation",
"s3:GetObject",
"s3:ListAllMyBuckets",
"ssm:DescribeInstanceInformation",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"ssm:GetDocument",
"s3:DeleteObject",
"s3:GetBucketLocation"
],
"Resource": "*"
}
]
}
```

Policy JSON for Certificate Management in AWS Classic and Application LoadBalancers:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"iam:GetServerCertificate",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:ModifyListener",
"elasticloadbalancing:DescribeListeners",
"acm:GetCertificate",
"ec2:DescribeRegions",
"elasticloadbalancing:DescribeTargetHealth",
"acm:ImportCertificate",
"elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
"iam:UploadServerCertificate"
],
"Resource": "*"
}
]
}
```

Policy JSON for Certificate Management in AWS Cloudfront:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"Effect": "Allow",
"Action": [
"ec2:DescribeRegions",
"cloudfront:ListDistributions",
"cloudfront:UpdateDistribution",
"cloudfront:GetDistributionConfig"
],
"Resource": "*"
}
]
}
```

Policy JSON for IAM Certificate Management:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"iam:GetServerCertificate",
"iam:UpdateServerCertificate",
"iam:ListServerCertificates",
"ec2:DescribeRegions",
"iam:UploadServerCertificate"
],
"Resource": "*"
}
]
}
```

Policy JSON for ACM Certificate Management:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"acm:DescribeCertificate",
"acm:RequestCertificate",
"acm:GetCertificate",
"ec2:DescribeRegions",
"acm:ListCertificates",
"acm:ImportCertificate"
],
"Resource": "*"
}
]
}
```

Prerequisite for Amazon Private CA.

Policies and Permissions required for AWS IAM User:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"s3:PutObject",
"s3:GetObjectAcl",
"s3:GetObject",
"s3:PutObjectAcl"
],
"Resource": [
"arn:aws:s3:::<bucketname>",
"arn:aws:s3:::<bucketname>/*"
]
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": [
"acm-pca:GetCertificate",
"ec2:DescribeRegions",
"acm-pca:GetCertificateAuthorityCertificate",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"acm-pca:RevokeCertificate",
"acm:RenewCertificate",
"acm-pca:ListCertificateAuthorities",
"acm-pca:DescribeCertificateAuthorityAuditReport",
"acm-pca:CreateCertificateAuthorityAuditReport",
"s3:ListAllMyBuckets",
"acm:DescribeCertificate",
"acm-pca:IssueCertificate",
"acm:RequestCertificate",
"acm:GetCertificate",
"acm:ListCertificates",
"acm-pca:DescribeCertificateAuthority"
],
"Resource": "*"
}
]
```

AWS Simple Storage Service (S3) Bucket Policy for parsing Audit log:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "acm-pca.amazonaws.com"
},
"Action": [
"s3:PutObject",
"s3:PutObjectAcl",
"s3:GetBucketAcl",
"s3:GetBucketLocation"
],
"Resource": [
"arn:aws:s3:::bucket_name/*",
"arn:aws:s3:::bucket_name"
]
}
```

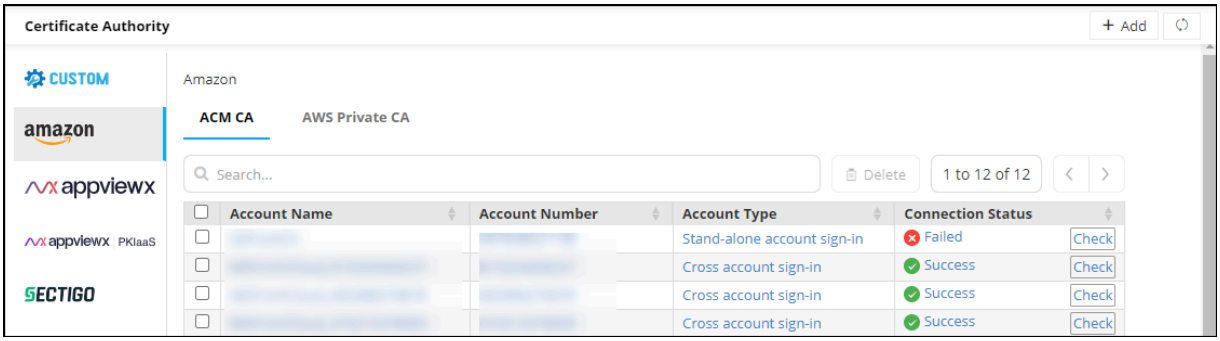
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
]
}
```

Configuring Amazon CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.

   The **Amazon** home page is displayed.



3. To configure Amazon CA, click **ACM CA** from the home page.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.

> **Note:** The **Configure Now** option is displayed if you are configuring a CA for the first time.

   The **Amazon** configuration page is displayed.

5. Enter/Select the following details in the **General Information** section:

General Information - Field Description Table

Fields	Description
***Account Type**	From the dropdown list, select one of the following account types: • **Standalone** (Traditional access key- and secret key-based communication) • **Cross or Federated** (Authentication using assume role)
***Account Name**	Unique name for the certificate authority (CA) account represented during certificate enrollment and policy creation
***Account Number**	Valid AWS account number
Account Description	Additional information related to the CA account being configured

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. The available options are, • Server • Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
***Default Region**	Default region for API communication
***Data Center (AppViewX's CA agent)**	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

6. Enter/Select the following **Credentials**-related information:

Credentials - Field Description Table

Fields	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account)
Access key*	Enter the access key for the customer's AWS account. This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret key*	Enter the secret key for the customer's AWS account. This field is displayed only when **Credential** type is set to **Manual Entry**.
*: *Mandatory fields*	

7. Enter/Select the following details in the **Discover resources** section:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Discover Resources - Field Description Table

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td>*Role ARN for Resource Discovery</td><td>This field is displayed only when Account Type is Cross or Federated.

To let the master account assume role for the child account (get temporary privileges to discover resources from the child account), configure the role ARN for resource discovery:

a. Click  (Settings).
b. Enter the following details:

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
Default: 3600 seconds (1 hour)</td></tr>
</table>
</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description

Fields	Description
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: i. In the **Enter Key** field, enter a key for the key-value pair. ii. In the **Enter Value** field, enter a value for the key-value pair. iii. Click **Add**. The added key-value pair is shown in the table below the fields.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Service Region**	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Discover Certificate	To enable instant certificate discovery at the time of device addition, select this checkbox.
***Cert Sync**	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic schedule-based synchronization: a. For **Auto Sync**, select the **Yes** checkbox. b. For **Schedule based discovery**, use the two dropdown lists to select a duration. For example, to schedule the auto sync after every 2 days, from the first dropdown list, select **2** and from the second dropdown list, select **Days**. By default, the auto sync is set to **1 Hours**. **Note:** The **Schedule based discovery** dropdown lists are displayed only when **Auto Sync** is enabled.

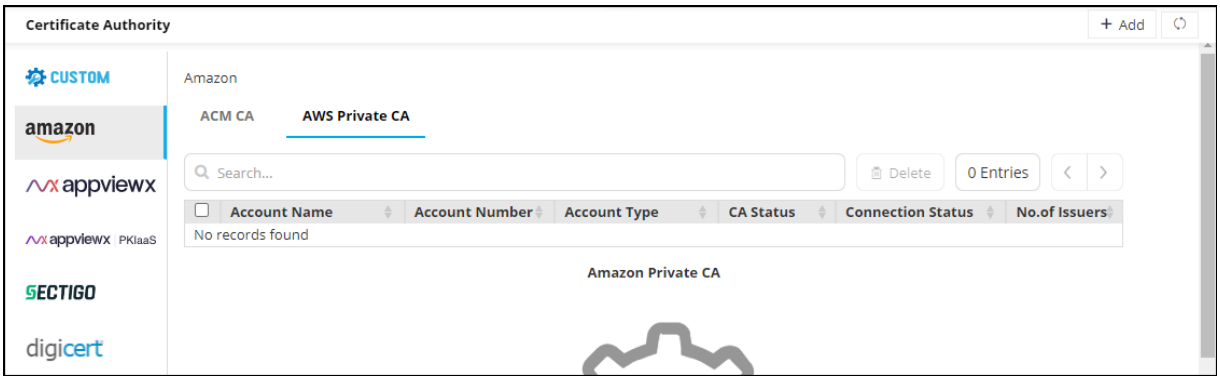
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle. **Important:** If Route53 has been configured for any of the older Amazon Public CAs, ensure that, after migration, the zones are manually updated.
*: *Mandatory fields*	

8. Click **Save**.

Configuring Amazon Private CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.
   The **Amazon** home page is displayed.
3. To configure the Amazon Private CA, click **AWS Private CA**.

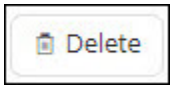
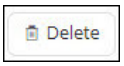
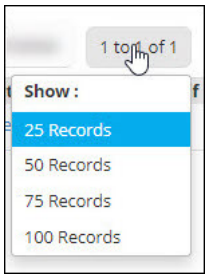


The **Amazon** home page is updated to display the inventory grid as shown in the image. In the inventory grid for the Amazon Private CA, master and child account details are logged as separate entries, instead of having just one master entry.

Fields in the inventory grid are explained in the table below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AWS Private CA - Screen Description Table

Fields	Description
Search	Use the **Search** field to search for accounts, by entering the value of one of the details listed in the inventory grid.
	To delete one or more accounts: a. From the inventory grid, select the checkbox corresponding to the account(s) you want to delete. b. Click  (Delete) . **Tip:** To delete all accounts listed in the inventory grid, select the checkbox in the grid header.
	To set the number of records that should be displayed on one page: a. Click  . b. From the **Show** menu displayed, select the required value. 
	If the inventory grid spans more than one page, use this control to navigate the pages, one page at a time.
Account Name	This is the unique name for the Certificate Authority (CA) account entered at the time of account creation.
Account Number	AWS account number
Account Type	**Multi account**: Indicates that the account is a cross account **Single account**: Indicates that the account is a standalone account
CA Status	For an account, after all configuration details for Amazon Private CA are entered, you will be required to click the **Fetch issuer and save** button

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	to sync and discover the issuers and the respective certificates for that account. The **CA Status** field shows the current status of this sync and discovery process. Possible values for this field are: • Completed • In progress **Note:** An account entry in the grid will be disabled till the **CA Status** is **In progress**.
Connection Status	To validate if connection has been established with the CA, click **Check**. If a connection has been established, this field is updated to display **Success** or **Failure**.
No. of Issuers	This field displays the number of issuers associated with the account. **Note:** For a master account, this field will show the number of issuers associated with only the master account. The value does not include the number of issuers associated with the child account.
*: *Mandatory fields*	

4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The **Amazon** page is updated to display fields for entering the CA configuration-related information.
5. On this screen, enter the following **Basic Information**:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Basic Information - Field Description Table

Fields	Description
***Account type**	From the dropdown list, from the following options, select the customer's AWS account type: • **Standalone**: The user account and the resources are available in the same account. • **Cross or Federated**: Resources are available across multiple accounts and users are given role-based access.
***Account name**	Enter a unique name for the Certificate Authority (CA) account that will be used during certificate enrollment and policy creation.
***Account number**	Enter the customer's AWS account number.
Account Description	Enter any additional details related to the account, if required.
***Purpose/Usage**	From the dropdown list, select the purpose of the certificate that can be requested using this account.
Proxy Required	To allow all communication to the Certificate Authority (CA) to use the proxy details (provided in general settings; refer the CLMaaS Platform User Guide for more details), select this checkbox.
***Default Region**	From the dropdown list, select the default region for API communication.
Data Center (AppViewX's CA Agent)	From the dropdown list, select the data center that will be used to establish communication with the Certificate Authority (CA)
*: *Mandatory fields*	

6. Enter the following **Credentials**-related information:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential type**	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account)
***Access key**	Enter the access key ID for the customer's AWS account. The access key and the secret access key (entered in the following field) are used together to authenticate requests. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
***Secret key**	Enter the secret access key ID for the customer's AWS account. The access key (entered in the previous field) and the secret access key are used together to authenticate requests. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
***Credential name**	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
*: *Mandatory fields*	

7. In the **Discover resources** section, enter the following details:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Discover Resources - Field Description Table

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td>Role ARN for Resource Discovery*</td><td>This field is displayed only when Account Type is Cross or Federated. To let the master account assume role for the child account (get temporary privileges to discover resources from the child account), configure the role ARN for resource discovery:
a. Click  (Settings).
b. Enter the following details:
<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be</td></tr>
</table>
</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td>Service Region*</td><td>Service regions are regions that are supported by the selected service.

To select a service region:
a. To fetch the service regions for the account information provided, click Fetch Region.The retrieved service regions are populated in the Select the Region(s) dropdown list.
b. From the Select the Region(s) dropdown list, select the required service region.</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td>CA Operation Mode*</td><td>From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority:
• ACM Private CA
• AWS Certificate Manager (ACM)</td></tr>
<tr><td>S3 Bucket*</td><td>This field is displayed only when the ACM Private CA operation mode is selected. Enter the S3 bucket name.</td></tr>
<tr><td>Role ARN for S3 Bucket</td><td>This field is displayed only when the ACM Private CA operation mode is selected for a Cross or Federated account.
a. Click  (Settings).
The ARN Advanced Settings action pane is displayed.
b. In the ARN Advanced Settings action pane, enter the following details:<table><tr><th>Fields</th><th>Description</th></tr><tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr><tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.</td></tr></table></td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description	
	Fields	Description
		Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) **Default**: 3600 seconds (1 hour)
	External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
	Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
	Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: i. In the **Enter Key** field, enter a key for the key-value pair. ii. In the **Enter Value** field, enter a value for the key-value pair. iii. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>The added key-value pair is shown in the table below the fields.</td></tr>
</table>
c. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td>CA Sync*</td><td>Select from one of the following options:
• Managed: AppViewX will connect with the customer’s AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
• Monitored: AppViewX will connect with the customer’s AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
• Ignored: AppViewX will connect with the customer’s AWS account but certificate discovery will be disabled.</td></tr>
<tr><td>Auto Sync</td><td>To enable/disable automatic synchronization, use the Auto Sync key.

If Auto Sync is enabled, to set the frequency of the schedule-based sync:
a. From the first dropdown list, select the interval between two schedule-based syncs.
b. From the second dropdown list, select a unit for the interval (Hours/Days).

For example, to set the frequency of the schedule-based sync to every 2 hours, from the first dropdown list, select 2 and from the second dropdown list, select Hours.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

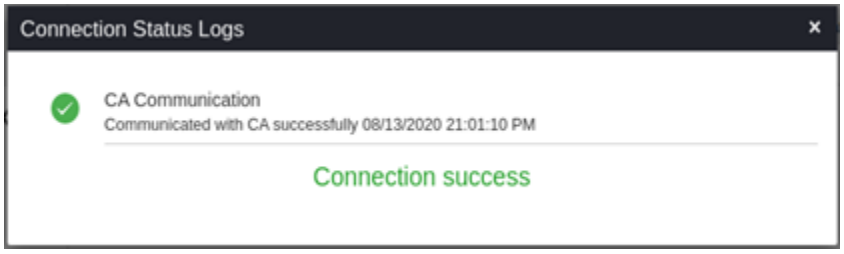
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

8. Click **Fetch issuer and save**.
   - AppViewX will now discover all the Private CA Certificate Authorities across the selected region(s).
   - The inventory grid on the Amazon CA home page will be populated with the properties and details retrieved from this discovery.

Validating Amazon

Once the Amazon settings are added, you need to validate the connection between AppViewX and Amazon, to make sure that the connection is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.
   The **Amazon** home page is displayed.
3. On the **Amazon** home page, select **Amazon** or **Amazon Private CA**.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **connection status** will be displayed as either **Connection success** or **Failure**.



Custom CA

- Before you Begin
- Configuring Custom CA

Before you Begin

The prerequisites for configuring Custom CA account in AppViewX are as follows:

- A logo to use it for the custom CA.
- An optional CA certificate and key to be used as a root certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Custom CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Custom**.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The **Custom** home page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***Custom CA Name**	A unique name to identify the CA name. No special characters allowed.
***Upload Custom CA Logo**	Upload a logo for the custom CA. This logo will appear in the product representing the custom CA.
Custom CA Certificate	Upload a certificate for the custom CA. This certificate will become the root certificate. The <.*pfx*> and <.*p12*> are certificate types are supported.
*: *Mandatory fields*	

5. Once the logo and certificate are uploaded, the entered CA will appear in the CA list with the logo presented.
6. Once the logo is added, users can click **Configure Now** to input the CA details.
7. Update the following details in the **General Information** section as described in the table:

Fields	Description
***Name**	Client authentication certificate for API communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

8. Update the following details in the **ROOT CSR parameters** section as described in the table:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Root CSR - Field Description Table

Fields	Description
Common Name	The common name of the root certificate. • Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain domain.com. • Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Algorithm	Type of the root certificate.
Hash Function	The hash function for the root certificate.
Organization Unit	Name of the Organisation unit.
Key Length	Key length for the root certificate.
Organization	Organization attribute for the root certificate.
Locality	Locality attribute for the root certificate.
State or Province	State attribute for the root certificate.
Country	Country attribute for the root certificate.
Email Address	Email address for the root certificate.
*: *Mandatory fields*	

9. Update the following details in the **Root Validity** section as described in the table.

Fields	Description
***Start Date**	Start date of the certificate issuance.
***End Date**	End date of the certificate issuance.
*: *Mandatory fields*	

10. Click **Save**.

    Once the setting is saved, the user will be directed to the root certificate submission holistic view as below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



11. Users can submit and fetch the root certificate.
12. On the CA setting page user can see the status of the created setting as shown below.



DigiCert CA

- Before you begin
- Configuring DigiCert
- Validating DigiCert

Before you begin

The prerequisites for configuring DigiCert CA account in AppViewX are as follows:

- A DigiCert CertCentral Account with **Administrator** role Access.
- An **API Key** configured in Digicert with required permissions to make API Requests from AppViewX.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring DigiCert

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **DigiCert**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **DigiCert** home page is displayed.

3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The **DigiCert** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Digicert CA APIs for Certificate Management:

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain just the hostname of the Digicert CA instance. For example, <https://www.digicert.com> **Note:** vendorSpecificSettings.url - invalid URL.
***Credential Type**	Select the type of credential as desired from the dropdown list. The available options are, • Manual EntryCredential • List - CyberArk.
***Credential List**	Select the required credential from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This field will be enabled if the Credential Type is selected as Credential List - CyberArk.
Account ID	Account id details of Digicert CA Account, which can be found under account manager details in Digicert CertCentral Account.
***API Key**	API key specific to the CA account. This API key should have required permission to make API Calls. Space is not allowed.
Auto Approve	Enable the**Auto Approve** option if all CLM requests from AppViewX do not need to be approved from Digicert CA Account. Auto approval checkbox is optional and its features work only for **one-step certificate requests** configured in the Digicert Cert Central Account.
Note: The asterisk (*) symbol indicates a mandatory field.	

6. Select **Fetch Divisions and Certificate Types.**
   The Division and Certificate types available in the DigiCert CA account will be fetched.
7. Click **Save**.

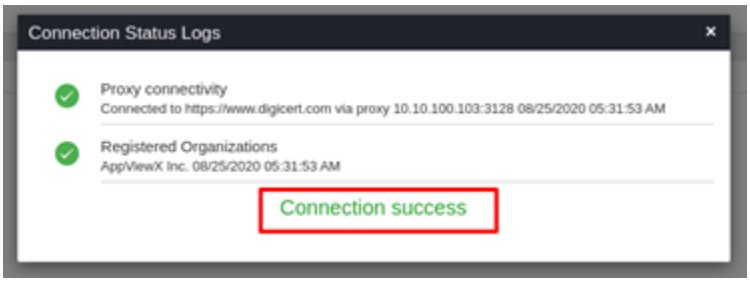
Validating DigiCert

Once the Digicert settings are added, the validation must be done to check whether the connection between AppViewX and Digicert is configured properly.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Digicert**.
   The **Digicert** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



DigiCert MPKI

- Before You Begin
- Configuring DigiCert MPKI
- Validating DigiCert MPKI Connection

Before You Begin

The prerequisites for configuring a Digicert MPKI CA account in AppViewX are as follows:

- A Digicert MPKI Account with **Administrator** role Access.
- An **API Key** configured in Digicert MPKI with required permissions to make API Requests from AppViewX.
- The AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring DigiCert MPKI

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **DigiCert**.
   The **DigiCert** home page is displayed.
3. Click the **DigiCert MPKI** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **DigiCert MPKI** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

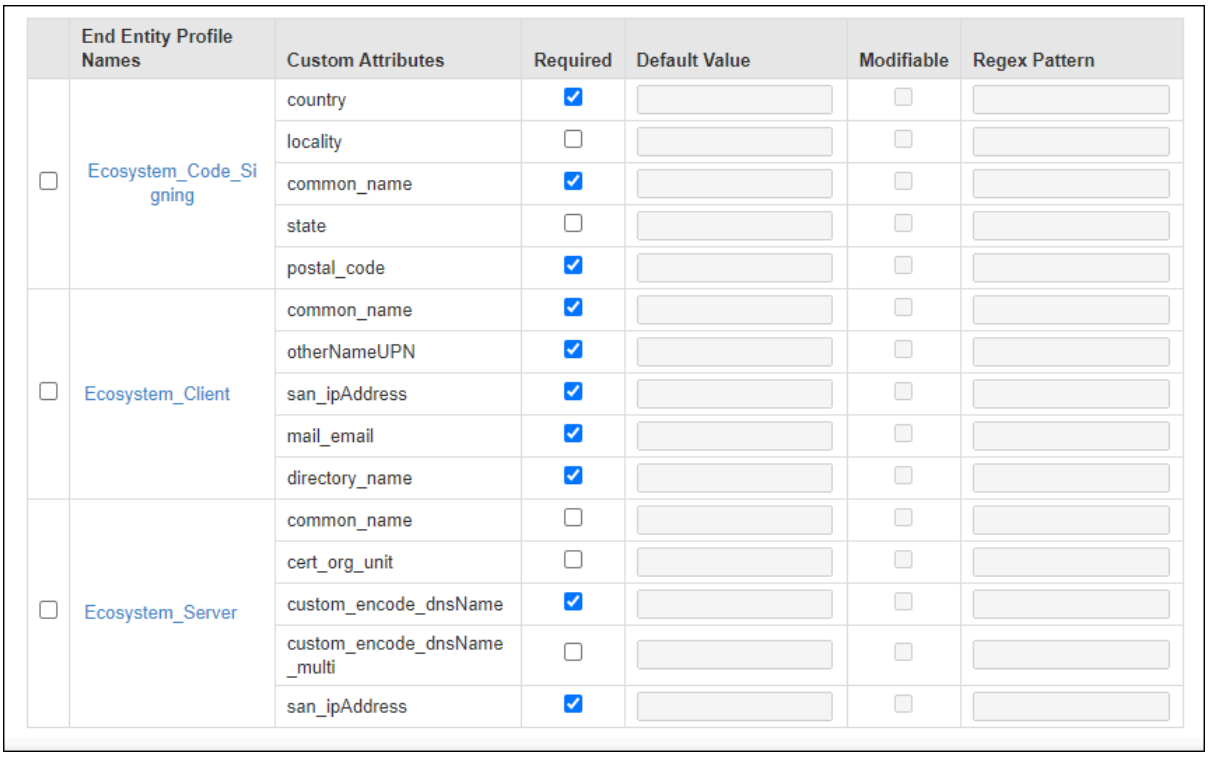
6. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Digicert CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain just the hostname of the Digicert CA instance. For example, <https://www.digicert.com>
***Seat ID**	Enter the unique seat id for discovering certificates.
***API Key**	Enter the API key, which is generic across all CAs
*: *Mandatory fields* **Note:** Auto approval checkbox is optional and features work only for **one-step certificate requests** configured in the DigiCert Central Account.	

7. Select **Fetch Divisions and Certificate Types.**
   The Division and Certificate types available in the Digicert CA account will be fetched and listed for the specific API key user in the table as shown below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



	End Entity Profile Names	Custom Attributes	Required	Default Value	Modifiable	Regex Pattern
☐	Ecosystem_Code_Signing	country	☑		☐	
		locality	☐		☐	
		common_name	☑		☐	
		state	☐		☐	
		postal_code	☑		☐	
☐	Ecosystem_Client	common_name	☑		☐	
		otherNameUPN	☑		☐	
		san_ipAddress	☑		☐	
		mail_email	☑		☐	
		directory_name	☑		☐	
☐	Ecosystem_Server	common_name	☐		☐	
		cert_org_unit	☐		☐	
		custom_encode_dnsName	☑		☐	
		custom_encode_dnsName_multi	☐		☐	
		san_ipAddress	☑		☐	

8. Click **Save**.
   A pop-up message is displayed as <CA_name> Settings Added.

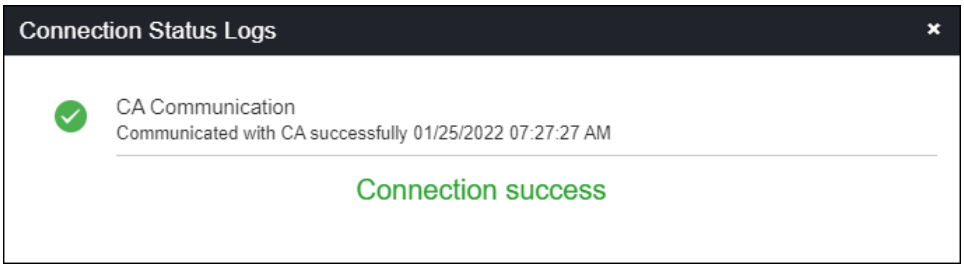
Validating DigiCert MPKI Connection

Once the Digicert MPKI settings are added, the validation must be done to check whether the connection between AppViewX and Digicert MPKI is configured properly.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **DigiCert**.
   The **DigiCert** home page is displayed.
3. Click **DigiCert MPKI** from the left pane of the page.
   The **DigiCert MPKI** home page is displayed.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



EJBCA CA

- Before you begin
- Configuring EJBCA
- Validating EJBCA

Before you begin

The prerequisites for configuring the EJBCA account in AppViewX are as follows:

- An EJBCA client certificate for a user having the necessary access for enrolling the certificates and other CLM operations.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring EJBCA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **EJBCA**.
   The **EJBCA** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **EJBCA** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/ Usage**	Certificate Type for which CLM actions will be enabled. E.g. Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Client Authentication**	Client authentication certificate for API communication. a. Enter the valid password once the **Authentication Details** window is displayed. b. Click **OK**. The value must be a valid <.*p12*> or <.*pfx*> file.
***URL**	EJBCA URL
***Discover by expiry days**	To get all the certificates that are expired and valid for specified days. The value must be number.
End entity profile names	Required end entity profiles for CA setting.
Custom attributes	Required custom attributes for the specific end entity profile. The validation can be added by the user in the regex box.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: *Mandatory fields*	

6. Click **Validate and Fetch**.
   The **End entity profiles** available for the CA account will be fetched along with the certificate profile from the **Certificate Authority**.
7. Update the following details in the **Certificate Attributes** section as described in the table:

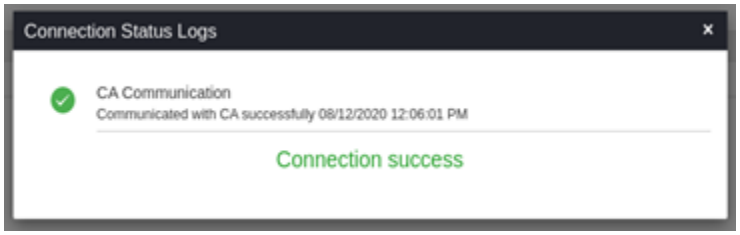
Fields	Description
***End Entry Profile Names**	Select the profile that is used in the certificate enrollment from the dropdown list.
Custom Attributes	Select the list attributes configured in CA to enroll certificates. Custom attributes should be configured as exactly as it is available in the EJBCA portal.
*: *Mandatory fields*	

8. Click **Save**.

Validating EJBCA

Once the EJBCA settings are added, validation needs to be done to check whether the connection between AppViewX and EJBCA is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **EJBCA**.
   The **EJBCA** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust CA

- Before You Begin
- Configuring Entrust
- Validating Entrust CA

Before You Begin

The prerequisites for configuring Entrust CA account in AppViewX are as follows:

- An Entrust client authentication certificate and credentials−API username (username) and API key (password) having necessary access for CLM actions.

  To get a private key + certificate that can be used to access to API. The general steps performed by a super admin are:
  - Generate a new private TLS/SSL key and a CSR.
  - Issue a certificate in the ECS account using the CSR. Client Authentication must be enabled in the certificate.
  - Import the private key and certificate into the system that will be invoking the API.
  - Test that TLS/SSL mutual authentication is successfully configured.

  Refer chapter **Authentication** and section **TLS with client certificate authertication** in the Entrust - Rest API Guide.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring Entrust

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed. The Entrust tab is selected by default.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Entrust** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server and Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Entrust CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Client Authentication**	The client authentication certificate from Entrust for API communication. **Note:** Must be a valid <.*p12*> file. To generate an CSR within AppViewX refer to Generating a CSR and download the CSR. Further, upload the CSR to the Entrust homepage as described in section - XXXXX.
***Base URL**	This URL will contain just the hostname of the Entrust CA instance. The value is https://api.entrust.net/enterprise/v2
User Name	Enter the API Username to communicate with the CA.
Password	Enter the API Password to communicate with the CA.
Auto Approve	Select the checkbox to avoid queuing of new certificates in the CA portal.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. Update the following details in the **Advanced Settings** section as described in the table.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	A check box field when selected will fetch the certificated immediately after CSR Submission on enrollment, renew, and reissue of certificate with the retry count and retry frequency as described below.
***Retry Count**	The number of times the polling will take place after CSR submission. Enter a value between 1 and 10.
***Retry Frequency**	The duration of the polling. enter the value between 1 and 30seconds
*: Mandatory fields	

7. Click **Fetch Custom Attributes**.
   The attributes available for the CA account will be fetched from the Certificate Authority along with the CA and profile names. A pop-up message is displayed as **CA and profiles fetched**.
8. Click **Save**.
   The created Entrust configuration settings will be added. A pop-up message is displayed as **<CA_name> Settings Added**.

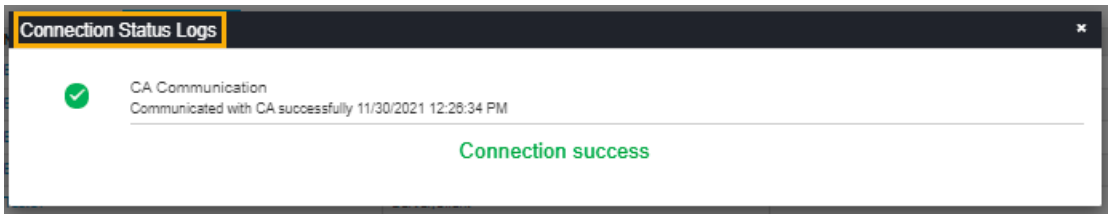
Validating Entrust CA

Once the Entrust settings are added, validation needs to be done to check whether the connection between AppViewX and Entrust is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



Entrust MPKI

- Before you begin
- Configuring Entrust MPKI
- Validating Entrust MPKI

Before you begin

The prerequisites for configuring Entrust MPKI CA account in AppViewX are as follows:

- An Entrust client authentication certificate and credentials having necessary access for CLM actions.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring Entrust MPKI

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. Click the **Entrust MPKI** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Entrust MPKI** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server and Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Entrust MPKI CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Client Authentication**	Client authentication certificate for API communication. **Note:** Must be a valid <.*p12*> file.
***Base URL**	This URL will contain just the hostname of the Entrust CA instance. Eg - https://api.entrust.net/enterprise/v2
**: Mandatory fields*	

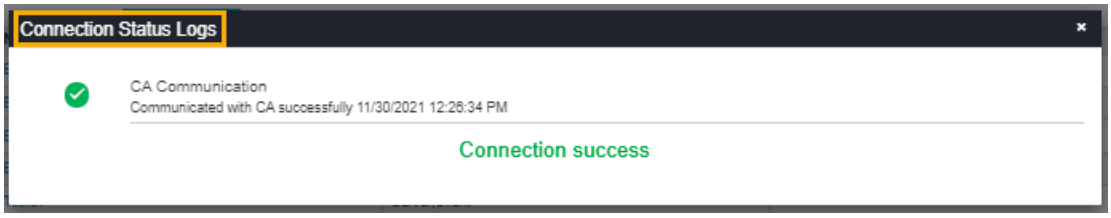
7. Click **Fetch CA and Profile Names.**
   The attributes available for the CA account will be fetched from the Certificate Authority along with the CA and profile names. A pop-up message is displayed as **CA and profiles fetched**.
8. Click **Save**.
   The created Entrust MPKI configuration settings will be added. A pop-up message is displayed as **<CA_name> Settings Added**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Validating Entrust MPKI

Once the Entrust settings are added, validation needs to be done to check whether the connection between AppViewX and Entrust is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. Click **Entrust MPKI** from the left pane of the page.
   The **Entrust MPKI** home page is displayed.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



GlobalSign MSSL CA

- Configuring GlobalSign MSSL
- Validating GlobalSign MSSL
- Limitations

Configuring GlobalSign MSSL

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click the **GlobalSign MSSL** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign MSSL** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, server and clients
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

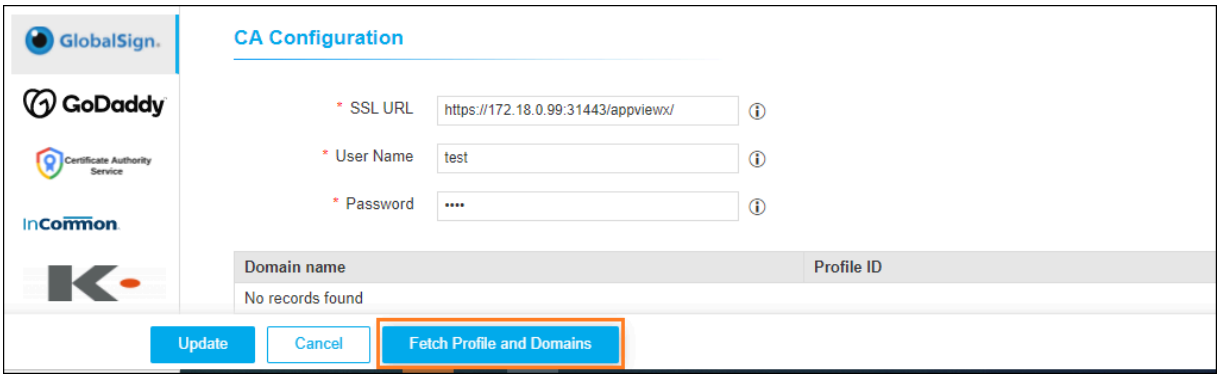
6. Update the following details in the **CA Configuration** section as described in the table.



Fields	Description
***SSL URL**	Base URL of the SSL API
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

7. Once all the details are configured, click **Save**.
8. In GlobalSign MSSL, we can now fetch profiles and domains by clicking on the **Fetch Profiles and Domain** button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

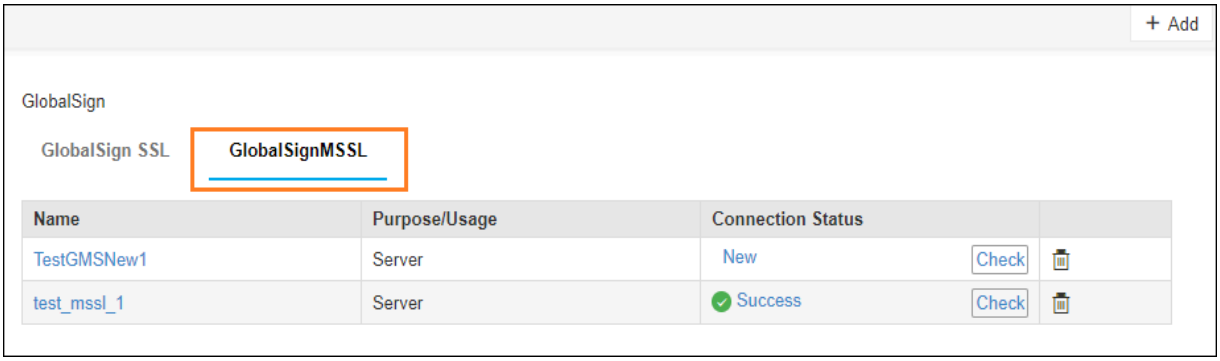


Note: The supported CSR key types are RSA **2048-8192, ECC P-256, ECC P-384** .

Validating GlobalSign MSSL

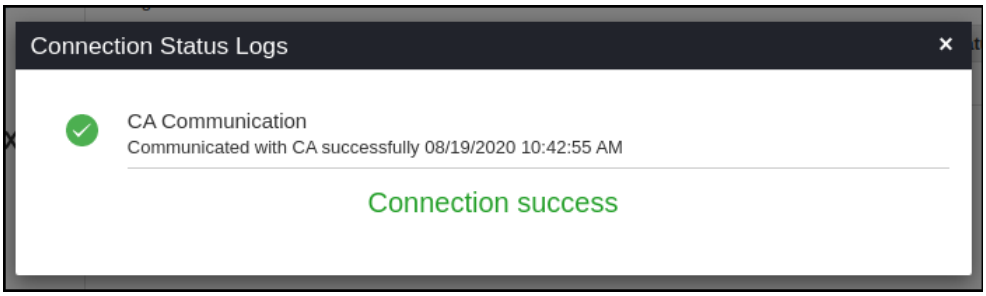
Once the GlobalSign MSSL settings are added, validation needs to be done to check whether the connection between AppViewX and GlobalSign MSSL is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **GlobalSign MSSL** from the left pane of the page.
   The **GlobalSign MSSL** home page is displayed.



4. In the **Status** column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



.

Limitations

Case/ Ticket number	Fix Description
CA Setting Update	Users need to click on the **Cancel** button once the MSSL domain/profile. ID details are fetched from the GlobalSign MSSL account. If the user clicks the Update button, MSSL domain/profile ID details will be removed from the associated policy. The steps to follow to update CA settings are as follows: 1. On the GlobalSign MSSL CA settings page, after adding/editing values, click the Update button. 2. Navigate back to updated CA settings and click the **Fetch Profiles and Domain** button. 3. Click the **Cancel** button instead of Update to bypass the existing issue.
Default CA policy mapping	The default CA policy is defined with all available values selected and validity data is mapped based on commonly used validity. Hence, it will not have values equivalent to API documents or CA portals. This can be modified or updated in the application accordingly to the default CA policy if changes are required.
Email Address	The email address provided in the email address field on the enrollment page is not considered as the primary email value during CLM actions, instead, the email address field defined in the contact information of the logged-in user will be used. The help info message besides the Email address field on enroll/edit page is as – “If the user email address is configured, that will be used for GlobalSign CA approval actions. If the user email is not configured, then the email address provided in this field will be used" - the second part is not valid anymore.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign Atlas CA

- Before You Begin
- Configuring GlobalSign Atlas
- Validating GlobalSign Atlas

Before You Begin

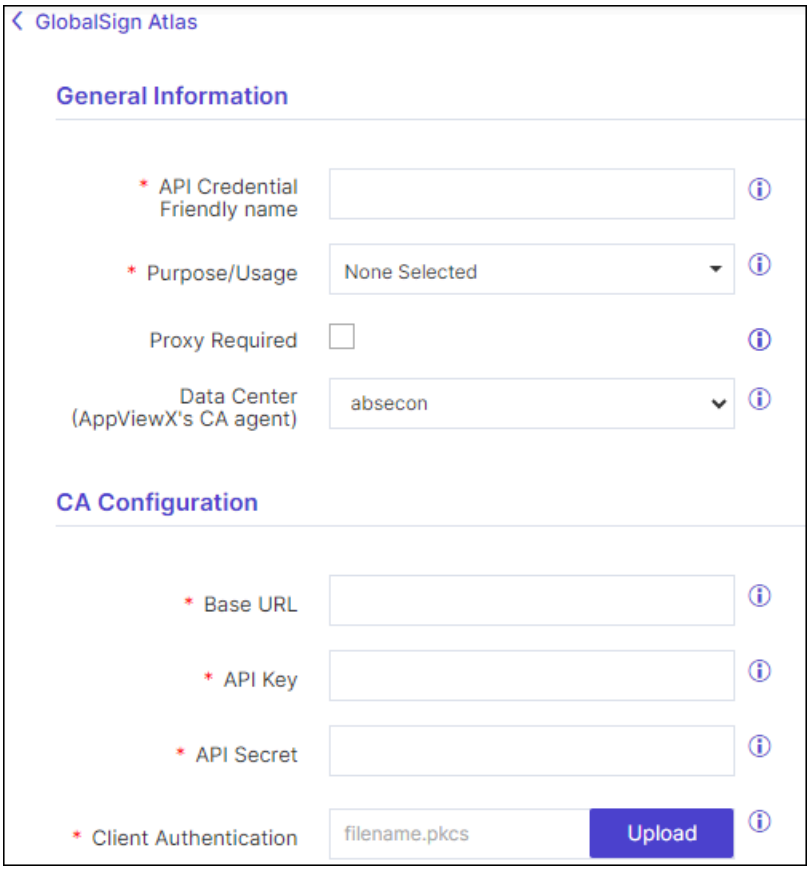
The prerequisites for configuring GlobalSign Atlas CA in AppViewX are as follows:

- Login and password to access AppViewX.
- Base URL, API Key, API Secret Key.
- A client certificate provided by the GlobalSign Atlas team.

Configuring GlobalSign Atlas

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Choose the **GlobalSign Atlas** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign Atlas** configuration page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***API Credential Friendly name**	Enter the API Credentials Friendly name (which is the CA Account name that will be used for the CA Policy and Enrollment).
***Purpose/Usage**	Select the purpose of the certificate that can be requested using this account. **Note:** Users can select *Server*, *Client* or both.
Proxy Required	Select the checkbox if communication to the Certificate Authority (CA) has to use the proxy details provided in the general settings
Data Center (AppViewX's CA agent)	Select the data center that will be used to establish the communication with the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

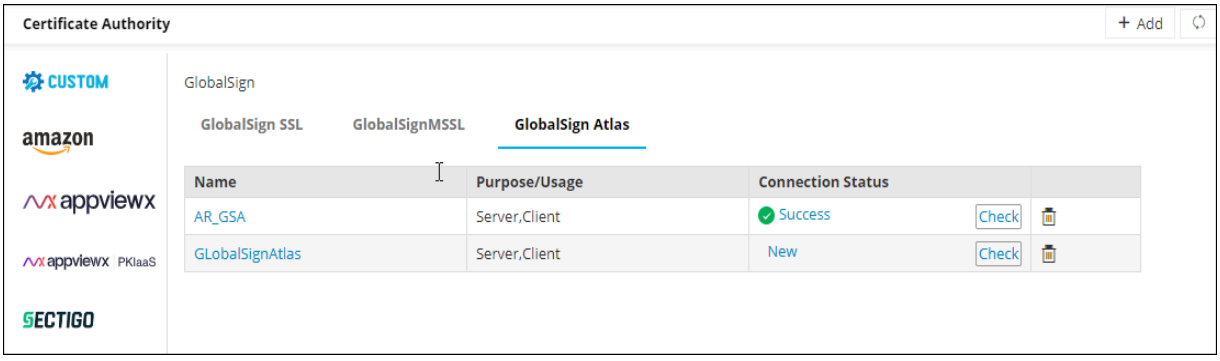
Fields	Description
*: Mandatory fields	

6. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Enter the base URL required for constructing the API request.
***API Key**	Enter the API key which is the unique identifier used to authenticate a user. **Note:** The API Key will be displayed as asterisks (*)
***API Secret**	Enter the API secret to communicate with the CA. **Note:** The API Key will be displayed as asterisks (*)
***Client Authentication**	Upload the certificate for client authentication in the .p12 or .pfx format only.
*: Mandatory fields	

7. Click the **Fetch Validation Policy and Save** button.
   A confirmation message will appear “Validation Policy fetched and settings have been updated.” and the CA is created successfully. The connection status for the CA is displayed as New.

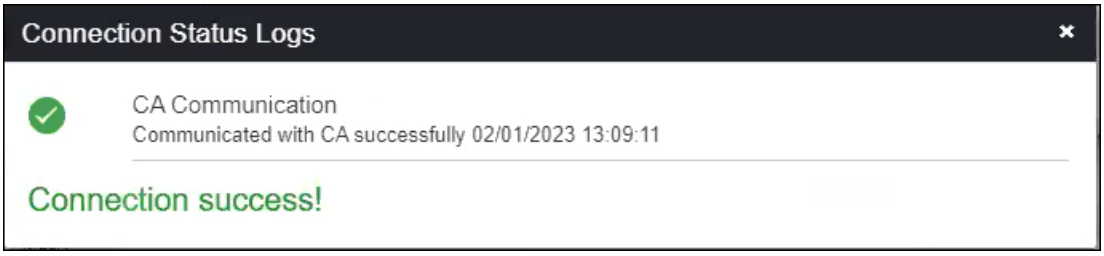


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Validating GlobalSign Atlas

Once the GlobalSign Atlas settings are added, validation needs to be done to check whether the connection between AppViewX and GlobalSign Atlas is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click **GlobalSign Atlas** from the left pane of the page.
   The **GlobalSign Atlas** home page is displayed.
4. In the **Status** column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



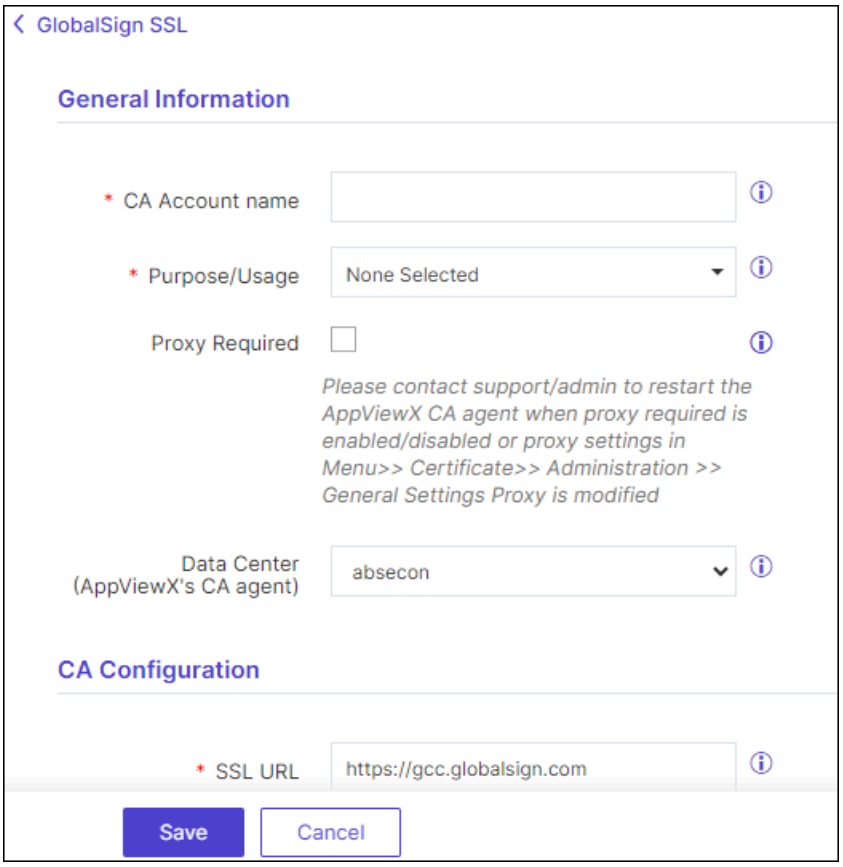
GlobalSign SSL CA

- Configuring GlobalSign SSL
- Validating GlobalSign SSL

Configuring GlobalSign SSL

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click the **GlobalSign SSL** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign SSL** configuration page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Update the following details in the **CA Configuration** section as described in the table.



CA Configuration - Field Description Table

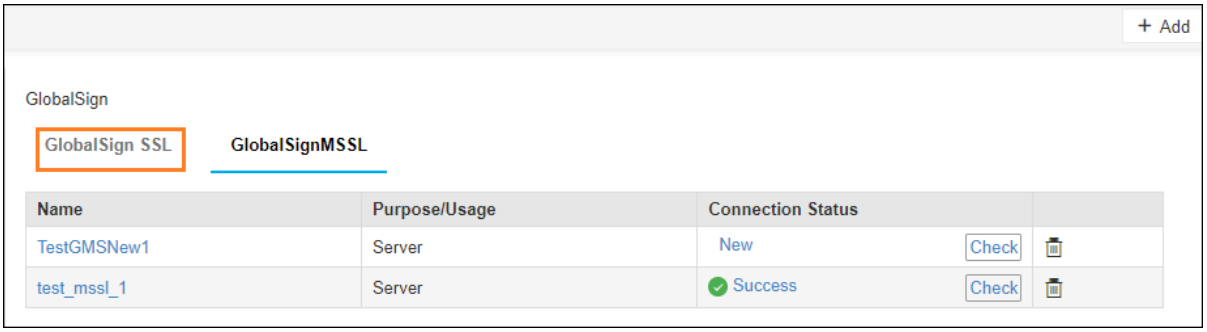
Fields	Description
***SSL URL**	Base URL of the SSL API.
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

7. Click **Save**.

Validating GlobalSign SSL

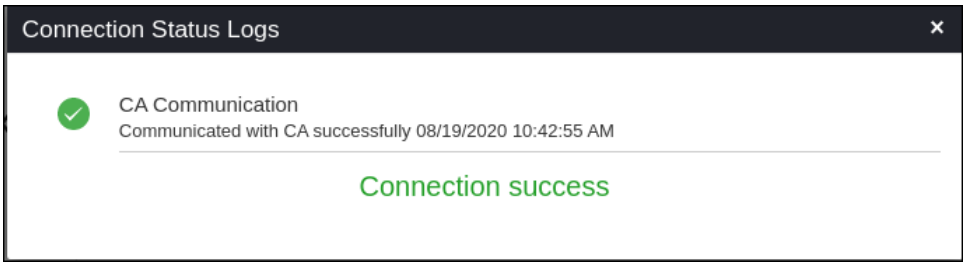
Once the GlobalSign SSL settings are added validation needs to be done to check whether the connection between AppViewX and GlobalSign SSL is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click **GlobalSign SSL** from the left pane of the page.
   The **GlobalSign SSL** home page is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the Connection Status will be shown as either Success or Failure.



GoDaddy CA

- Before you begin
- Configuring GoDaddy
- Validating GoDaddy
- View GoDaddy Product Units

Before you begin

The prerequisites for configuring GoDaddy CA in AppViewX are as follows:

1. GoDaddy Customer Number, API key, and secret are required to make API Requests from AppViewX in order to perform CLM (Certificate Lifecycle Management) operations.
2. AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.
3. Customer Number, API key, and secret configuration in GoDaddy Account:
   a. After logging into the GoDaddy portal with proper account credentials go to https://developer.godaddy.com/keys
   b. Users will be asked to add an optional name, and the secret will be displayed which needs to be copied and will not be displayed further.
   c. This API key and secret will be used for further communication.
   d. Customer Number details are available on the Accounts page of the GoDaddy website
4. Product units should be available in the customer's GoDaddy account to perform CLM operations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring GoDaddy

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GoDaddy** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the GoDaddy CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain the Base URL of the GoDaddy CA API instance. For example: https://api.godaddy.com

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Customer Number**	Each user will have a unique customer number which is used to obtain the certificates from the GoDaddy CA account.
***API Key**	API key generated in the GoDaddy portal which is used for GoDaddy API communications.
***API Secret**	API Secret generated in the GoDaddy portal which is used for GoDaddy API communications.
First Name	First name of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes.
Last Name	Last name of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes.
Email Address	Email Id of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes. **Note**: Valid email address.
Phone Number	Phone number of the GoDaddy Account user as provided in the portal to be used for certificate creation purposes. **Note:** Phone numbers must contain a minimum of 7 and a maximum of 15 numeric values.
**: Mandatory fields*	

6. Click **Save**.

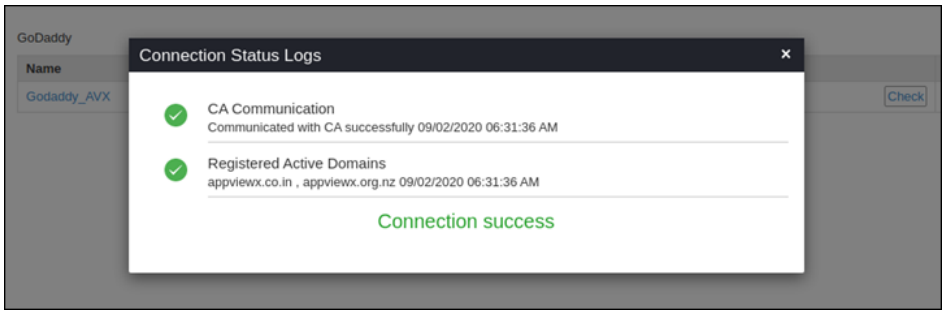
Validating GoDaddy

Once the GoDaddy settings are added validation needs to be done to check whether the connection between AppViewX and GoDaddy is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

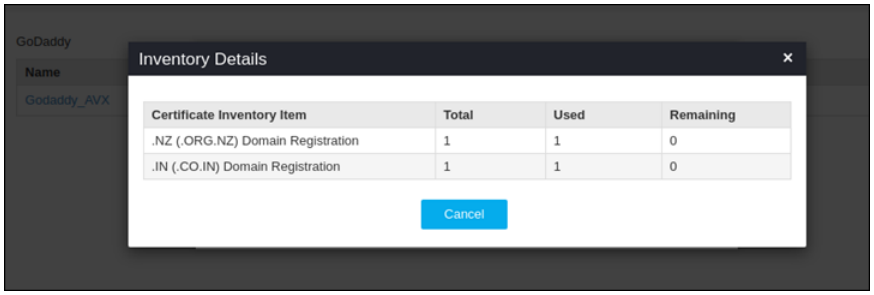
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



View GoDaddy Product Units

Each GoDaddy account has different types of SSL products and units. The below steps will allow users to know the availability of the products and their remaining units.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.
3. On the **GoDaddy** page, click **View** to fetch the product types and the units available for the GoDaddy account configured.
   Once clicked, users can view the available and used product units.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google CA

- Before you begin
- Configuring Google
- Validating Google

Before you begin

The prerequisites for configuring a Google CA account in AppViewX are as follows:

- A Google client certificate or Google client authentication Json for a user having necessary access for enrolling the certificates and for other Certificate Lifecycle Management (CLM) operations.
- AppViewX servers should either have internet access or have a proxy configured in AppViewX general settings.
- The URL https://www.googleapis.com should be reachable from AppViewX.

Configuring Google

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Google**.
   The **Google** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Google** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Configure either Certificate Upload or JSON Upload. These fields are necessary for invoking the Google CA APIs via Certificate Upload for Certificate Management. Select the Certificate Upload check box,
   Update the following details in the **CA Configuration** section as described in the table.

Fields	Description
***Certificate and Key**	Client authentication certificate for API communication.
***Email address**	Email address of the user
***Project Id**	Id of the project
**: Mandatory fields*	

6. Select the JSON Upload check box and configure a CA. Click the Upload button to upload the JSON file.
7. Click **Validate and Fetch**. The issuer names available for the CA account will be fetched along with the validity of the issuers from the Certificate Authority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

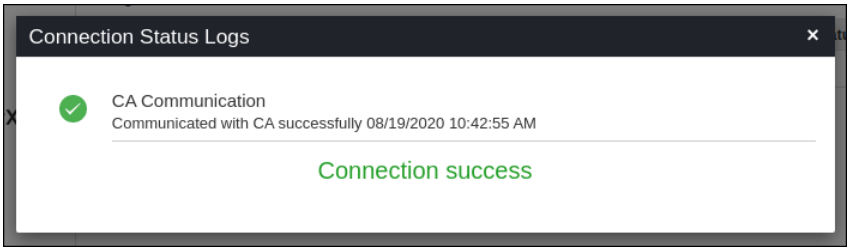
Location	CA Name	Validity	Delete
us-central1	pre-prod-root-ca	05/13/2030 20:02:21	
	testbed-root-ca	05/13/2030 20:27:49	
	prod-root-ca	04/23/2030 12:23:32	
	prod-inter-ca-level-981	06/14/2020 09:03:33	
	prod-inter-ca-level-200	06/14/2020 09:08:43	
	prod-inter-ca-level-201	06/14/2020 09:09:09	
	prod-inter-ca-level-000	06/14/2020 08:51:09	
	prod-inter-ca	04/23/2030 12:27:40	
	prod-inter-ca-level-01	06/14/2020 09:00:50	
europe-west1	test-bed-root-ca	05/13/2030 21:09:13	

8. Click **Save**.

Validating Google

Once the Google settings are added validation needs to be done to check whether the connection between AppViewX and Google is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Google**.
   The **Google** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HashiCorp Vault CA

- Before You Begin
- Configuring HashiCorp Vault
- Validating HashiCorp Vault

Before You Begin

The prerequisites for configuring Hashicorp Vault CA account in AppViewX are as follows:

- Login and password to access AppViewX.
- Base URL, Role ID, and Secret Key for the **APP ROLE method** and Base URL, Access Key, Secret Key, and Role Name for the **AWS method** in the CA Configurations.

Configuring HashiCorp Vault

Steps to Configure HashiCorp Vault CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **HashiCorp Vault**.
   The **HashiCorp Vault** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **HashiCorp Vault** configuration page is displayed.
4. Update the details in the General Information section as described in the table below:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-', and '_' are allowed. Names should not start with special characters.
***Purpose/Usage**	The dropdown contains checkboxes for the certificate type for which the CLM actions will be enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The values are: • Server • Client • Code Signing One or more values can be selected depending on the type of account users need to create.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the details in the **CA Configuration** section as described in the tables below. These fields are necessary for invoking the Hashicorp CA Secret Engine for Certificate Management. The fields displayed in the CA Configuration section depend on the value selected in the **Method** field. The two auth method values are
   - **APP ROLE** - The APP ROLE auth method allows machines or apps to authenticate with Vault-defined roles. An "AppRole" represents a set of Vault policies and login constraints that must be met to receive a token with those policies. An AppRole can be created for a particular machine, or even a particular user on that machine or a service spread across machines. The credentials required for successful login depend upon the constraints set on the AppRole associated with the credentials.
   - **AWS** - The AWS auth method provides an automated mechanism to retrieve a Vault token for IAM principals and AWS EC2 instances. Unlike most Vault auth methods, this method does not require manual first-deploying or provisioning of security-sensitive credentials (tokens, username/password, client certificates, etc), by operators under many circumstances.

CA Configuration for App Role - Field Description Table

Fields	Description
***Base URL**	The base of URL of the CA account.
***Method**	**APP ROLE**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Role ID**	RoleID is an identifier that selects the AppRole against which the other credentials are evaluated. When authenticating against this auth method's login endpoint, the RoleID is a required argument at all times. By default, RoleIDs are unique UUIDs, which allow them to serve as secondary secrets to the other credential information.
***Secret Key**	Secrey Key (SecretID) is a credential that is required by default for any login and is intended to always be secret. They can be created against an AppRole either via generation of a 128-bit purely random UUID by the role itself or via specific, custom values. Similarly to tokens, Secret keys have properties like usage-limit, TTLs and expirations.
**: Mandatory fields*	

CA Configuration for AWS - Field Description Table

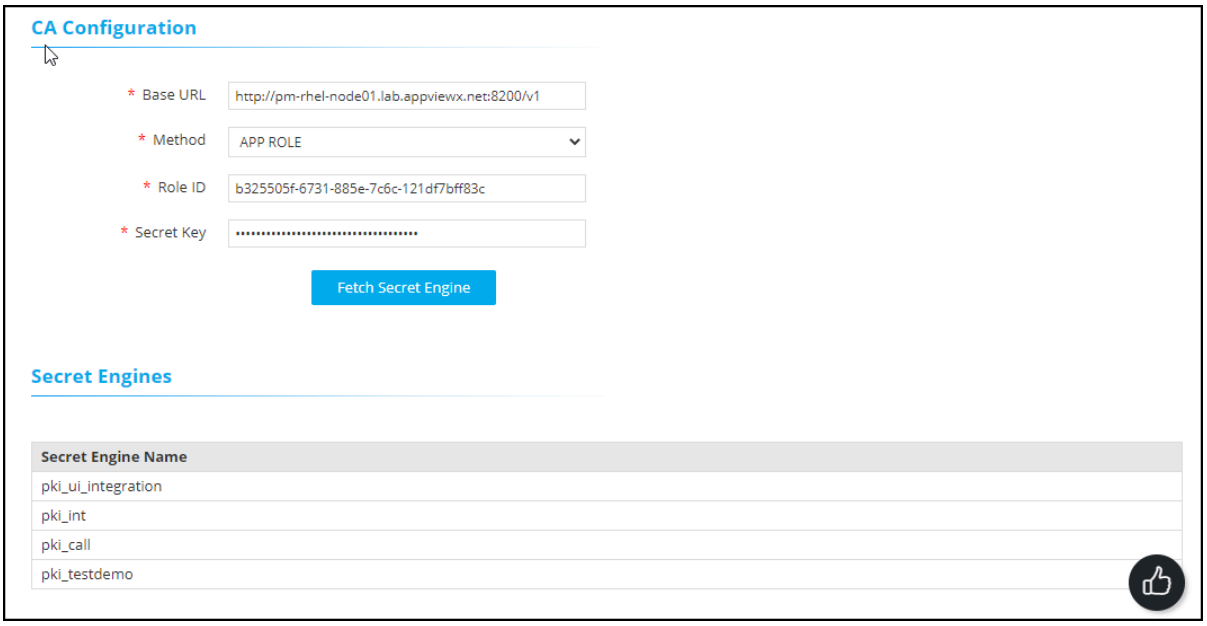
Fields	Description
***Base URL**	The base of URL of the CA account.
***Method**	**AWS**
***Access Key**	Access Keys are used to sign the requests that are sent. Access Key and Secret Key are used for programmatic (API) access to AWS services.
***Secret Key**	Secret Key (SecretID) is a credential that is required by default for any login and is intended to always be secret. Similar to tokens, SecretIDs have properties like usage-limit, TTLs, and expirations.
***Role Name**	The basic mechanism of operation (AWS authorization workflow) is per-role. Roles are registered in the method and associated with a specific authentication type that cannot be changed once the role has been created. Roles can also be associated with various optional restrictions, such as the set of allowed policies and max TTLs on the generated tokens.
**: Mandatory fields*	

The correct values entered in the fields establish a connection with the Hashicorp vault to be able to fetch the secret engine.

6. Click the **Fetch Secret Engine** button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

A list of PKI secret engines is displayed. These will be presented to users in the policy. from where they can select the respective secret engines.



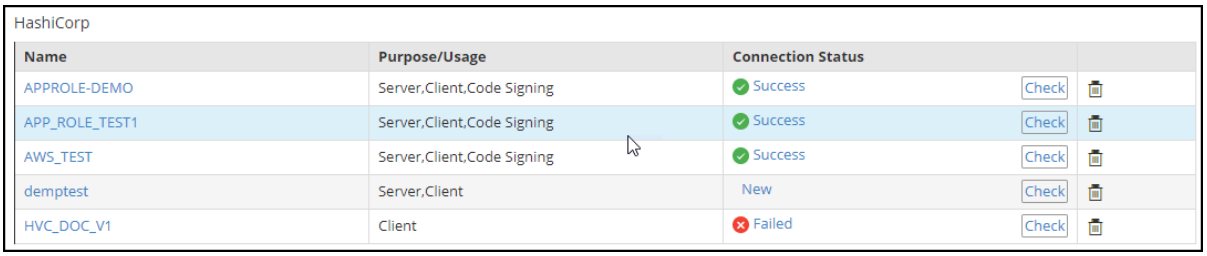
7. Click **Save**.

   The Account details are displayed in a grid at the bottom of the screen, with options to options to edit, check (connection status), and delete.

Editing an Account

1. Go to the **HashiCorp Vault** CA account home page

   The list of Accounts is displayed in the grid.



2. Click the account name from the ‘Name’ column in the grid.

   The General Information and CA Configuration sections are displayed with pre-populated values.

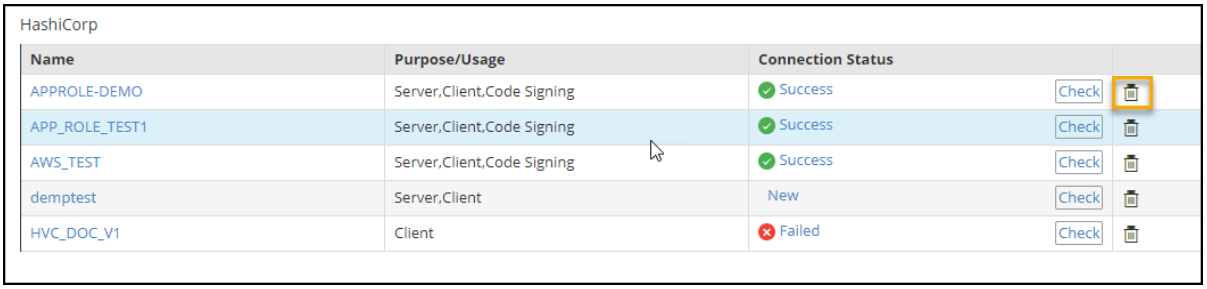
3. Change any of the editable fields and click the **Fetch Secret Engine** button.
4. Click the **Update** button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Deleting an Account

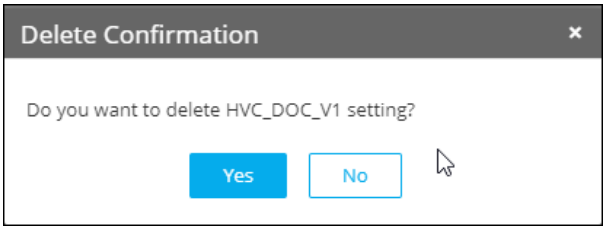
1. Go to the **HashiCorp Vault** CA account home page

   The list of Accounts is displayed in the grid.



2. In the last column of the grid with the listed accounts, click the **Delete** or bin icon.

   The Delete Confirmation pop-up is displayed.



3. Click **Yes**.

Validating HashiCorp Vault

To check the connection status of an account,

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **HashiCorp Vault**.

   The **HashiCorp Vault** home page is displayed.
3. In the Status column of the grid with the listed accounts, click the **Check** button.

   The Success or Failure value is displayed.
4. Update the account details accordingly to get a “success” status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HydrantID CA

- Before You Begin
- Configuring HydrantID CA
- Validating HydrantID CA

Before You Begin

The prerequisites for configuring a HydrantID CA account in AppViewX as follows:

1. To create a CA configuration the following values are required:
   - Base URL
   - API Key ID
   - API Key

   Once the organization (AppViewX) has subscribed for a HydrantID account, you will be provided with a **Username**, **Password**, and **Login URL**.
2. The API Key ID and API Key should be of the following User Roles in HydrantId:
   - Account Auditor
   - Organization Admin
   - Organization Auditor
   - Requestor
3. Users with role **Account Admin** in the HydrantID application can create the above roles. Only account admins can generate the API Key ID and API Key for the roles. Both values can be viewed for a limited time only. Ensure to note these values after the roles are added.

Configuring HydrantID CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **HydrantID**.
   The **HydrantID** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The HydrantID CA details page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. Permissible special characters are '.', '-','_'. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Server, Client and Code-signing are the supported types.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the HydrantId APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain the hostname of the HydrantID CA instance and used for constructing the API requests. the default value is https://acm.hydrantid.com/api/v2
***API Key ID**	Enter the API Key ID generated in the HydrantID application. Its is a unique value specific to the user created in hydrant and is used to authenticate the user.
***API Key**	Enter the API Key generated in the HydrantID application. Its is a unique value specific to the user created in hydrant and used to authenticate and authorize requests.
**: Mandatory fields*	

6. Click **Fetch hydrantID policies**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

A list of policies associated with the account are displayed. These are made available from HydrantID and are used for requesting different types of certificates.

Note: Configuration can only be saved in AppViewX if the profiles are available.

7. Update the following details in the **Advanced Settings** section as described in the table.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	A check box field when selected will fetch the certificated immediately after CSR Submission on enrollment, renew, and reissue of certificate with the retry count and retry frequency as described below.
***Retry Count**	The number of times the polling will take place after CSR submission. Enter a value between 1 and 10.
***Retry Frequency**	The duration of the polling. enter the value between 1 and 30seconds.
**: Mandatory fields*	

8. Click **Save**.
   The created HydrantID configuration settings will be added. A pop-up message is displayed as **<CA_name> Settings Added**.

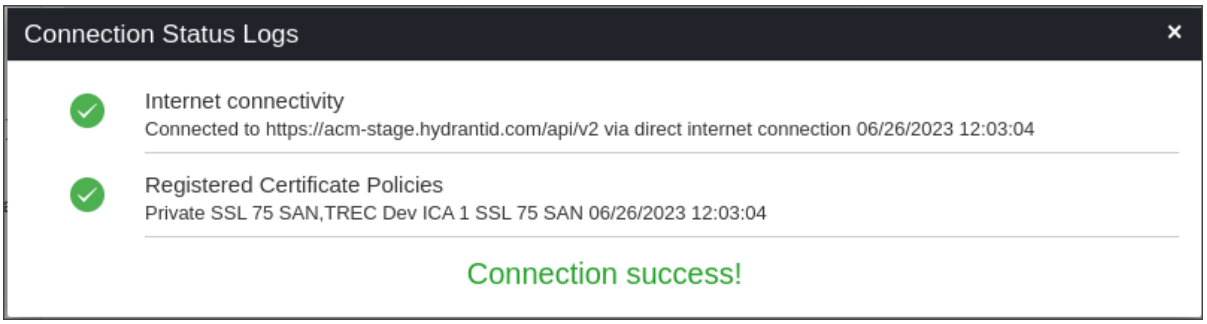
Validating HydrantID CA

Once the HydrantID settings are added, validation needs to be done to check whether the connection between AppViewX and HydrantID is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **HydrantID**.
   The **HydrantID** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**



IDnomic CA

- Before you begin
- Configuring IDnomic CA
- Validating IDnomic CA

Before you begin

The prerequisites for configuring IDnomic CA account in AppViewX are as follows:

- CA Base URL
- Partition name
- Client authentication certificate (.p12 or .pfx format)
- (*Optional*) SOAP signing authentication certificate (.p12 or .pfx format)
- (*Optional*) RA Base URL
- (*Optional*) RA client authentication certificate (.p12 or .pfx format)

Configuring IDnomic CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **IDnomic**.
   The **IDnomic** home page is displayed.
3. Click the **Configure Now** or **+Add** icon from the middle or top-right of the page respectively.
   The IDnomic configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

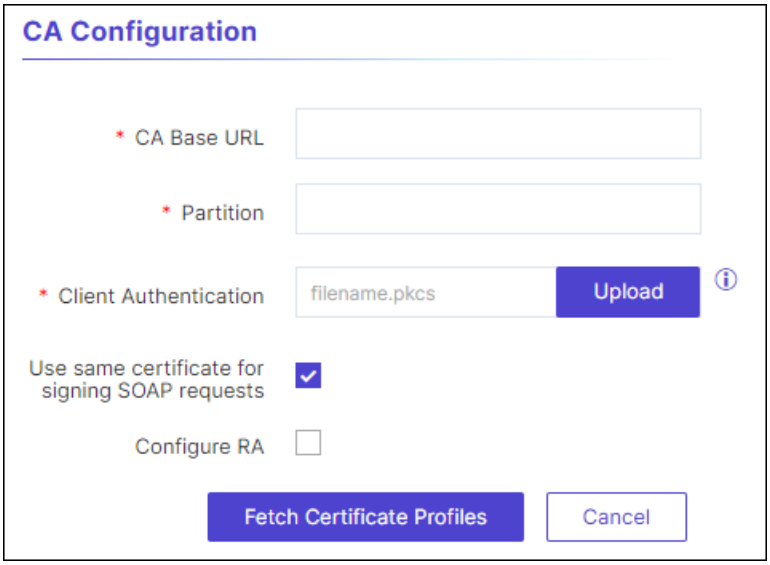
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General Information - Field Description table

Fields	Description
***CA Account name**	A unique name to identify the CA setting No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

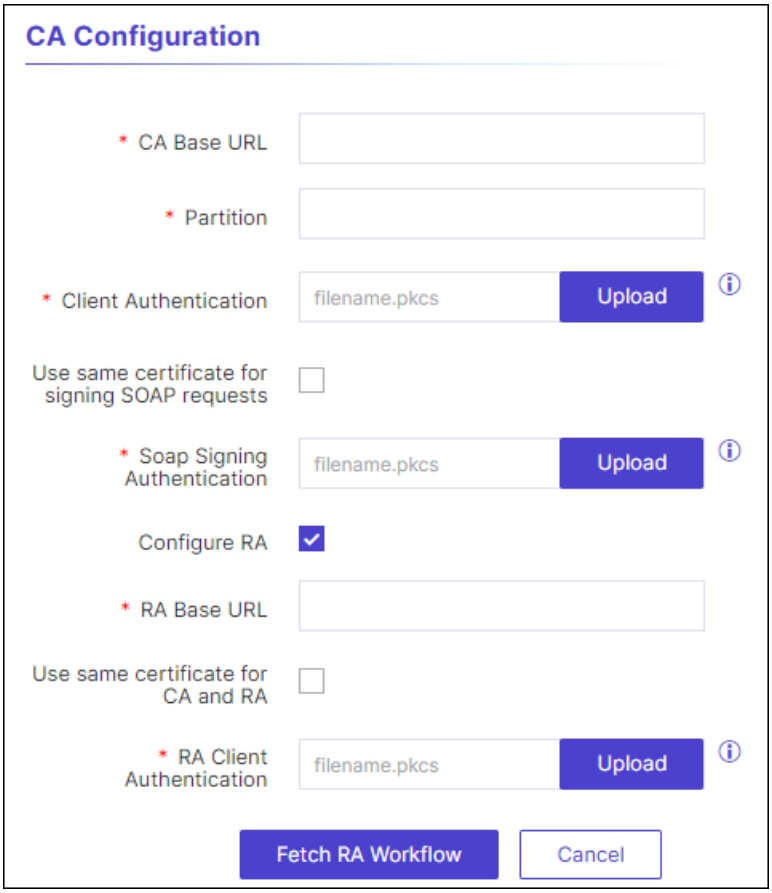
5. Update the following details in the **CA Configuration** section as described in the table below.

Figure 1. Default CA Configuration



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Figure 2. CA Configuration with RA



CA Configuration - Field Description table

Fields	Description
***CA Base URL**	Enter the base URL of the IDnomic CA API instance. For example: https://api-ca.idnomic.com
***Partition**	The name of the partition assigned to the organization's application; it is the workspace dedicated to the organization. The partitioning system allows implementing multi-tenancy within ID CA and ID RA. Partitions are defined in a tree structure, each node being a partitioning in which resources (e.g. Configurations, Certificate, etc) can be attached. According to the customer's needs we can isolate or share common resources.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Client Authentication**	Upload the certificate for client authentication in the .p12 or .pfx format only.
Use same certificates for signing SOAP requests	If checked, allow user to use the same certificate uploaded in Client certificate field, if not checked, you can upload another certificate in the enabled field **Soap Signing certificate**.
***SOAP Signing Authentication**	Upload the certificate for soap signing authentication in the .p12 or .pfx format only.
Configure RA	The field is unchecked by default. If you want to allow a user or device to request a digital certificate from a specific website or application you can select the checkbox and update the fields below. A registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.
***RA Base URL**	Enter the base URL of the IDnomic RA API instance. For example: https://api-ra.idnomic.com
Use same certificate for CA and RA	This field is checked by default. In that case, use the same client certificate uploaded in the “Client Certificate” section. If unchecked, you may upload a new certificate in the enabled field labeled as **RA Client Authentication**.
***RA Client Authentication**	Upload the certificate for RA client authentication in the .p12 or .pfx format only.
**: Mandatory fields*	

6. Click **Fetch Certificate Profiles**. (If RA is used the button label changes to **Fetch RA Workflow**)
   If only CAs are used in the configuration, then a list of certificate profiles are displayed and if RAs are configured then only the certificate RA workflows are displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Click **Save**.
   A confirmation message will appear “Validation Policy fetched and settings have been updated.” and the CA is created successfully. The connection status for the CA is displayed as New.

Validating IDnomic CA

Once the IDnomic settings are added validation needs to be done to check whether the connection between AppViewX and IDnomic is properly configured. To validate the IDnomic CA,

1. Go to **(Menu) > CERT+ > ADMINISTRATION > Certificate Authority.**
2. From the displayed CA, Select **IDnomic**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the Connection Status will be shown as either Success or Failure.

Figure 3. RA Validation

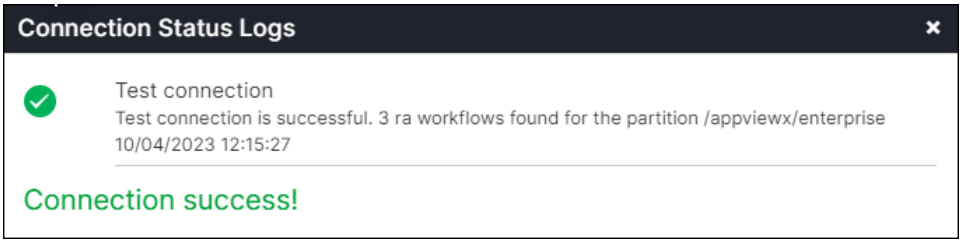
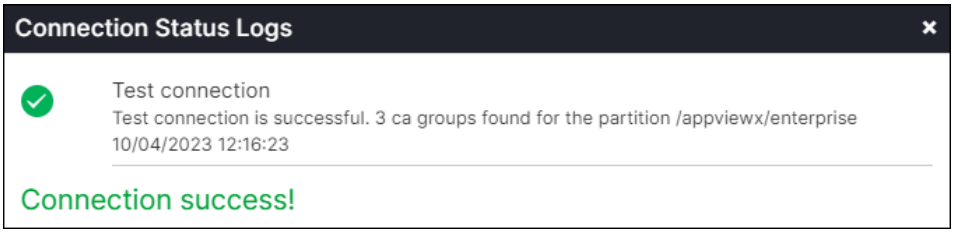


Figure 4. CA Validation



InCommon CA

- Before you begin
- Configuring InCommon CA
- Validating InCommon CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before you begin

The prerequisites for configuring InCommon CA account in AppViewX are as follows:

- InCommon Certificate Manager credentials having necessary access for enrolling the certificates.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Check Proxy Setup for the steps to configure the **proxy. https://adminguide.appviewx.com/proxy-4**
- Username and Password as set up in the Certificate Manager tool.
- An OrgID as provided by InCommon Certificate Manager.
- The login URL and URI.

Configuring InCommon CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **InCommon**.
   The **InCommon** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **InCommon** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Purpose/ Usage**	Certificate Type for which CLM actions will be enabled. Eg. Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the InCommon CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain just the hostname of the InCommon CA instance. Eg - https://cert-manager.com/customer/<<customer_uri>>/ssl- here base URL is **https://cert-manager.com.** **Note:** No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Login URL**	URI specific to the InCommon CA Customer Account. Eg https://cert-manager.com/customer/<<customer_uri>>/ssl- here URI is **customer_uri**.
***User Name**	User name for the account created with InCommon CA.
***Password**	Password for the account created with InCommon CA.
***Organization ID**	InCommon supports organization hierarchy. Id of the **Organization Unit/ Department** in which Certificates need to be managed has to be specified here. **CLM** actions done using this CA account will be specific to this particular organization's id/department.
*: Mandatory fields **Note:** If the certificates from multiple organization's units/departments need to be managed, then a separate CA has to be configured for each organization unit/department in the Incommon CA setting page.	

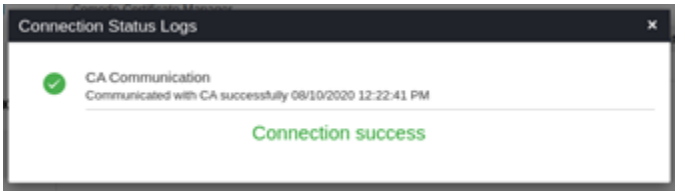
6. Select **Fetch Certificate Types**
   The Certificate types available for the CA account will be fetched from the Certificate Authority.
7. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Validating InCommon CA

Once the InCommon settings are added validation needs to be done to check whether the connection between AppViewX and InCommon is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **InCommon**.
   The **InCommon** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



Let's Encrypt CA

- Before you begin
- Configuring Let's Encrypt CA
- Validating Let's Encrypt

Before you begin

The prerequisites for configuring Let's Encrypt CA account in AppViewX are as follows:

- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Check Proxy Setup for the steps to configure proxy. https://adminguide.appviewx.com/proxy-4
- Any one of the following Let's Encrypt certificate enrolment URL as per requirement :
  - https://acme-staging-v02.api.letsencrypt.org for **staging**.
  - https://acme-v02.api.letsencrypt.org for **production**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Let’s Encrypt CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Let's Encrypt**.
   The **Let's Encrypt** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Let's Encrypt configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***Name**	A unique name to identify the CA setting. **Note:** No special characters other than ‘.’, ‘-’,’_’ are allowed. The name must not start with special characters.
***Purpose/Usage**	The certificate types will be managed by these settings. For now, Let’s Encrypt is having only one purpose **Server**.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Let’s Encrypt CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Let’s Encrypt certificate enrolment URL either staging or production based on the requirement.
***Email ID(s)**	Enter email ID(s) in this field to receive notifications from Let's Encrypt. Multiple email ID must be separated by comma (,).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. Click **Save**.

Validating Let’s Encrypt

Once the Let’s Encrypt settings are added validation needs to be done to check whether the connection between AppViewX and Let’s Encrypt is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Let's Encrypt**.
   The **Let's Encrypt** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Microsoft Enterprise CA

- Before you begin
- Configuring Microsoft Enterprise CA
- Validating Microsoft Enterprise

Before you begin

The prerequisites for configuring Microsoft Enterprise CA in AppViewX are as follows:

- AppViewX Windows Gateway installer should be installed in a windows machine, running and reachable from AppViewX vendor plugin through the Communication Modes described below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Communication Mode Table

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account.
	User permission	NA	Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users Enroll permission at Certificate template level for the service account or the service account group or authenticated users
	Services	RPC service	RPC service certutil.exe command availability
	Ports	NA	135 as the incoming port
POWERSHELL	User account type	Service account	Service account.
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability.
	Ports	NA	5985

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Communication Mode Table (continued)

Communication mode	Category	Windows gateway machine	Microsoft CA
WMI	User account type	Service account	Service account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	NA.	135, 445 or 139

Configuring Microsoft Enterprise CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Enterprise** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
5. Enter/Select the CA **General Information**.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than ‘.’, ‘-’,’_’ are allowed. Names should not start with special characters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example. Server, Client, Code Signing
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Enter/Select the **CA Configuration** details.

CA Configuration - Field Description Table

Fields	Description
Windows Gateway Mode	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).
***Windows Gateway URL**	For **Windows Gateway Mode** = **External**, enter the URL of the endpoint where the AppViewX Windows Gateway Agent is installed and running.
Command Execution Type	Select the command type that will be used for communication with the External AppViewX Windows Gateway Agent. **Note:** The integrated gateway uses only the PowerShell command execution type and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Command execution host (IP/FQDN)	**Note:** This field is displayed when **Windows Gateway Mode** = **Integrated**. Enter the IP address/FQDN of the remote Windows device that the integrated gateway will use for CA communication.
***Credential Type**	You will be required to enter credentials to access the command execution host/Windows device on which the gateway agent is running. From this dropdown list, select the mode through which the credentials will be entered (manually or fetched from a credential list).
***Username**	Enter the username for accessing the Windows device.
***Password**	Enter the password for accessing the Windows device.
Client Authentication Certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

7. Click **Fetch CA Names** to retrieve CAs accessible from Windows Gateway installed machine. Upon successful completion of Fetch CA Names, all reachable CAs listed in **Select CA**.
8. Click on one specific CA and proceed.

CA Details - Field Description Table

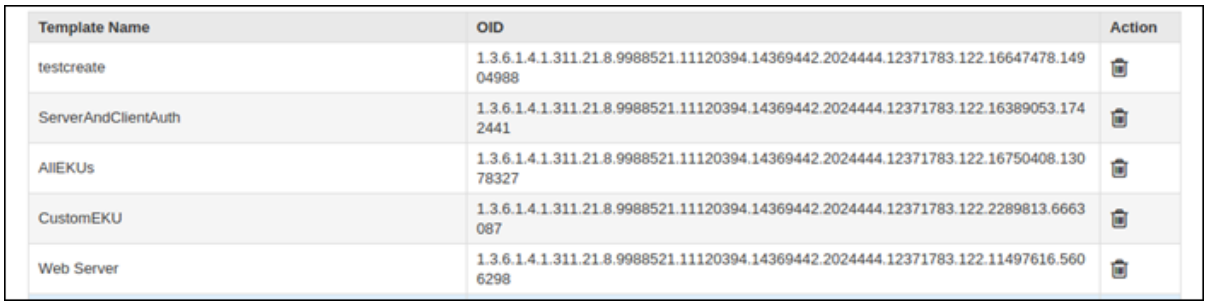
Fields	Description
Select CA	All the reachable CAs are listed here.
***CA Machine Hostname**	Host name of the CA Machine will be auto-filled.
***CA Name**	Name of the CA chosen which will be auto-filled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
CA Manager Approval	Approves the pending enroll / Renew request submitted from AppViewX Certificate.
***Time Zone**	To perform scheduled and Optimized CA discovery, please provide time zone value.
**: Mandatory fields*	

a. Configure the **Template Details**.

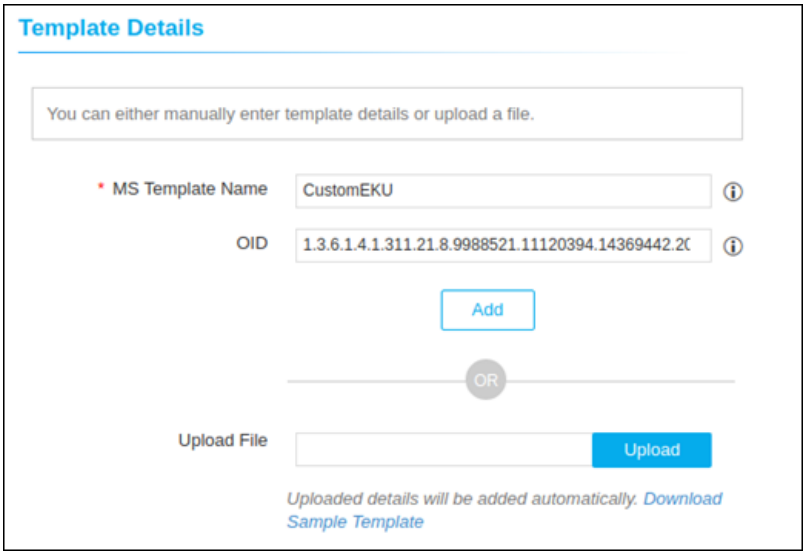
Once CA is selected from the **Select CA** list, the **Template** details should have auto-filled as shown below.



Note: If the desired template is not listed, it might not be published in AD. Users can add it manually through MS Template name and OID fields as shown below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

b. In the Template Details section, select/enter the details as shown below.



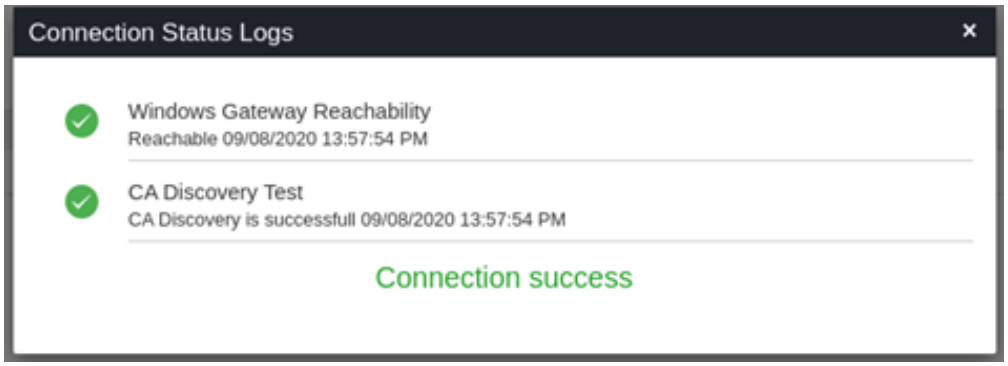
9. Click **Save.**

Validating Microsoft Enterprise

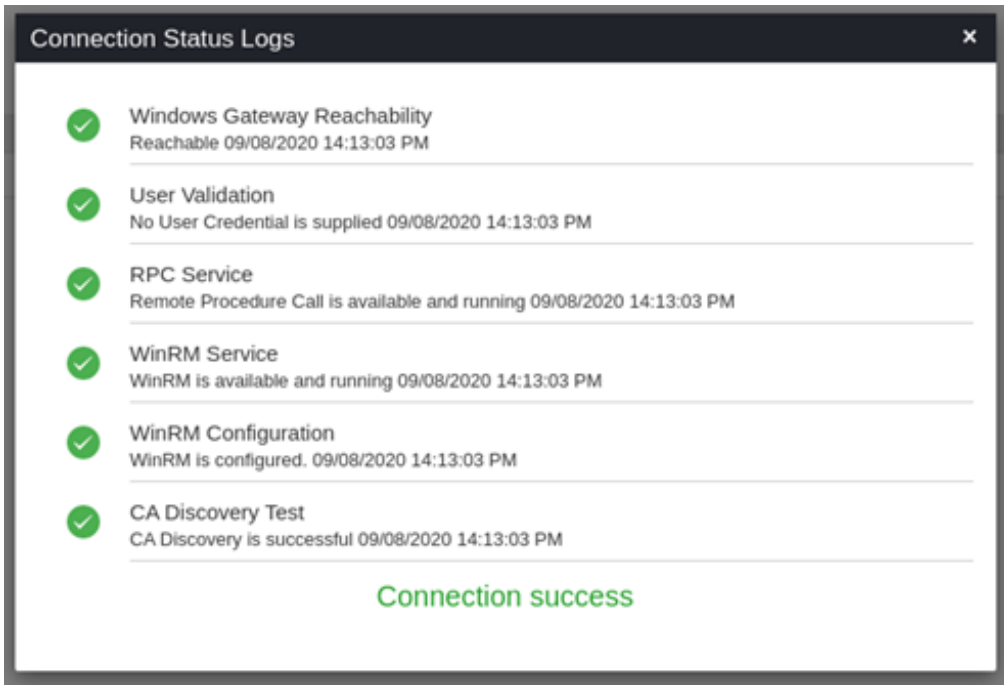
Once the Microsoft Enterprise settings are added validation needs to be done to check whether the connection between AppViewX and Microsoft Enterprise is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Enterprise** tab.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

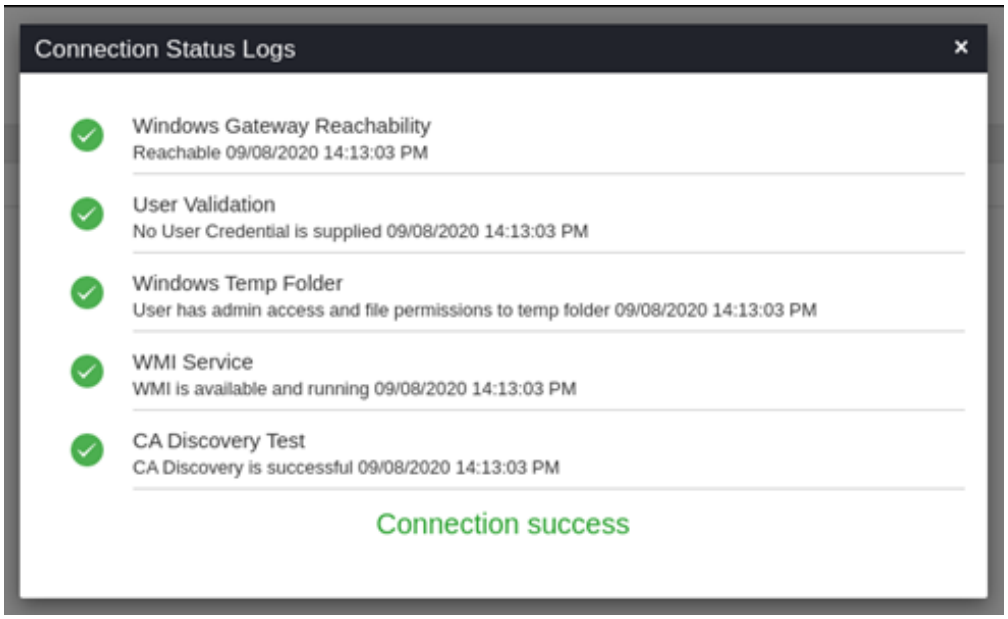


Success Scenario for Native API

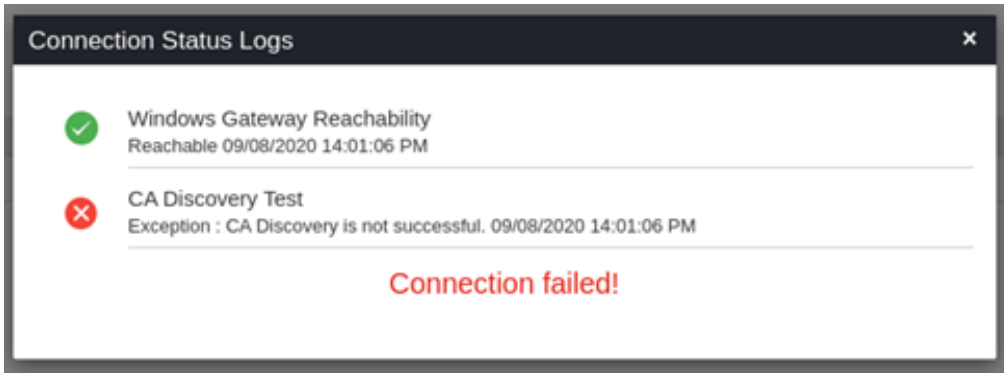


Success Scenario for Powershell

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Failure scenario for WMI



Microsoft Standalone CA

- Before you begin
- Configuring Microsoft Standalone CA
- Validating Microsoft Standalone

Before you begin

The prerequisites for configuring Microsoft Standalone CA in AppViewX are as follows:

- AppViewX Windows Gateway installer should be installed in a windows machine, running and reachable from AppViewX vendor plugin through the Communication Modes described below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Communication Mode Table

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account
	User permission	NA	Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users Enroll permission at Certificate template level for the service account or the service account group or authenticated users
	Services	RPC service	RPC service certutil.exe command availability
	Ports	NA	135 as incoming port
POWERSHELL	User account type	Service account	Service account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service,WinRM Service,WinRM Configuration, Powershell remoting,certutil.exe command availability
	Ports	NA	5985

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Communication Mode Table (continued)

Communication mode	Category	Windows gateway machine	Microsoft CA
WMI	User account type	Service account	Service account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	NA	135, 445 or 139

Configuring Microsoft Standalone CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Standalone** tab.
4. In the Status column of the grid with the listed accounts, click and then click **+Add** icon or **Configure Now** button.
5. Enter/Select the CA **General Information**.

General Information - Field Description Table

Fields	Description
Name	A unique name to identify the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server, Client, and Code Signing.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Enter/Select the **CA Configuration** details.

CA Configuration - Field Description Table

Fields	Description
Windows Gateway Mode	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).
***Windows Gateway URL**	For **Windows Gateway Mode** = **External**, enter the URL of the endpoint where the AppViewX Windows Gateway Agent is installed and running.
Command Execution Type	Select the command type that will be used for communication with the External AppViewX Windows Gateway Agent.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The integrated gateway uses only the PowerShell command execution type and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
Command execution host (IP/FQDN)	**Note:** This field is displayed when **Windows Gateway Mode** = **Integrated**. Enter the IP address/FQDN of the remote Windows device that the integrated gateway will use for CA communication.
***Credential Type**	You will be required to enter credentials to access the command execution host/Windows device on which the gateway agent is running. From this dropdown list, select the mode through which the credentials will be entered (manually or fetched from a credential list).
Username	Enter the username for accessing the Windows device.
Password	Enter the password for accessing the Windows device.
Client Authentication Certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

7. Click **Fetch CA Names** to retrieve CAs accessible from Windows Gateway installed machine.
   Upon successful completion of Fetch CA Names, all reachable CAs listed in **Select CA**.
8. Click on one specific CA and proceed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Dynamic Fields for Select CA Section

Fields	Description
Select CA	All the reachable CAs are listed here.
***CA Machine Hostname**	Host name of the CA Machine will be auto-filled.
***CA Name**	Name of the CA chosen which will be auto-filled.
CA Manager Approval	Approves the pending enroll / Renew request submitted from AppViewX Certificate.
**: Mandatory fields*	

9. Click **Save**.

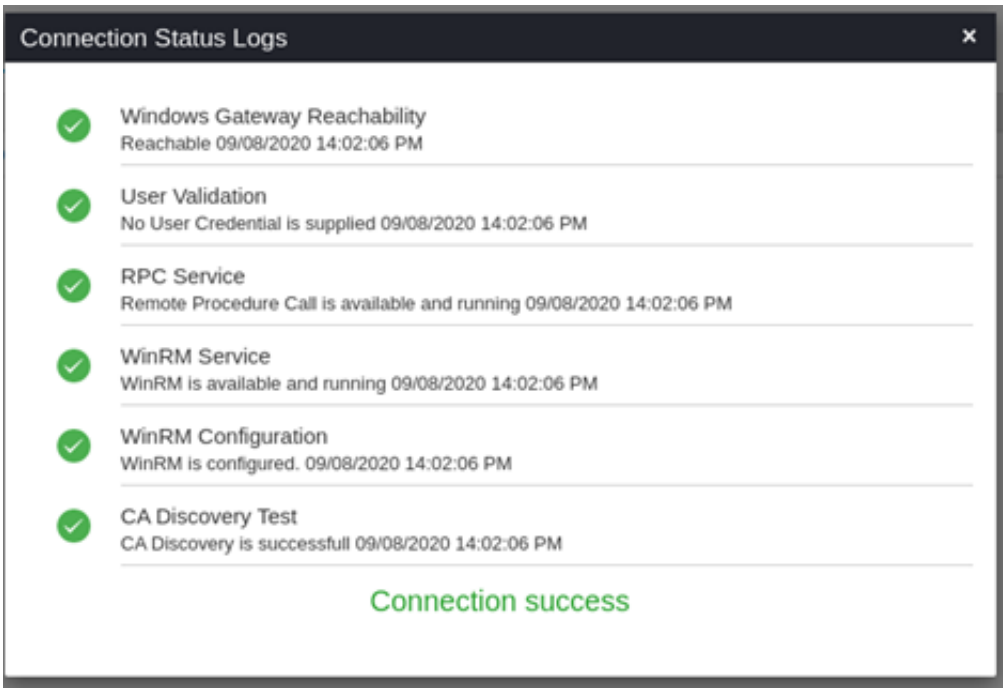
Validating Microsoft Standalone

Once the Microsoft Standalone settings are added validation needs to be done to check whether the connection between AppViewX and Microsoft Enterprise is properly configured.

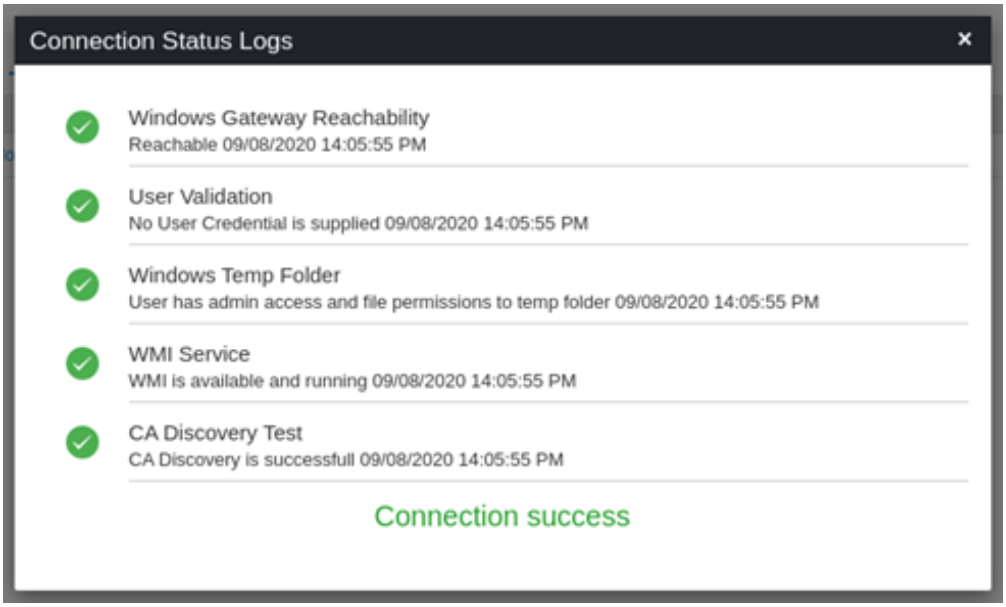
1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Standalone** tab.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.Success scenario for Native APISuccess scenario for PowershellSuccess scenario for WMI.

   Success scenario for Native API

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

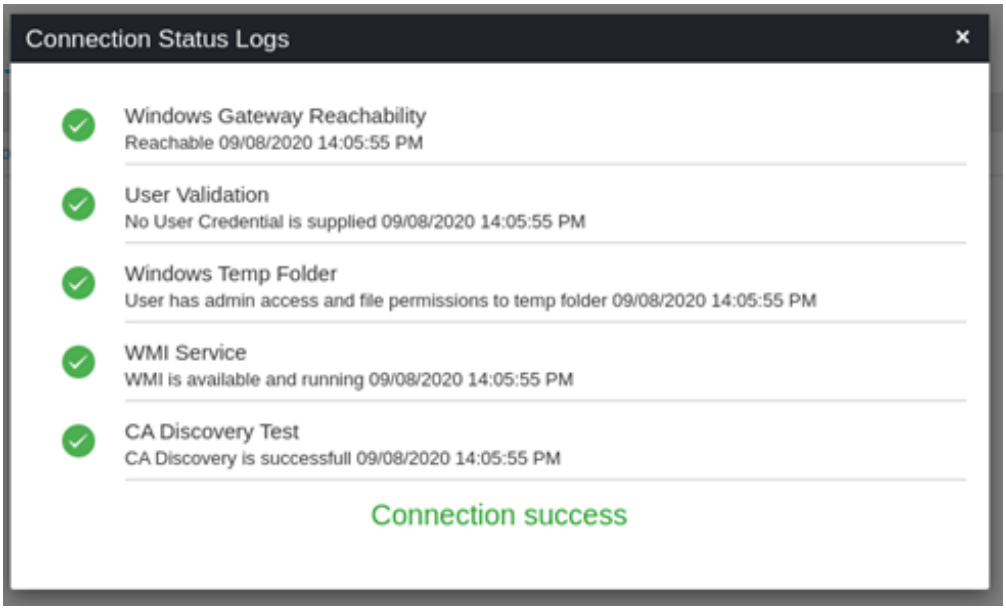


Success scenario for Powershell



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Success scenario for WMI



Nexus CA

- Before you Begin
- Configuring Nexus
- Validating Nexus

Before you Begin

The prerequisites for configuring a Nexus CA account in AppViewX are as follows:

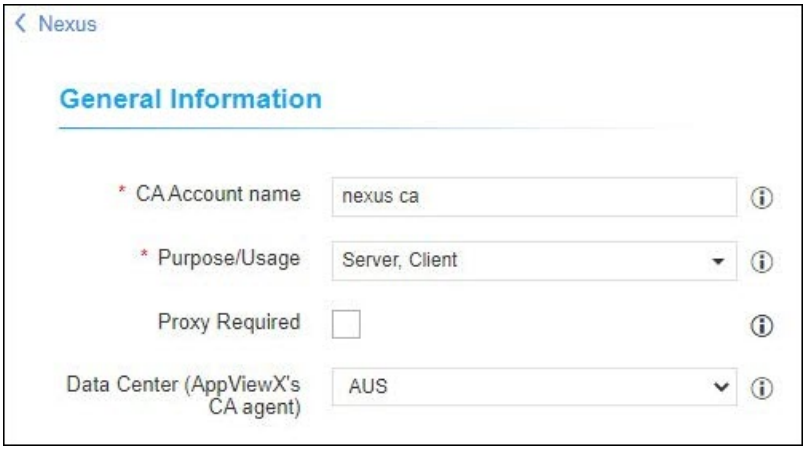
- A Nexus Account with Administrator role Access.
- Before discovery or enrollment, the customer must upload the CA certificates manually.
- The AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Configuring Nexus

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Nexus**.
   The **Nexus** home page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The Nexus configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

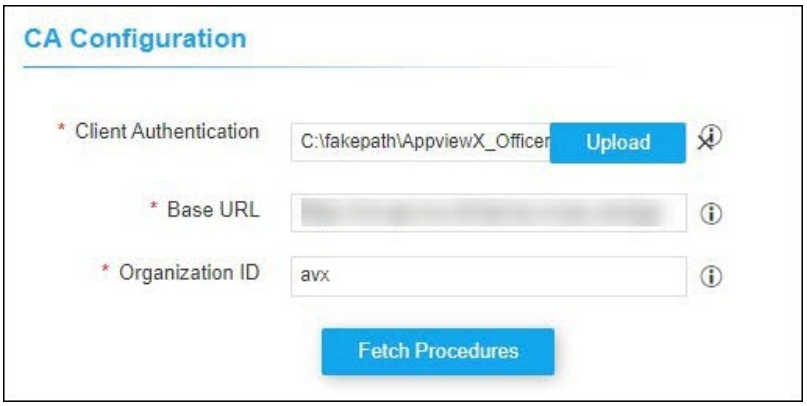


General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, server and clients
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

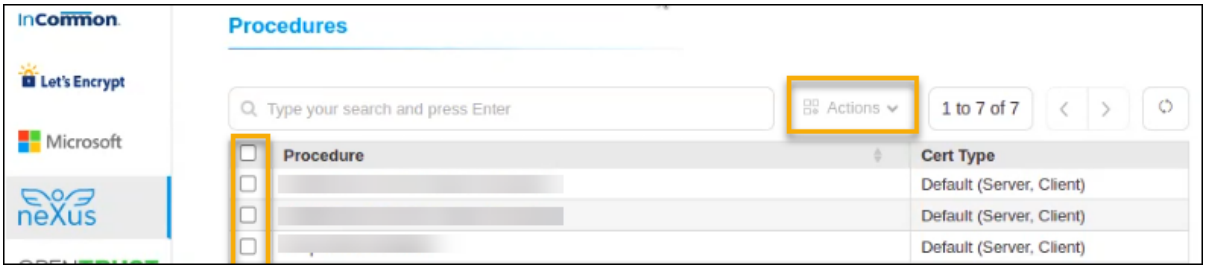


CA Configuration - Field Description Table

Fields	Description
***SSL URL**	Base URL of the SSL API
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

6. Select **Fetch Procedures**.

   The procedures available in the Nexus CA account will be fetched and listed for the specific user.



7. To map the fetched procedures, click on one or many and click the **Actions** dropdown
   - **CASE 1** - If the user selects Server only in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will only have - **Map as Server**. and **MAP as Default**
   - **CASE 2** - If the user selects Client only in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will only have - **Map as Client**. and **MAP as Default**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **CASE 3** - If the user selects Server and Client both in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will have both the actions **Map as Client** , **Map as Server**, and **MAP as Default**

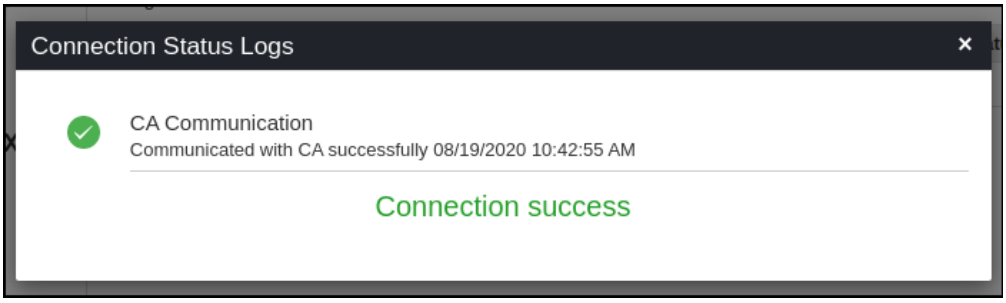


8. Click **Save**.

Validating Nexus

Once the Nexus settings are added, the validation must be done to check whether the connection between AppViewX and Nexus is configured properly.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Nexus**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo CA

- Before you begin
- Configuring Sectigo CA
- Validating Sectigo CA

Before you begin

The prerequisites for configuring a Sectigo CA account in AppViewX are as follows:

1. To create a CA configuration the following values are required:
   - Base URL
   - Login URI
   - Username (The new administrator's login name. Refer point 2.)
   - Password
   - Organization ID (Refer point 4.)

   Once your organization has subscribed for a Sectigo account, you will be provided with a **Username**, **Password**, and **Login URL** for SCM (Sectigo Certificate Manager). The default format of this URL is https://cert-manager.com/customer/<customer URI>/, where **<customer URI>** is a path segment specific to your company.
2. The Username and Password should be of the following administrators:
   - Master Registration Authority Officer (MRAO)
   - Registration Authority Officer (RAO)
3. The above administrators should have the following privileges.

Privileges	
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to Certificates > SSL Certificates.
Allow SSL auto approve	SSL certificates requested by the MRAO are automatically approved, and those requested by a RAO SSL and DRAO SSL are automatically approved by the administrator of same level and await approval from higher level administrator.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To review the administrator details in the SCM, navigate to **Settings > Admins**, select the administrator in the list, and click **Edit**. This displays the Edit Client Admin dialog, Add/Edit the necessary privileges and click **Save**.

4. **Organization Id:** Organizations are umbrella entities created by administrators for the purposes of requesting, issuing, and managing certificates for domains and employees. The Organizations page is used to add and modify the organizations.

   To review the organization details in the SCM, navigate to **Organizations**, select the organization in the list, and click **Edit**. This displays the Edit Organization dialog shown in the following illustration.

Configuring Sectigo CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Symantec**.
   The **Sectigo** home page is displayed.
3. (Optional if creating for the first time) Select the **Comodo Certificate Manager** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Sectigo CA details page is displayed.
5. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. *Example*: Server and Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Sectigo CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain the hostname of the Sectigo CA instance and used for constructing the API requests.
***Login URI**	Provide the customer login URI for API authentication.
***User Name**	Enter the Username of the Sectigo portal to communicate with the CA.
***Password**	Enter the Password of the Sectigo portal to communicate with the CA.
***Organization Id**	Enter the organization id used for the certificate lifecycle action. (You will find it in the Organization tab of the Sectigo portal)
**: Mandatory fields*	

7. Click **Fetch Certificate Types**
   The certificate types that are assigned to the configured user which will be used during certificate enrollment, policy creation, through out the product.
8. Update the following details in the **Advanced Settings** section as described in the table.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	A check box field when selected will fetch the certificated immediately after CSR Submission on enrollment, renew, and reissue of certificate with the retry count and retry frequency as described below.
***Retry Count**	The number of times the polling will take place after CSR submission. Enter a value between 1 and 10.
***Retry Frequency**	The duration of the polling. enter the value between 1 and 30seconds
**: Mandatory fields*	

9. Click **Fetch Custom Attributes**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

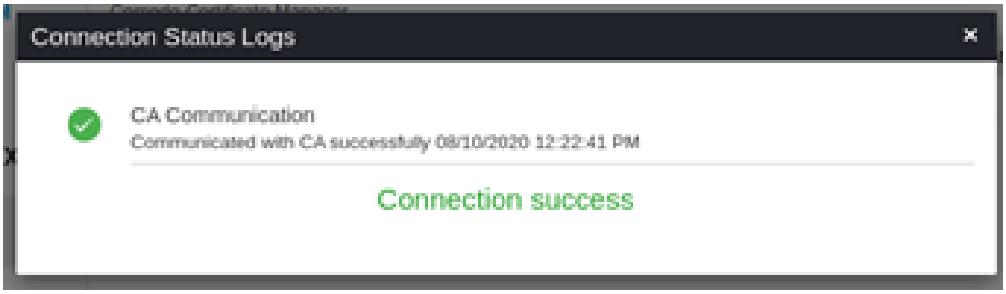
The attributes available for the CA account will be fetched from the Certificate Authority along with the CA and profile names. A pop-up message is displayed as **CA and profiles fetched**.

10. Click **Save**.
    The created Sectigo configuration settings will be added. The pop-up message is displayed as **<CA_name> Settings Added**.

Validating Sectigo CA

Once the Sectigo settings are added, validation needs to be done to check whether the connection between AppViewX and Sectigo is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Sectigo**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



Symantec CA

- Before you begin
- Configuring Symantec CA
- Validating Symantec

Before you begin

The prerequisites for configuring a Symantec account in AppViewX are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- A Symantec client certificate for a user having the necessary access for enrolling the certificates and other Certificate Lifecycle Management(CLM) operations.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Check Proxy Setup for the steps to configure proxy. https://adminguide.appviewx.com/proxy-4
- Symantec users should be associated with the role **“w=VICE2 web services application”**.
- Required organization status should be “valid”.
- If the EV certificate type is enabled, then the EV status of the organization should be “Yes”.
- The required domain should be registered with the organization.
- The required certificate types should be enabled with the required values in the portal.
- Unit values should be available for the required certificate type.

Configuring Symantec CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Symantec**.
   The **Symantec** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Symantec** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than ‘.’, ‘-’,’_’ are allowed. The name must not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Symantec CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Certificate and Key**	Client authentication certificate for API communication. **Note:** Must be a valid <.p12> or <.pfx> file.
***URL**	Symantec URL used for API communications. For example, **https://certmanager-webservices.websecurity.symantec.com/vswebservices/**
***Jurisdiction hash**	Jurisdiction hash of the Symantec account. Available in the top right corner of the Symantec portal.
***First name**	First name of the user.
***Last name**	Last name of the user.
**: Mandatory fields*	

6. Click **Save**.

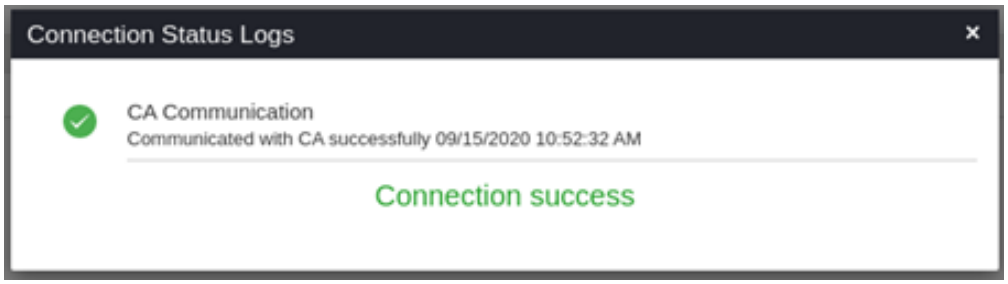
Validating Symantec

Once the Symantec settings are added validation needs to be done to check whether the connection between AppViewX and Symantec is properly configured.

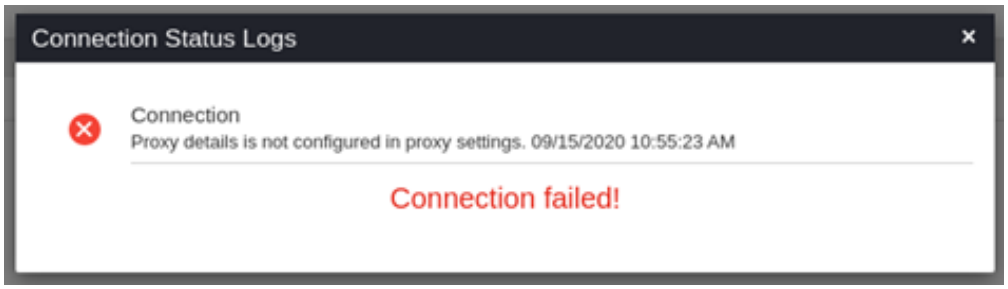
1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Symantec**.
   The **Symantec** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Success Scenario

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Failed Scenario



Trustwave CA

- Before you Begin
- Configuring Trustwave CA
- Validating Trustwave

Before you Begin

The prerequisites for configuring Trustwave CA account in AppViewX are as follows:

- Trustwave API URL. Ex: https://testapi.ssl.trustwave.com/3.0/
- Reachability from AppViewX southbound to Trustwave API URL via proxy or direct internet connection
- Valid credentials for communicating to Trustwave CA via API
- Reseller id
- Account details provided inTrustwave account such as Organization Name, Email address, Organization Address, City, State, Zip code, Country, Phone number
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Trustwave CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Trustwave**.
   The **Trustwave** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Trustwave CA details page is displayed.
4. Configure the **General Information** details as follows:

General Information - Field Description Table

Fields	Description
***CA Account name**	Provide an account name for the CA setting.
***Purpose/Usage**	Choose the certificate categories that will be managed by this setting. Possible certificate categories could be: a. Server b. Code Signing
Proxy Required	Enable this field if the CA communication needs to happen via **Proxy**.
Data Center (AppViewX's CA agent	Choose the appropriate **Data Center**.
**: Mandatory fields*	

5. Configure the **CA Configuration** with information you want to configure:

CA Configuration - Field Description Table

Fields	Description
***API URL**	The Trustwave API URL to communicate. E.g.: https://testapi.ssl.trustwave.com/3.0/
***Username**	The username for API authentication.
***Password**	The password for API authentication.
***Reseller ID**	The Reseller Id for the account.
**: Mandatory fields*	

6. Configure the **Account Details** with information you want to configure:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CA Configuration - Field Description Table

Fields	Description
***Name**	The Organization name given in the Trustwave account.
***Email Address**	The Administrator or organization email address given in the Trustwave account.
***Address**	The Organization Address given in the Trustwave account.
***City**	The city name given in the Trustwave account.
***State**	The state name given in the Trustwave account.
***Zip code**	The zip code given in the Trustwave account.
***Country**	The country code given in the Trustwave account. E.g.: US.
***Phone number**	The phone number given in the Trustwave account.
**: Mandatory fields*	

7. Click **Save**.

Validating Trustwave

Once the Trustwave settings are added validation needs to be done to check whether the connection between AppViewX and Trustwave is properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Trustwave**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

CA Policy

You can enforce your organization standards by configuring **Certificate Policy** in **CERT+**. Thus the attributes of discovered certificates are compared against the certificate policy to ensure they are complaint. If the certificate attribute deviates, it is marked as non-complaint and notified to users. Users can request for a new certificate (in-line to organization standards) to Certificate Authority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before you Begin

Following are the prerequisites for configuring a CA based **Policy** in **CERT+**:

- Certificate Group(s) must be available to map the **Policy** to them.
- CA accounts (settings) must be available to which the policy is going to be created.
- Key Algorithm, Encryption Type must be available under the CA accounts.
- AppViewX permission required (**Accounts > Roles** *- Click here to check Accounts management)*

Access the following

- **CERT+ > Policy > View Policy** - To view the policy.
- **CERT+ > Policy > Add / Modify** - To create/ modify the policy.

- Configuring Policy Details
- Configuring Policy for Amazon CA
- Configuring Policy for Amazon Private CA
- Configuring Policy for Digicert CA
- Configuring Policy for EJBCA CA
- Configuring Policy for Entrust CA
- Configuring Policy for Entrust MPKI CA
- Configuring Policy for GlobalSign Atlas CA
- Configuring Policy for GlobalSign CA
- Configuring Policy for GlobalSign MSSL CA
- Configuring Policy for GoDaddy CA
- Configuring Policy for Google CA
- Configuring Policy for HashiCorp Vault CA
- Configuring Policy for HydrantID CA
- Configuring Policy for IDnomic CA
- Configuring Policy for Let's Encrypt CA
- Configuring Policy for Microsoft Enterprise CA
- Configuring Policy for Microsoft Standalone CA
- Configuring Policy for Nexus CA
- Configuring Policy for OpenTrust CA
- Configuring Policy for Sectigo CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Configuring Policy for Symantec CA
- Configuring Policy for Trustwave CA

Configuring Policy Details

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

   Note: CERT+ is packaged with the following: default policies **Default** and **Certificate-Gateway**.

2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Enter/Select the **Policy Details**.

Field description for Policy Details

Fields	Description
***Policy name**	Enter a unique name for the CA policy. **Note:** No special characters other than **.**, **-**, and _ are allowed. The policy name should not start with special characters.
Description	Enter a description of the policy.
***Policy Enforcement Type**	Select **Strict** (default) or **Suggestive.** • **Strict** - Enforces standards defined in the policy where a user cannot modify any parameters. • **Suggestive** - Suggests policy parameters. A user can modify to the suggested values if required.
Certificate Requests Need Approval	When enabled, this feature will enforce peer approval process for any requests made for creation/renewal/regeneration/reissue or revocation of certificates. Peer approval for requests is defined in the approval workflow.
Enable Access to Private Key	When enabled, allows the user to download private keys from the holistic view.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Enable certificate push-bind access for a read-only user	Enabling this feature will allow a user from a read-only user group to perform certificate push, bind, and rollback operations from the holistic view.
Validate issuer and root certificate for compliance	Enabling this option will validate if the issuer and root of a certificate are also compliant with the standards defined in the policy.
**: Mandatory fields*	

Note: You can configure the **Policy Details** section based on your organization's standards.

4. From the **Group selection** section, select one or more groups to map to the policy.
5. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the Job Scheduler.

Configuring Policy for Amazon CA

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** pane in the left, select **Amazon** .

Field description for Amazon CA Details

Fields	Description
***CA Accounts**	The Amazon CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. From the **CA Accounts** dropdown list., select the required CA account.
6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter/Select the **Certificate Parameters**.

Field description for certificate parameters

Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

10. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Amazon** option to indicate that the details are successfully stored.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click the **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Amazon Private CA

Prerequisites:

- You must configure the CA setting with Amazon Private CA credentials.
- You must have validated and fetched the Amazon Intermediate CAs along with the issuer region details in the CA settings page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Amazon Private CA**.
   The **CA Details** section is updated to display fields relevant to Amazon Private CA.
5. Enter/Select the policy details for Amazon Private CA.

Field description to create CA policy for Amazon Private CA

Field	Description
***CA Accounts**	From the dropdown list, select the certificate authority account.
***Issuer Region**	From the dropdown list, select the issuer region.
***Issuer Name**	From the dropdown list, select the issuer name.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	All the key types are listed with their corresponding bit length. You can select one or more than one bit length - key type pair from the dropdown list. The discovered certificate's key type and bit length will be compared against the selected bit length - key type(s) to to check for compliance with the policy. The selected bit length - key type(s) is enforced while performing any certificate request operations such as new, renew, regenerate. Amazon Private CA supports the following bit type and length:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	<table><tr><th>Type</th><th>Length</th></tr><tr><td>RSA</td><td>2048 4096</td></tr><tr><td>EC</td><td>prime256v1 sec384r1</td></tr></table>
***Hash Function**	From the dropdown list, select one or more than one supported **Hash Function**. The supported hash functions are: • SHA256 • SHA384 • SHA512
***Signature Algorithm**	From the dropdown list, select the required signatire algorithm. **Note:** The issuer will print the issuer algorithm that the users select from the Signature Algorithm in this field.
**: Mandatory fields*	

6. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforcedat the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

7. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against **Amazon Private CA** to indicate that the details are successfully stored.
8. From the **Group selection**, select one or more groups to map to the policy.
9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

   Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy**.
    The policy is created and a confirmation message is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Policy for Digicert CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **DigiCert**.
   The **CA Details** section is updated to display fields relevant to DigiCert.
5. Enter/Select the policy details for DigiCert.

Field description for CA details

Fields	Description
***CA Account**	The GlobalSign CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.
***Division**	Select the division from the dropdown list.
***Certificate Type**	Certificate types corresponding to the selected CA account are listed. Select one (or) more certificate types from the list to create the policy.
***Validity**	Enter a validity period for the certificate. The available options are: **Days** - You can enter more than one validity period in days, to choose one in certificate enrolment. **Month** - You can enter more than one validity period in Months, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment.
**: Mandatory fields*	

6. In the **Vendor Specific Details** section, select/enter the details as listed in the table

Field description for Vendor Specific Details

Fields	Description
***Server Type**	Select the server type from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

7. Click **Add**.
   The CA details are added to the table below the **Add** button and a confirmation message is displayed.

> **Note:** You can use the **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

8. Select the **Bit Length -Key Type**, **ECDSA curve**, and the **Hash Function**.
9. Based on your organization's policies and standards, enter/select values for the **Certificate Parameters**.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	.
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Digicert** to indicate that the details are successfully stored.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the Job Scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message displays.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Policy for EJBCA CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **EJBCA**.
   The **CA Details** section is updated to display fields relevant to EJBCA.
5. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

   Field descriptions for the vendor-specific details

Fields	Description
End entity user name	Enter the name of the end entity user.
***End entity Profile name**	Enter the name of the end entity profile.
***Issuer Common Name**	Enter the common user name.
***Certificate Profile Name**	Enter a certificate profile name.
**: Mandatory fields*	

6. Click **Add** .
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), - (hyphen), . (period)
*: Mandatory fields	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **EJBCA** to indicate the details are successfully stored.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the Job Scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Entrust CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Entrust**.
   The **CA Details** section is updated to display fields relevant to Entrust.
5. Enter/Select the CA details for Entrust.

Field Description for CA Details

Fields	Description
***CA Accounts**	The Entrust CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The **Certificate Types** corresponding to the selected CA account are listed. Select one (or) more certificate types from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. In the **Vendor Specific Details** section, select/enter the details as listed in the table:

Fields	Description
Additional Emails	Enter the valid email address in the field.

7. Click **Add**.
   The CA details are saved to the table and the confirmation message displays.

   You can use the **Edit** option in the table to modify the configuration and **the Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

10. Enter/Select the **Certificate parameters to be Compared or Enforced**.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Use this toggle button to restrict the creation of wild card certificates using the policy.
Disable CT Logs	For Entrust CA, AppViewX lets you disable sending certificate data to the Certificate Transparency logs everytime a certificate is enrolled, renewed, regenerated, and/or reissued. To do this: • At the time of configuring the Entrust CA policy , turn on the **Disable CT Logs** button. Now, every time this Entrust policy is used to enroll/renew/ regenerate/reissue a certificate, its CT logs will not be generated and the contents of the certificate, including host names, will not be publicly visible.
Host Name	Enter the host name. The host name cannot start and end with a **.** (period)
Allowed Domain Names	Enter from the list of white-listed domain names. To add multiple domain names, press **Enter** after adding each domain name.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

11. Click **Save CA Details** to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Entrust** option to indicate that the details are successfully stored.
12. From the **Group selection**, select one or more groups to map to the policy.
13. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the **Job Scheduler**.

14. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Policy for Entrust MPKI CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Entrust MPKI**.
   The **CA Details** section is updated to display fields relevant to Amazon Private CA.
5. Enter/Select the policy details for Entrust MPKI.

Field description for CA details

Fields	Description
***CA Accounts**	Select a CA account from the list to create the policy. The selected CA account will be listed in the **CA Accounts** table.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length-key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

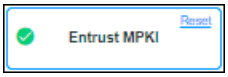
Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **Entrust MPKI** to indicate that the details are successfully stored.



8. From the **Group selection**, select one or more groups to map to the policy.
9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for GlobalSign Atlas CA

Before You Begin: The prerequisites for configuring the policy are as follows:

- Certificate group(s) must be available to map the policy to them.
- CA accounts (settings) must be available to which the policy is going to be created.
- AppViewX permissionis required (**Accounts** > **Roles** - Click here to check Accounts Management).

To configure policy for GlobalSign Atlas CA:

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

   CERT+ is packaged with the following default policies: **Default** and **Certificate-Gateway**.

> **Note:** The **Default** CA Policy will have the **GlobalSign Atlas CA** details.

2. Click **+ Create** to configure GlobalSign Atlas custom policy.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Policy Details**
- **Group Selection**
- **Compliance Check**

4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GlobalSign Atlas**.
   The **CA Details** section is updated to display fields relevant to GlobalSign Atlas.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The GlobalSign Atlas CA accounts configured in the CA settings screen are listed here. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length- key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

The updated fields for the CA are displayed on the right.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Add**.
   The CA details are saved in the table and the confirmation message is displayed.

   You can use the **Edit** (pencil)option in the table to modify the configuration and the **Remove** (bin) option to delete the configuration.

7. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

8. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign MSSL** to indicate that the details are successfully stored.
9. From the **Group selection**, select one or more groups to map to the policy.
10. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

11. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for GlobalSign CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **EJBCA**.
   The **CA Details** section is updated to display fields relevant to EJBCA.
5. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for vendor specific details

Fields	Description
***Incorporating Agency Reg. No**	Enter the agency registration number.
***Designation**	Enter the designation.
***Business Category**	Select the business category from the dropdown list.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.  **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign** to indicate that the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for GlobalSign MSSL CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** to configure a GlobalSign MSSL based policy.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GlobalSign MSSL**.
   The **CA Details** section is updated to display fields relevant to GlobalSign MSSL.
5. Enter/Select the CA details.

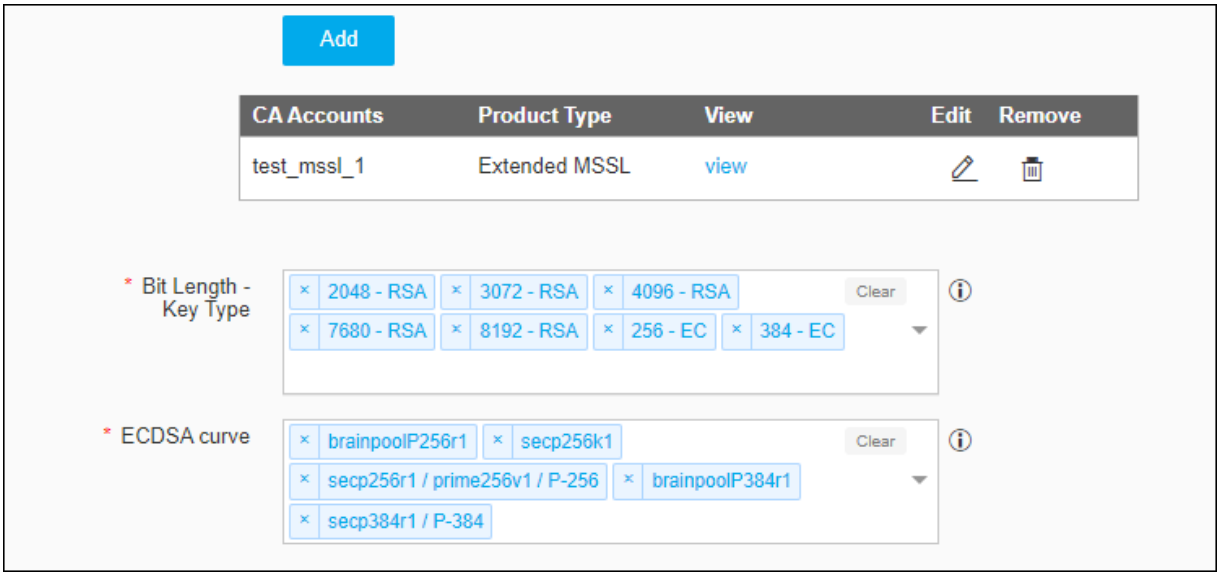
Field description for CA details

Fields	Description
***CA Accounts**	The GlobalSign MSSL CA accounts configured on the CA settings screen are listed. Select a CA account from the list to create the policy.
* **Product Type**	All Managed SSL Product Types require that the Organization's information and at least one Domain be registered in the Managed SSL account prior to ordering.
***Signature Algorithm**	Select the signature algorithm from the dropdown list list.
* **MSSL Profile Allowed Domain Name**	Select the **MSSL Profile Allowed Domain Name** from the dropdown list list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.



   You can use **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign MSSL** to indicate that the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for GoDaddy CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GoDaddy**.
   The **CA Details** section is updated to display fields relevant to GoDaddy.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Account**	The GoDaddy CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	The **Certificate Types** corresponding to the selected CA account are listed. Select one (or) more **Certificate Type** from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
7. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
9. Enter/Select the certificate parameters.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GoDaddy** to indicate that the details are successfully stored.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Google CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Google**.
   The **CA Details** section is updated to display fields relevant to Google.
5. Enter/Select the CA details.

Field description for CA details

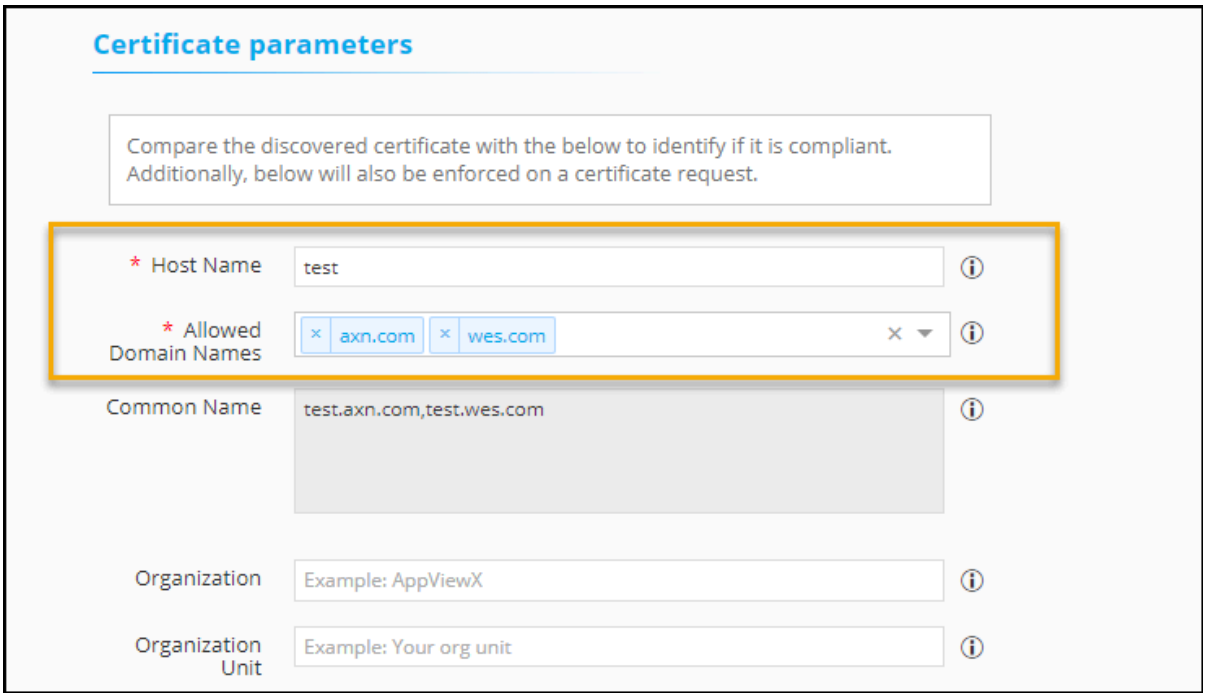
Fields	Description
***CA Accounts**	The Google CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Issuer Location**	The issuer locations corresponding to the selected CA account are listed. Select an issuer location from the list to create the policy.
***Issuer Name**	The issuer names corresponding to the selected CA account are listed. Select an issuer name from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

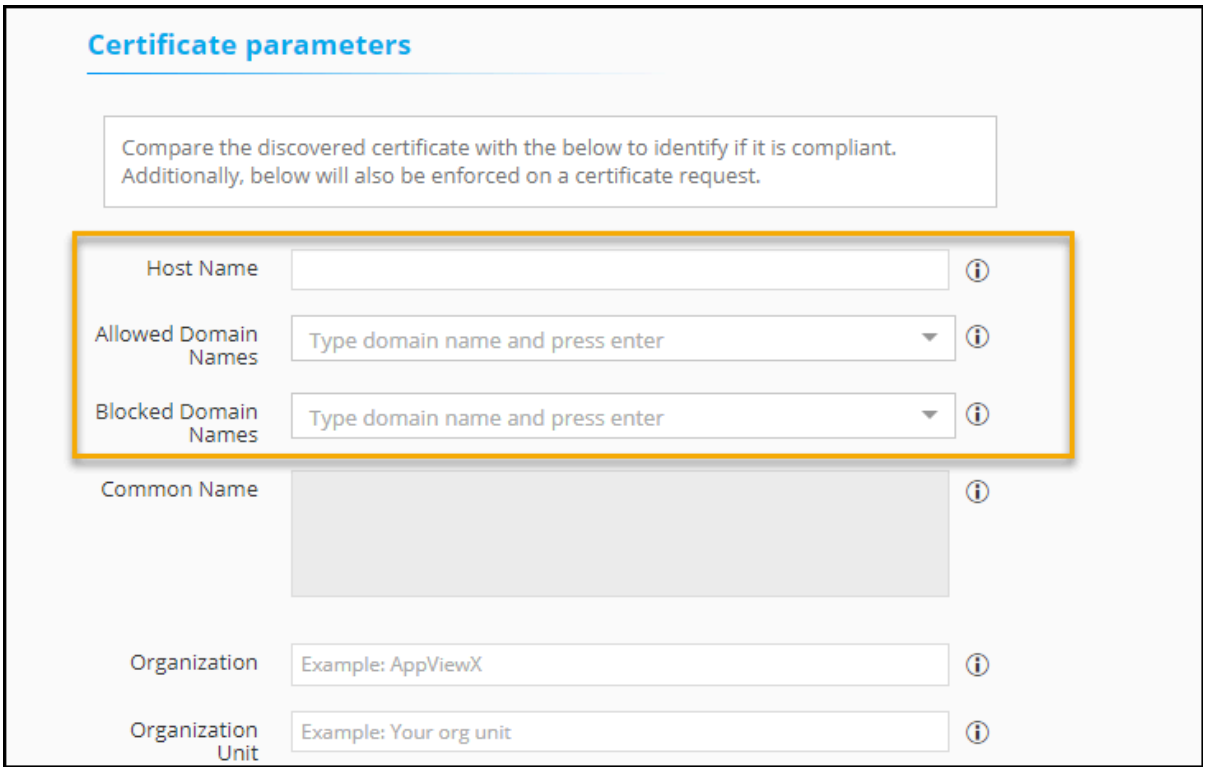
Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length-key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

6. Enter/Select the certificate parameters.
   For **Policy Enforcement Type** = **Strict**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



For **Policy Enforcement Type** = **Suggestive**



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for certificate Parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Hostname	This text field is displayed if the **Policy Enforcement Type = Strict** or **Suggestive**. Enter the unique name or label for the host. The field is **mandatory** only when the **Policy Enforcement Type = Strict**. **Note:** The hostname should not start or end with a dot.
Allowed Domain Name	This text field is displayed if the **Policy Enforcement Type = Strict** or **Suggestive**. The field is **mandatory** only when the **Policy Enforcement Type = Strict**. Enter the valid domain name (two parts separated by a dot, such as example.com) .
Blocked Domain Name	This text field is displayed only if the **Policy Enforcement Type = Suggestive** Enter the domain names (two parts separated by a dot, such as example.com) that need to be blocked .
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

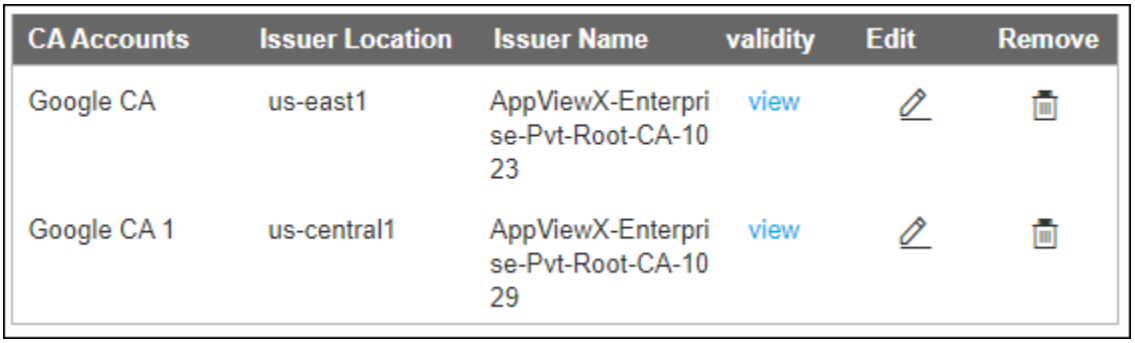
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	You can provide the organization's name. The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify if they are complaints. The organization is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	You can provide an organization unit. The discovered certificate's **Subject Organization Unit** will be compared against the organization unit provided in the policy to identify if they are Complaint. Organization Unit is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	You can provide a locality. The discovered certificate's **Locality** will be compared against the locality provided in the policy to identify if they are complaints. The locality is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	You can provide state. The discovered certificate's **State** will be compared against the state provided in the policy to identify if they are complaints. The state is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	You can provide a country code. The discovered certificate's **Country code** will be compared against the country code provided in the policy to identify if they are complaints.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Country code is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	You can provide an organization unit mail address. The discovered certificate's **mail address** will be compared against the email address provided in the policy to identify if they are Complaint. Mail address is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	You can provide the subject alternative name (SAN) It helps enforce additional domains for which a certificate can be requested. Subject Alternative Name is enforced while performing certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain domain.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.), At (@).
**: Mandatory fields*	

You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.



CA Accounts	Issuer Location	Issuer Name	validity	Edit	Remove
Google CA	us-east1	AppViewX-Enterprise-Pvt-Root-CA-1023	view		
Google CA 1	us-central1	AppViewX-Enterprise-Pvt-Root-CA-1029	view		

7. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **Google** to indicate the details are successfully stored.
8. From the **Group selection**, select one or more groups to map to the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

   Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for HashiCorp Vault CA

Before You Begin

- Certificate Group(s) must be available to map the Policy to them.
- CA accounts (settings) must be available to which the policy is going to be created.
- Key Algorithm, Encryption Type must be available under the CA accounts.
- AppViewX permission required (Accounts > Roles - Click here to check Accounts management).

To configure a Hashicorp Vault CA policy:

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed with a list of policies and their associated groups.

   Note: A **Default** policy will always be present in the list. Most of the roles are mapped to this policy. This policy can be used for any of the configured CAs.

2. To create a custom policy, click **+Create** from the top-right corner of the **CA Policy** page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **HashicorpVault**.
   The **CA Details** section is updated to display fields relevant to HashicorpVault.
5. Enter/Select the CA details.

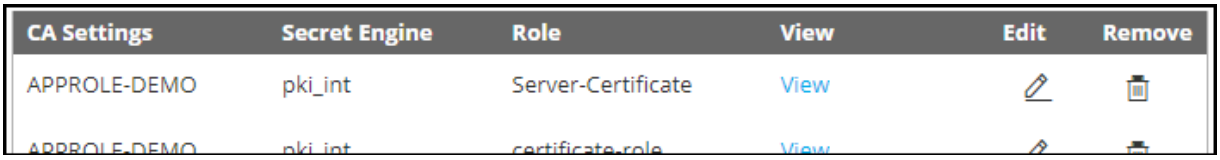
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for CA Details

Fields	Description
***CA Accounts**	Select a CA account from the list to create the policy.
***Secret Engine**	The single-select dropdown contains all the secret engines associated with the account. In a secret engine, a role describes an identity with a set of permissions, groups, or policies you want to attach to a user of the secret engine. User identity is often mapped to a specific role. Hence, a single secret engine needs to be selected to populate role (below) specific to it.
***Role**	The dropdown list contains all the roles mapped to the secret engine.
**: Mandatory fields*	

6. Click **Add**.

   The CA details are saved to the table and the confirmation message is displayed.



   Multiple values can be configured based on the available CA settings and secret engines with different bit length - key type and hash function. The supported values include:

   - **Key Type**: RSA, EC
   - **Bit Length:**
     - *RSA key type*: 2048 (default), 3072, or 4096
     - *EC key type*: 224, 256 (default), 384, or 521
   - **Hash Function**: SHA-256, SHA-384, SHA-512

   The CA Details table has options to **View**, **Edit**, and **Delete**.

   a. To view the CA details, click the **View** link in the **View** column. The CA account details are displayed in a pop-up window with the **Bit Length - Key Type** and **Hash Function.**
   b. To update the CA details, click the edit icon in the **Edit** column.
   c. To delete the CA details, click the delete icon.

7. Enter/Select the certificate parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

8. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against the **Hashicorp Vault** option to indicate that the details are successfully saved.
9. In the **Group Selection**, select one or more groups to map to the policy. Refer to the **Certificate Group** section to add/update groups.
10. Under the **Compliance Check** section, enable the **Perform Compliance Check** option to perform an immediate compliance check.
11. Click **Create Policy** button.
    The policy is created and a confirmation message is displayed.

Configuring Policy for HydrantID CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **HydrantID**.
   The **CA Details** section is updated to display fields relevant to HydrantID.
5. Enter/Select the CA details.

Field Description for CA Details

Fields	Description
***CA Accounts**	The HydrantID CA accounts configured in the CA settings screen are listed here. Select a CA account from the list to create the policy.
***HydrantID Policy**	Policies associated with the account will be displayed here. Select a policy from the dropdown (single select).
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against the **HydrantID** CA option to indicate that the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for IDnomic CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed with a list of policies and their associated groups.

> **Note:** A **Default** policy will always be present in the list. Most of the roles are mapped to this policy. This policy can be used for any of the configured CAs.

2. To create a custom policy, click **+Create** from the top-right corner of the **CA Policy** page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **IDnomic**.
   The **CA Details** section is updated to display fields relevant to IDnomic.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The IDnomic CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Management Profile**OR ***Certificate Workflows**	If the selected CA Account is configured with a certificate profile then the field label is Certificate Management Profile and displays only certificate profiles. If configured with a registration authority (RA) the field label is Certificate Workflows and displays the certificate workflows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The Certificate Types corresponding to the selected CA account are listed. Select one (or) more Certificate Type from the list to create the policy.
***Validity**	Enter the validity period for the certificate. The available options are: • **Days** - You may enter more than one validity period in days, to choose one in certificate enrollment. • **Month** - You can enter more than one validity period in Months, to choose one in certificate enrollment. • **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment.
***Bit Length - Key Type**	All the Key Types are listed with corresponding Bit Length. You can select one (or) more than one Bit Length - Key Type(s) from the dropdown list. The discovered certificate's Key Type and Bit length will be compared against the selected Bit Length - Key Type(s) to identify if they are compliant with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	Supported Hash Function(s) are listed here. You can select one (or) more Hash Function(s) from the dropdown list. The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are compliant with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed. You may use the **Edit** (pencil) option in the table to modify the configuration and the **Remove** (bin) option to delete the configuration.
7. Enter/Select the certificate parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Restrict users of the associated group policy from requesting Wildcard Certificates. Choosing this option will not allow Common Name or DNS starting with *.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.  **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

8. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against the **IDnomic** option to indicate that the details are successfully saved.
9. In the **Group Selection**, select one or more groups to map to the policy. Refer to the **Certificate Group** section to add/update groups.
10. Under the **Compliance Check** section, enable the **Perform Compliance Check** option to perform an immediate compliance check.
11. Click **Create Policy** button.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Let's Encrypt CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **LetsEncrypt**.
   The **CA Details** section is updated to display fields relevant to LetsEncrypt.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Let's Encrypt CA accounts configured in CA settings are listed here. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/ years, and one can then be chosen from the entered values at the time of certificate enrollment.

Note: The asterisk (*) symbol indicates a mandatory field.

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

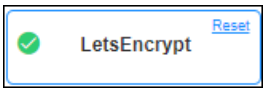
Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **LetsEncrypt** to indicate that the details are successfully stored.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Microsoft Enterprise CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Microsoft Enterprise**.
   The **CA Details** section is updated to display fields relevant to Microsoft Enterprise.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Microsoft Enterprise CA accounts configured in the CA settings are listed. Select a CA account from the list to create the policy.
***MS Template List**	The MS templates configured for the selected CA account are listed. Select MS template(s) from the list to associate with the policy.
**: Mandatory fields*	

6. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The CA details are saved to the table and the confirmation message is displayed.

You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Microsoft Enterprise** to indicate the details are successfully stored.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Microsoft Standalone CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Microsoft Standalone**.
   The **CA Details** section is updated to display fields relevant to Microsoft Standalone.
5. Enter/Select the CA details.

   Field description for CA details

Fields	Description
***CA Accounts**	The Microsoft Standalone CA accounts configured in the CA settings are listed. Select a CA account from the list to create the policy.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Microsoft Standalone** to indicate the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Nexus CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Nexus**.
   The **CA Details** section is updated to display fields relevant to Nexus.
5. Enter/Select the CA details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for CA details

Fields	Description
***CA Accounts**	The Nexus CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Once the CA account and the validity fields are populated, a new section called **Vendor Specific Details** is enabled. Select the **Procedure** field from the dropdown list list and click **Add** to save the CA details to the table. You can also use the **Remove** option to delete the configuration.
   Select the details as follows:
   a. **Case 1 -** Select **Server** check box, the procedures listed in the **Procedures** dropdown will be - Mapped to servers and default procedures.
   b. **Case 2 -** Select **Client** check box, the procedures listed in the **Procedures** dropdown will be - mapped to client and default procedures.
   c. **Case 3 -** Select **Server** and **Client** check box, the procedures listed in the **Procedures** dropdown will be - mapped to server, client, and default procedures.

   Note: The procedures displayed in the dropdown should have the **cert type** appended in the value. For example: - *Procedure name_Server/client/default/Code-Signing*.

7. Click **Add**. The CA details are saved to the table and the confirmation message displays.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

9. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
11. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name.

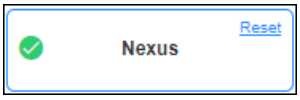
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Nexus** to indicate that the details are successfully stored.



13. From the **Group selection**, select one or more groups to map to the policy.
14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

15. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for OpenTrust CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **OpenTrust**.
   The **CA Details** section is updated to display fields relevant to OpenTrust.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Account**	The OpenTrust CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Management Profile**	Select the certificate management profile from the dropdown list.
***Zone**	Select the zone from the dropdown list.
**: Mandatory fields*	

6. Enter/Select the **Profile Parameters**.

Field Description for profile parameters

Fields	Description
***Common Name**	Enter a common name for the policy.
Organizational Unit	Enter the organizational unit.
Organization	Enter the name of the organization.
**: Mandatory fields*	

7. Click **Add** button.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

9. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
11. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark displays in the **Certificate Authority** pane against **OpenTrust** to indicate that the details are successfully stored.
13. From the **Group selection**, select one or more groups to map to the policy.
14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

15. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Policy for Sectigo CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Comodo Certificate Manager**.
   The **CA Details** section is updated to display fields relevant to Comodo Certificate Manager.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Sectigo CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

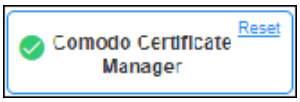
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

11. Click **Save CA Details** button to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Comodo Certificate Manager** to indicate that the details are successfully stored.



12. From the **Group selection**, select one or more groups to map to the policy.
13. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

14. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Symantec CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Symantec**.
   The **CA Details** section is updated to display fields relevant to Symantec.
5. Enter/Select the CA details.

Field description for CA details

Fields	Description
***CA Account**	The Symantec CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. In the **Vendor Specific Details section**, select the server type from the dropdown list.
7. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
11. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Symantec** to indicate that the details are successfully stored.



13. From the **Group selection**, select one or more groups to map to the policy.
14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

15. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Policy for Trustwave CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Trustwave**.
   The **CA Details** section is updated to display fields relevant to Trustwave.
5. Enter/Select the CA details.

Field description for CA Details

Fields	Description
***CA Account**	The Trustwave CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for complaince with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Trustwave** to indicate that the details are successfully stored.



11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

13. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Certificate Group

Before you Begin

Know the following before starting the **Certificate Groups** configuration:

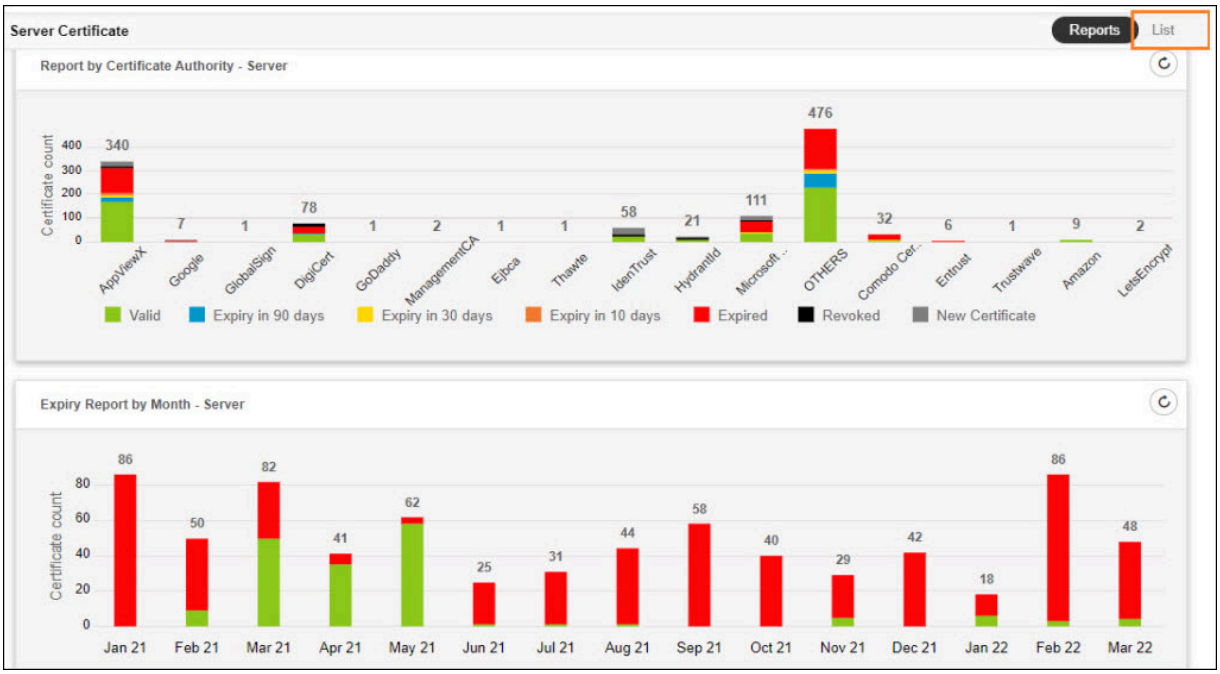
- **Certificate Groups** are used to categorize the certificates according to various **business units.**
- In some organizations, **Certificate Groups** are also used to assign access permissions. Only privileged users (inherits from Resource > User Group) can view the respective **Certificate Groups**.
- Users should be assigned to a **Role** (inherited from Role > User Group) that has access to perform the below actions,
  - View a group
  - Assign a group
  - Unassign a group
- With these actions, users can assign a group during **Certificate Discovery** to avoid movement of certificates post-discovery.
- Along with the view, assign, and unassign options, administrators should be assigned to a **Role** that has access for additional actions,
  - Create/ modify a group
  - Delete a group
  - Edit Default group

- Assigning a Certificate to a Group
- Unassigning a Certificate from a Group
- Creating a Group
- Deleting a Group
- Modifying a Group

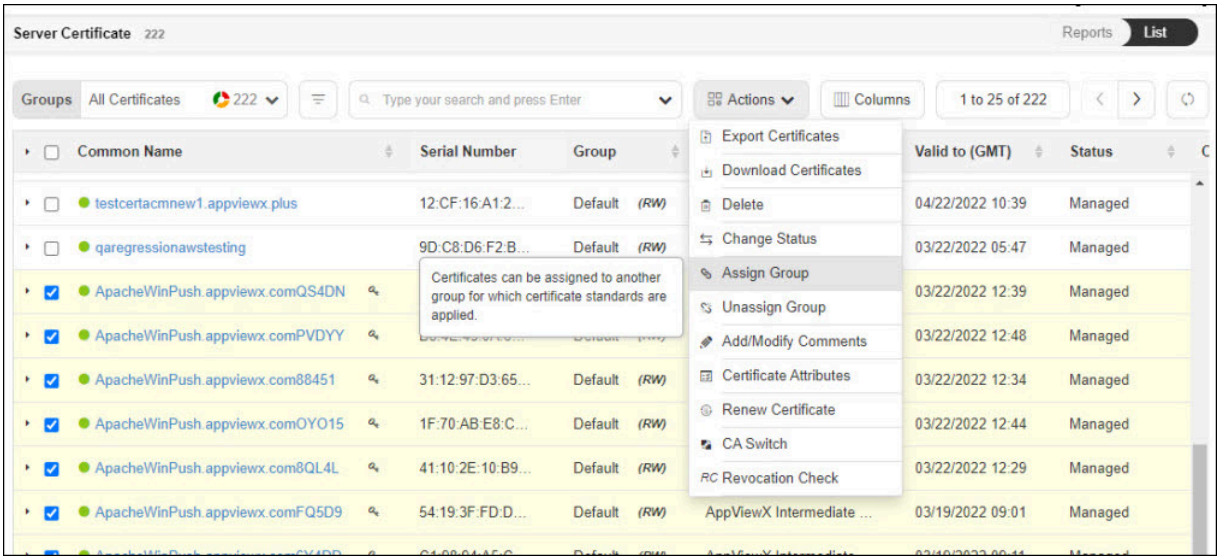
Assigning a Certificate to a Group

1. Go to (**Menu**) > **CERT+**.
   The **Server Certificate** Inventory is displayed.
2. Click **List** button on upper right of the server certificate inventory screen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

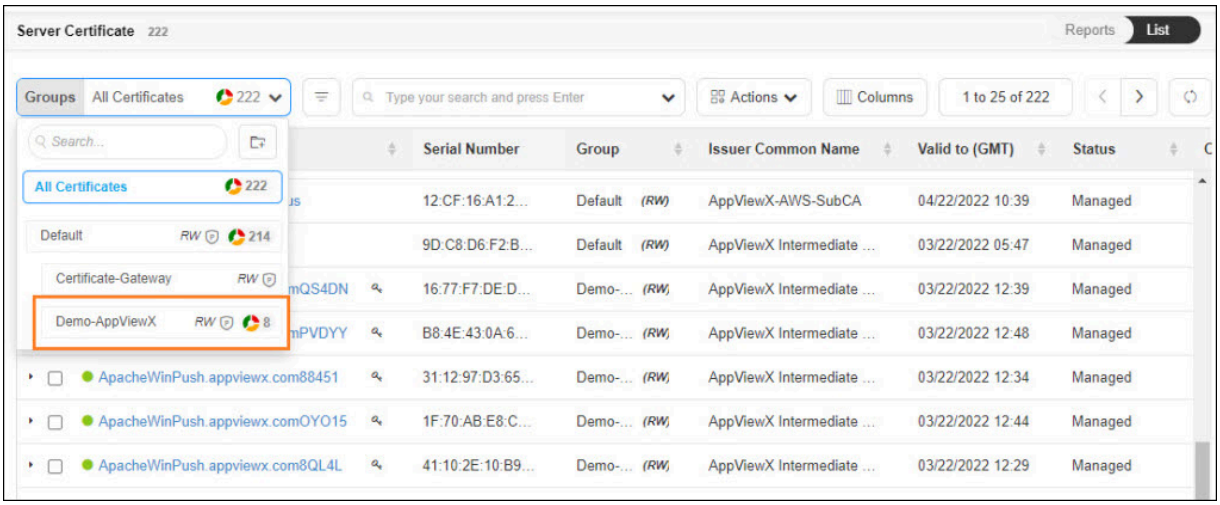


3. Select the check box against the certificate(s) you want to assign to a group.
4. Click the **Actions** dropdown list and select the **Assign Group** option from the dropdown list.

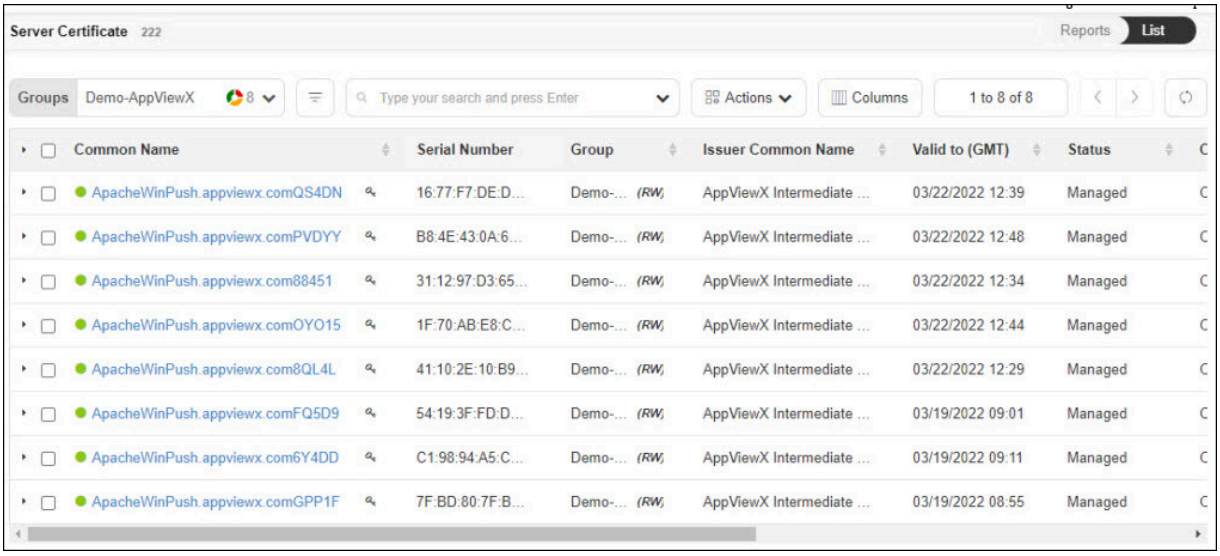


5. The **Assign to Group** pop-up is displayed. Select the **Group** from the list.
6. Click the **Assign** button to move the certificate(s) to the selected **Group.**
7. Click the **Groups** dropdown list and select your **Group** from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



8. You can view the certificate(s) assigned to the **Group**. The table provides certificate(s) details.

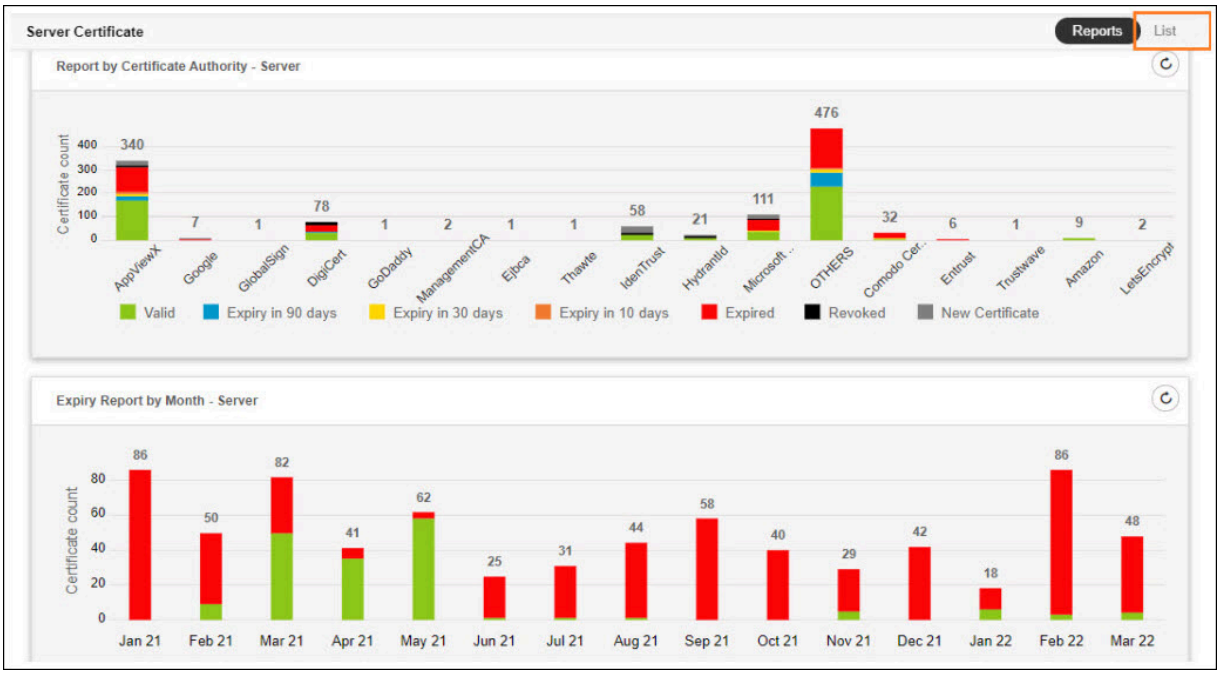


Unassigning a Certificate from a Group

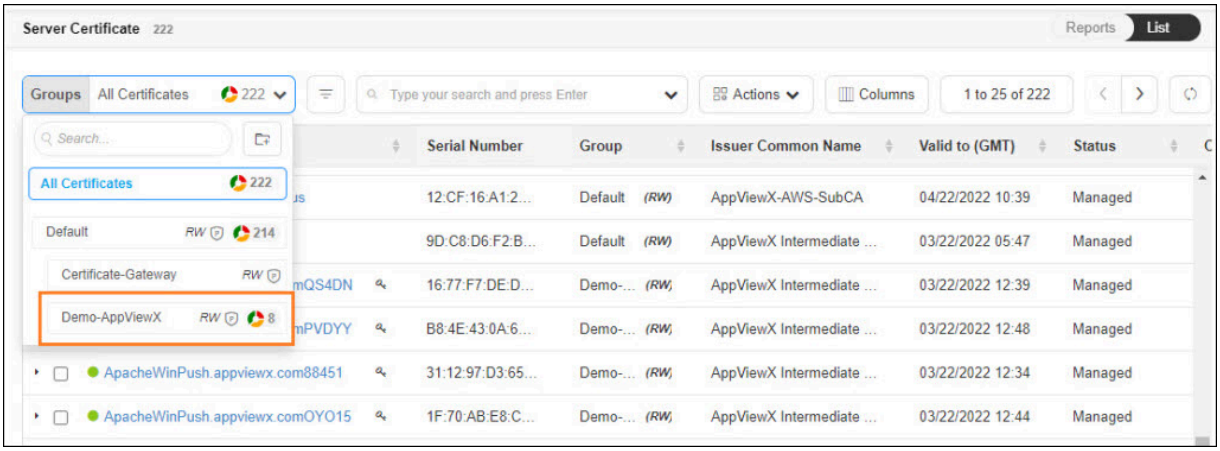
1. Go to (**Menu**) > **CERT+**.

   The **Server Certificate** Inventory is displayed.
2. Click the **List** button on the upper right of the server certificate inventory screen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

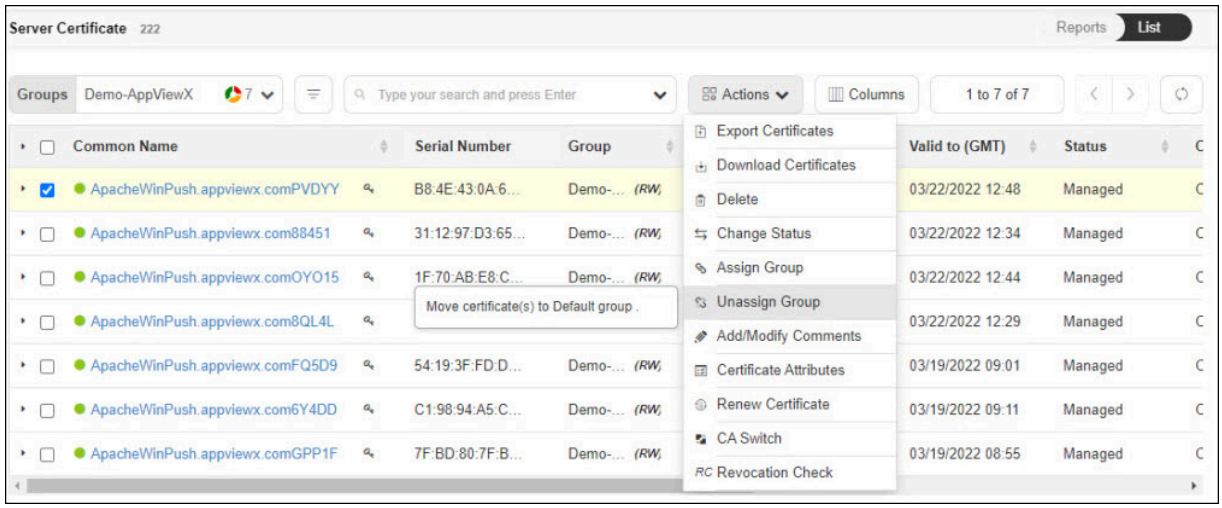


3. Click the **Groups** dropdown list and select a **Group** from the dropdown list.



4. Select the check box against the certificate you want to unassign from the group.
5. Click the **Actions** dropdown list and select the **Unassign Group** option from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



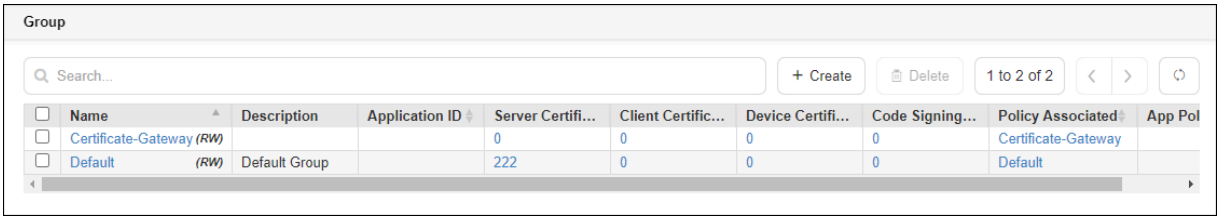
6. The certificate is unassigned from your **Group** and automatically assigned to the **Default Group**.

A certificate should always assign to a **Group** to compliance with the **Policy**. Certificate unassigned from a group will automatically assign to **Default Group** and compliance against **Default Policy**.

Creating a Group

Assign the user to a user group that (inherits from resource and role) have access to certificate group.

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. Click the **+ Create** button in the command bar to create a new group.



The following table provides the field description under the **Group Details** section:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Group Details - Field Description Table

Field	Description
***Select Group Hierarchy**	From the dropdown list, from the following options, select the parent group to which the new group should be associated: • **Default** • **Certificate Gateway** • **Private CA Certificates** • **Public CA Certificates**
Group Name	Enter a unique name for the new group. **Note:** The name should not start with special characters and spaces. No special characters are allowed except('.', '-', '_') and name cannot end with space.
Application ID	Provide organization ID (if any) to associate with the new group
Description	Provide the purpose of the new group
**: Mandatory fields*	

3. Group Name is mandatory in the **Group Details** section. Provide the **Group Name** to create a new group.
   The following table provides the field description under the **Other Details** section:

Name	Type	Mandatory	Description	Validation
Contact Name	Text	No	Provide contact person to whom changes should be intimated	NA
Line of Business Name	Text	No	Provide the name of the business unit	NA
Email	Text	No	Provide contact mail address	NA
Environment Name	Text	No	Provide environment name	NA
Phone Number	Text	No	Provide a phone number for contact	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Type	Mandatory	Description	Validation
Inventory Number	Text	No	Provide inventory number	NA
Cost Center/ Hierarchy	Text	No	Provide Cost Center code/ label	NA
Push Certificate Automatically	Check box	No	By enabling the check box, the renewed/ reissued certificates in this group are automatically associated with their device	NA
Renew Automatically	Toggle button	No	Turn **On** to automatically renew the certificate belongs to this group.	NA
Associated Policy	Dropdown (disabled)	Yes	Displays the policy associated with this group.	NA

The fields in the **Other Details** section are used based on the organization's needs.

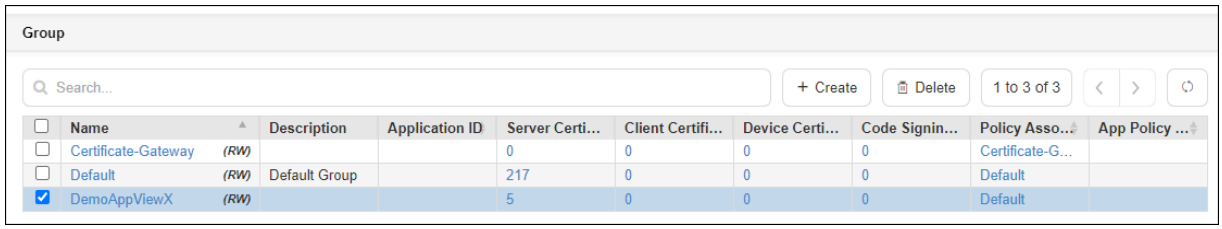
4. Click **Create** button to create the group.
   Users can view the group only if it is associated with the **Resource** of their **User Group**. To associate the **Group** to a **Resource** click the **Update Group and Configure the Resources for User Access** button instead of **Create** button. This will create the group and navigates to **Resource**.
   The newly created **Group** is added to the Group inventory. Click the **Name** (Group name) to view the group details.

   Post certificate discovery, you can view the count of certificates (Server, Client, Device, and Code Signing) associated with this group.
5. Click the count in the Server Certificates column to view the certificates.

Deleting a Group

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. In the group inventory, select the check box against the group you want to delete.
3. Click the (**Delete**) icon in the command bar to delete the Group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



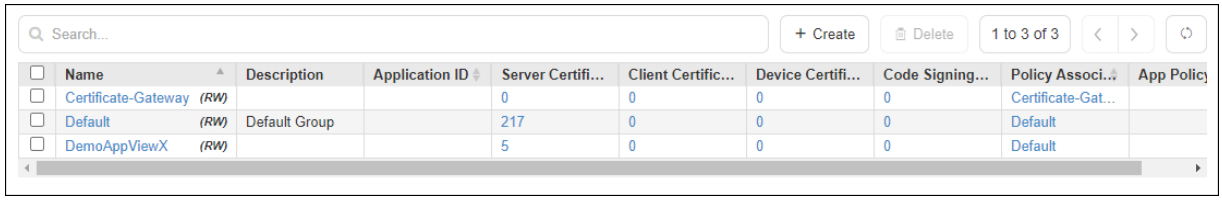
A confirmation pop-up is displayed. Click the **Yes** button to proceed.

The group is deleted and a confirmation message displays.

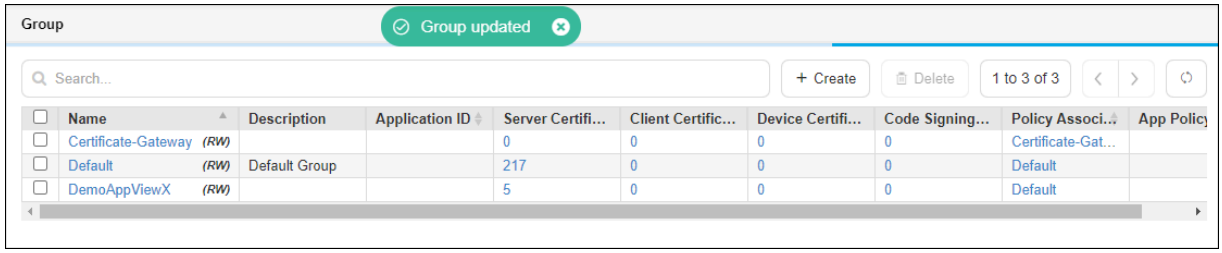
Modifying a Group

Assign the user to a user group that (inherits from resource and role) have access to the certificate group

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. Click the **Name** (Group name) to view the group details.



3. Modify required fields in the group and click the **Update** button. Field descriptions are available in Create a Group section.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Certificates

• Configuring Certificate Settings
• Configuring Certificate Attributes
• Configuring Certificate Profiles

Configuring Certificate Settings

• Configuring Password Vault
• Password Protected Certificates

Configuring Password Vault

The password vault option is used to store all certificate passwords of the selected ADC devices. All the password-protected certificates that are discovered, will be decrypted and pushed to the discovery grid in the AppViewX Inventory. This happens only if passwords are matched with passwords that are stored in the vault.

Before you Begin

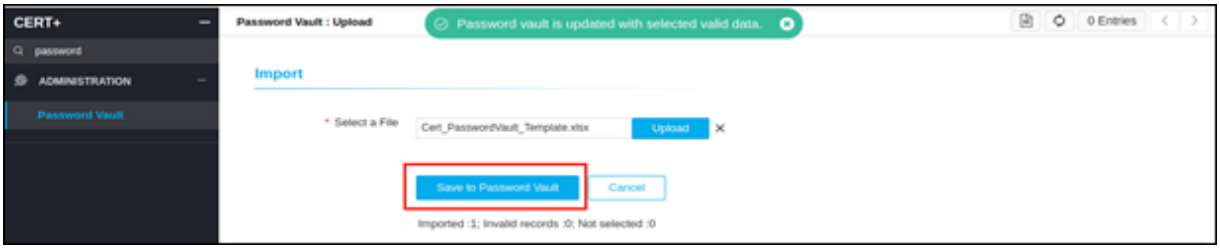
The prerequisites for configuring the Password Vault in AppViewX as are follows:

• A valid certificate password for password-protected certificates to decrypt.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** and click **Password Vault**.
2. On the screen that is displayed, enter an **Identity Name** of the password you want to add in the vault.
3. From the **Device Name** dropdown list, select the ADC device whose password-protected certificate details you want to store.
4. In the **File Name** field, enter a certificate file name to help users identify it.
5. In the **Password** field, enter the password that is associated with the certificate.
6. Click **Save**.
7. To import a file (in XLS or CSV format) with a list of all certificate passwords, on the top-right corner, click **Import**. This option is used to store the certificate passwords directly in the vault instead of adding them manually.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





8. Click **Export Password** on the top-right to export all stored certificate passwords from the vault as a zip file to your computer.
9. To modify the existing details, Click **Edit.**
10. To update the password, click **Update.**
11. To delete the password details, click **Delete.**

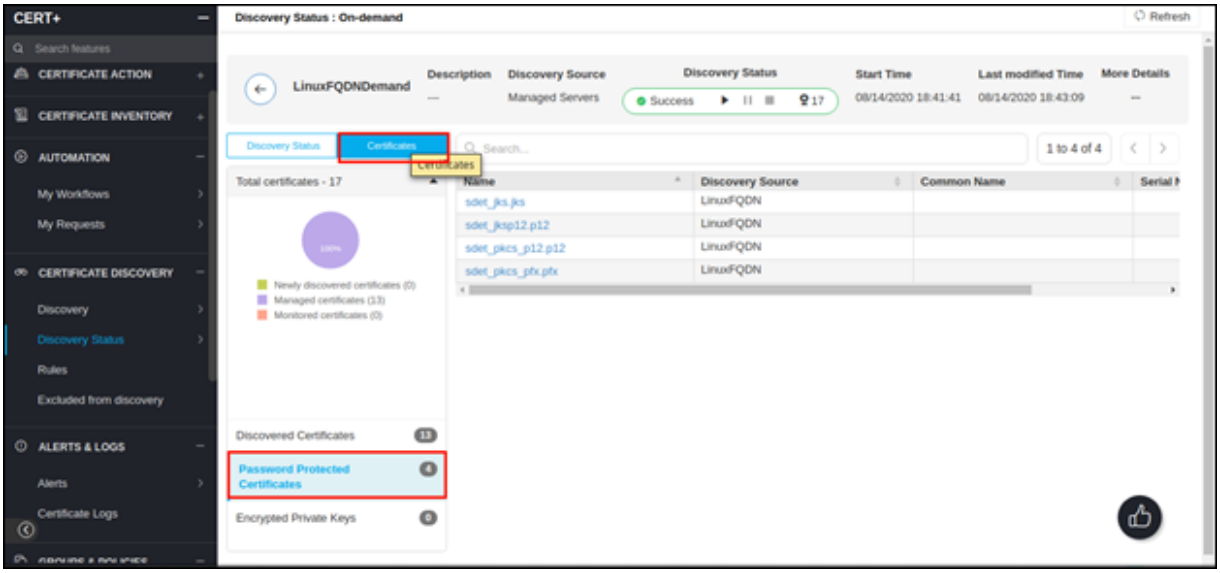
Password Protected Certificates

Password mismatch or password unavailable in the vault for the password-protected certificates that are discovered will be under the password-protected certificates section.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **OnDemand**.
2. Click on the **discovery name** under discovery inventory.
3. Click **Certificates** under the tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. To view all password-protected certificates, click **Password Protected Certificates.**



Configuring Certificate Attributes

- Configuring Attribute Information
- Deleting Certificate Attributes
- Updating Certificate Attributes
- Certificate Attributes in Certificate Enrollment
- Certificate Attributes in Certificate Inventory

Configuring Attribute Information

Certificate Attributes are a CERT+ way of creating additional placeholder fields which can be used to track a certificate. An administrator can create one or more fields that a requester enrolling a certificate can fill and use for future tracking.

Before you Begin

The prerequisites for configuration the certificate attributes are as follows:

- Certificate attributes are CA or organization-specific attributes, apart from the CSR parameters.
- Once configured, these attributes will be shown to collect values during certificate enrollment.
- Business units specific parameters can be stored for quick filtering and auditing.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
2. Click **Add New**.
3. Configure the **Attribute Information** details as mentioned below.

Attribute Information Table

Fields	Description
***Key ID**	Unique key for the attribute. Key ID must not start with special characters. No special characters except -, _ are allowed.
***Label Name**	Attribute name which will be shown during certificate enrollment. E.g. Email Contact, Owner. Label name should not start with special characters. No special characters except -, _ and spaces are allowed.
Mandatory	Enable if this field needs to be mandatory.
Default Value	Set default value to the attribute.

Note: These attributes support only text fields and are applicable for all CAs.

4. Click **Save**on the pop-up.

Deleting Certificate Attributes

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
2. Under **Actions**, click **Delete**.

Updating Certificate Attributes

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** and click **Certificate Attributes**.
2. Select the **Edit** icon under **Actions**.
3. Update the existing values.
4. Click **Update**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Attributes in Certificate Enrollment

After configuring certificate attributes, these attributes will be displayed in the certificate enrollment page. We can provide values for these attributes. If the default values have been provided for these attributes in configuration, those values will be shown.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate**.
2. Select any one from **Server** or **Client** or **Code Signing**.

Certificate Attributes in Certificate Inventory

Provided attributes and their values will be shown in the certificate inventory along with the certificate information.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > select **Server** or **Client** or **Code Signing**.
2. Click the **Columns** icon.
3. Select certificate attributes to display in the certificate inventory.

• Configuring Auto-Removal of Expired Certificates

Configuring Auto-Removal of Expired Certificates

Before you Begin

- This feature, if enabled, will delete all the expired certificates after configured no. of days from their expiration date and will remove them from the certificate inventory.

• Configuring Expired Certificates

• Fetch Expired Certificates in the Inventory

• Configuring Renew/Regenerate History

Configuring Expired Certificates

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
   The **Expired Certificates** screen is displayed.
2. Enter the information required as per the table given below. Each of the fields used for configuration of expired certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Expired Certificates Page

Name	Description
***Do you want to delete the expired certificate after its expiry?**	Option to enable/disable auto removal of expired certificates after expiry.
***Number of days after expiry**	Specify no. of days, once enabled, expired certificates will be automatically deleted after configured no. of days from expiry. • Only numbers allowed • Enter expiry days (Expiry days can not be empty) • Expiry days cannot exceed three characters.
**: Mandatory fields*	

3. Click **Save**.
4. Click **Reset** to revert to the previously saved settings.

Fetch Expired Certificates in the Inventory

All the Expired certificates can be fetched in the certificate inventory by following the steps shown below.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > select **Server** or **Client** or **Code Signing**.
2. To get a list of all the certificates present in the selected inventory, click the **List** tab on the top-right corner of the page.
3. Click on the **Filter Summary** icon then select **Expired** to get a list of all the expired certificates present in the inventory.

Configuring Renew/Regenerate History

Before you Begin

- This feature, if enabled, will keep the history of old certificates before renewing/reissue/regenerate action in the inventory and they will be tracked in the holistic view as well.
- By default, the History of Certificates is enabled, this means that the parent certificate will be present in inventory after the renewal/regeneration and will be tracked in the holistic view as well.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Configuring History of Certificates
• Checking History of Renewed/Regenerated Certificates

Configuring History of Certificates

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **History of Certificates**.
   The History of Certificates page is displayed.
2. Enter the field information as per the table below.

Field Description for History of Certificates

Name	Description
***Do you want to maintain the history of the certificate after its renew/reissue/regeneration?**	Option to select if the user wants to maintain the history of the certificates after it's renewed/reissue/regeneration or not.
**: Mandatory fields*	

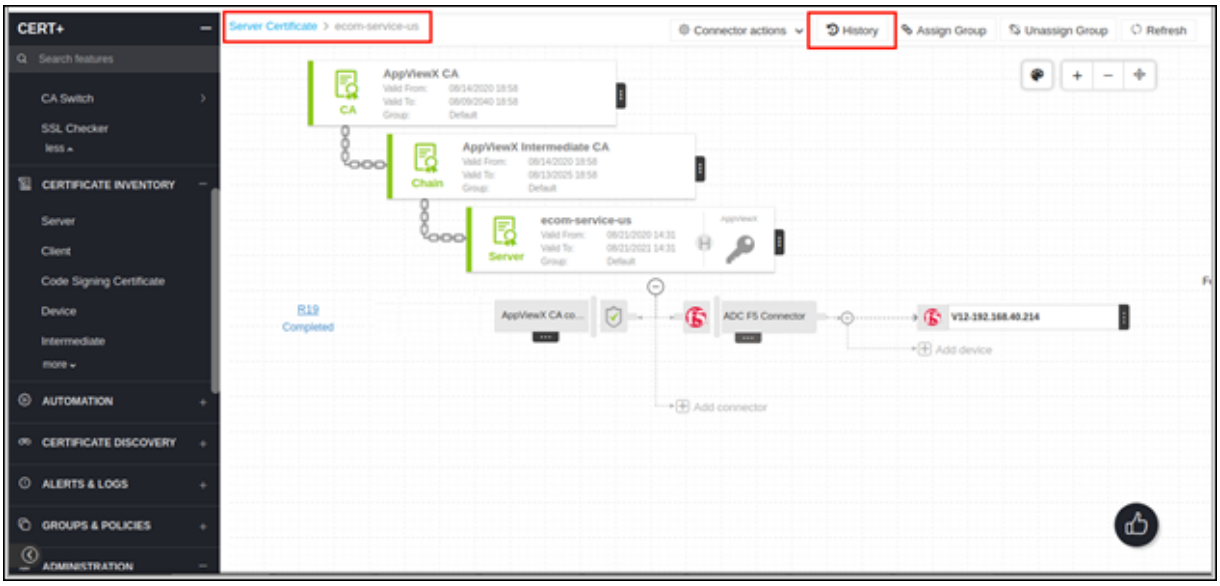
3. Click **Save**.
4. Click **Reset** to revert to the previously saved settings.

Checking History of Renewed/Regenerated Certificates

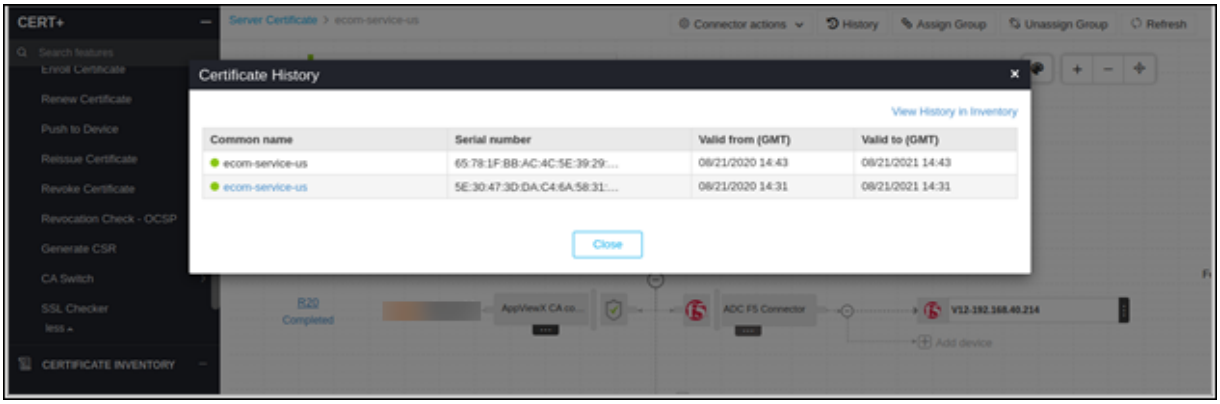
History of certificates, if enabled, can be checked on the Certificate Topology page by following these steps:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > select **Server** or **Client** or **Code Signing**.
2. Click on the **List** tab on the top-right corner to view the certificates list page.
3. On the certificate list view page, click on the Common Name of the certificate for which to check the history that has been successfully renewed/regenerated.
4. To check the History of certificate, click on the **History** icon on the certificate topology page. (If the certificate renewal/regeneration was successful, the History icon will be present).

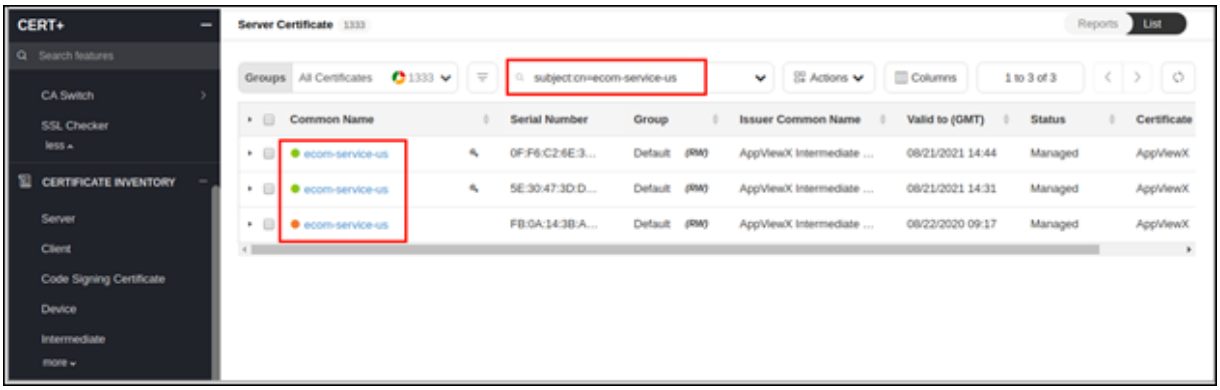
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Click on the History to view the history of the certificate in the pop-up window.



6. The respective query for this will be automatically framed and search results will be shown.



After successful renewal/regeneration, the new certificate is available in the Certificate Inventory. The parent certificate used for renewal/regeneration will be available in the inventory based on the below

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

configuration. If the History of Certificates is selected as Yes, parent certificates will be available along with renewed/regenerated certificates but if selected otherwise, the parent certificate from which the certificate was renewed/regenerated will be deleted from inventory and no history will be maintained for the child certificate. By default, the history will be maintained.

Configuring Certificate Profiles

AppViewX Cert+ offers administrators capability to define the type or purpose of a certificate through Certificate Profiles. An administrator can configure multiple Profiles defining the Key Usage and Extended Key Usage for a certificate enrolled through AppViewX. The Profiles defined are applicable on Certificates enrolled through AppViewX CA or Custom CA.

An Administrator can white label AppViewX CA through Custom CA.

Before you Begin

Following are the points needed to be known before starting to configure Certificate profile -

- Certificate profiles configure Key usage extensions that define the purpose of the public key contained in a certificate.
- Once configured, these profiles would be used to define Key Usage and Enhanced Key Usage while the signing a CSR through AppViewX CA and white labeled AppViewX CA or Custom CA.
- System comes prebuilt with three profiles corresponding to a standard Server Authentication, Client Authentication and CodeSigning Certificate.

- Configuring Certificate Profiles
- Updating a Certificate Profile
- Deleting a Certificate Profile

Configuring Certificate Profiles

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Click **+ Add** icon on the top right corner.
3. Configure the **General Information** details as follows:

General Information - Field Description Table

Field	Description
***Name**	Unique name to identify the profile.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Profile name should not start with special characters. Can contain only alphanumeric characters, no special characters except -, _, . are allowed.
***Purpose/Usage**	Certificate Type to which the Key Usage extensions are signed with. For example: Server or Client.
**: Mandatory fields*	

4. Configure the **Key Usages** as given below.

Key Usages - Field Description Table

Field	Description
***Critical**	Enable this field to sign the Key Usage extensions as **critical**.
***Key Usage(s)**	Key Usage extensions along with which the CSR is signed.
**: Mandatory fields*	

5. Configure the **Extended Key Usages** as given below.

Extended Key Usages - Field Description Table

Field	Description
***Critical**	Enable this field to sign the Extended Key Usage extensions as **critical**.
***Key Usage(s)**	Extended Key Usage extensions along with which the CSR is signed.
**: Mandatory fields*	

6. In the **Policy ID** section, enter the policy id in the field..
7. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Updating a Certificate Profile

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Under Administration, select **Certificate Profile**.
3. Click on the profile that needs to be edited.
4. Edit existing values.
5. Click **Update.**

Deleting a Certificate Profile

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Click  (**Delete**) against the Profile to be deleted.
3. Click **Yes** in the **Delete Confirmation** pop-up.

Managing Devices

See *CERT+ User Guide* for prerequisites to manage ADC, Servers, Firewall, Cloud devices into AppViewX Device inventory.

Managing a Device into AppViewX device inventory allows administrators or users of the platform to discover certificates currently in use on the devices. Also, an administrator or user can provision or push a certificate to the device through the platform.

- Configuring Servers
- Configuring Firewall
- Configuring Cloud
- Configuring WAFs

Configuring Servers

- Adding a Server
- Deleting Server
- Import Server
- Export Server
- Manage Server
- Unmanage Server

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Fetch Config for Server
- Add Credentials
- Device Setting

Adding a Server

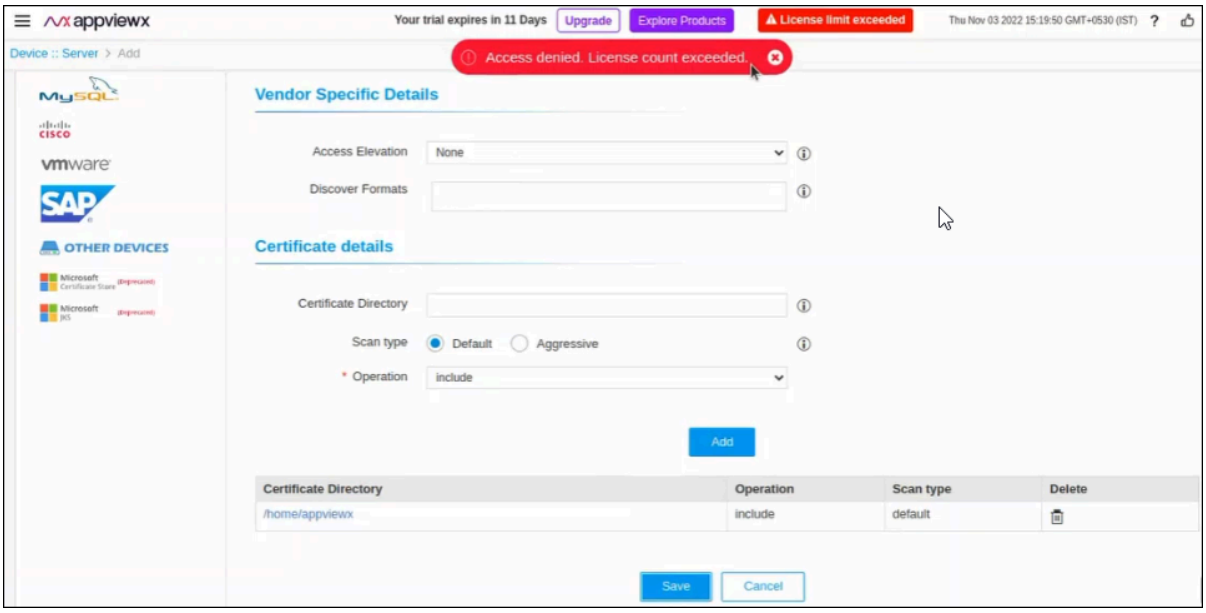
This section describes the process of onboarding IIS and non-IIS web servers into AppViewX.

- Akamai
- Apache Linux
- Apache Windows
- Arbor
- CISCO
- Dell
- HP-ILO
- IBM
- JBoss
- Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- Microsoft SQL
- MySQL
- NGINX
- Oracle
- Other Devices
- RabbitMQ
- SAP
- VMware

License Enforcement

AppViewX has enabled a feature to set a limit for the licensed certificates. If the number of certs exceeds this limit then the additional certs added to the inventory will be moved into the **Monitored** status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- A red indicator labeled "**License Limit Exceed**" is displayed on the title bar of the page, if the limit has exceeded.
- A pop-up message "**Access denied. License count exceeded.**" is displayed on the click of the **Save** button while adding a new server device.
- All the new on-boarded server certs (Server/ADC/Firewall/WAF Device config sync) into the inventory will be mapped to the**Monitored** state.

Akamai

The Akamai CPS (Certificate Provisioning System) provides full life cycle management of SSL/TLS certificates for Akamai Secure Delivery Network applications.

Before you begin

- Create authentication credentials. before using the API.
- To enable this API, choose the API service named Certificate Provisioning System, and set the access level to READ-WRITE.
- To allow new features to roll out flexibly, the CPS API supports a system of versioned objects that uses `Content-Type` and `Accept` headers. Refer Object versioning.

To onboard the Akamai CPS device,

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click the **Server** tab.
3. Click the  **(Add)** icon.
4. Select **Akamai** logo from the Vendors list.
   The **Akamai** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the server name, a unique name for the device addition.
***IP address/ FQDN**	Enter the valid IP address or FQDN for device communication and integration with the Akamai CPS.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Akamai server.
Proxy	Select the checkbox to enable the secure proxy service.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter details as mentioned below.

Credentials - Field Description Table

Fields	Description
***Client token**	Enter the client token as provided by the vendor.
***Client secret**	Enter the client secret as provided by the vendor.
***Access token**	Enter the access token as provided by the vendor.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***API Version**	Enter the value, example cps/v2. (The same value is provided as the placeholder.)
**: Mandatory fields*	

7. Click **Update**.
   The device is added successfully.

Apache Linux

Apache

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Linux** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Linux server.
***IP address/ FQDN**	Enter the IP address of the Apache Server or its fully qualified domain name (FQDN) that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. (The field label changes to ***Account Name** if **SSM** is the communication mode)
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/ dzdo.
Temp Directory	Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: It is used as an intermediate location to store the actual keystore and then perform actions on the certificates in the keystore. The keystore is then moved back to the original location after performing the actions.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Region	Enter the geographic region of the AWS instance. *Example*: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
Account number	Enter the 12-digit AWS account number.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: 012345678901

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the actual directory/path where certificates are stored in the Apache server. *Example*: /cert/files
Key location	Enter the actual directory/path where keys are stored in the Apache server. *Example*: /key/files
Intermediate location	Enter the temporary or intermediate directory/path where certificates and keys are stored in the Apache server. *Example*: /inter/files

9. Click **Add**.
   Once the server is added successfully, the certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
11. Click **Save**.

Tomcat

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Linux** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Tomcat** radio button.
***Server name**	Enter the name of the designated Apache Tomcat server.
***IP address**	Enter the IP address of the Apache Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.

   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
Temp Directory	Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files
*: Mandatory fields	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Region	Enter the geographic region of the AWS instance. *Example*: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Server path	Enter the directory/path where the application is installed. *Example*: /opt/tomcat/apache-tomcat-9.0.52

9. Click **Add**.
   Once the server is added successfully, the certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the location details from the list.
11. Click **Save**.

Apache Windows

Apache

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Windows** from the Vendors list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Apache server.
***Hostname**	Enter the hostname of the Apache Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: C:\Tomcat8\Apache-Tomcat-8.5.35
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Same as above
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

8. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM.**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

9. Click **Save**.
   The device is onboarded successfully.

Tomcat

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Windows** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Tomcat** radio button.
***Server name**	Enter the name of the designated Apache Tomcat server.
***IP address**	Enter the IP address of the Apache Server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. In the **Certificate details** section, select/enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
***Server path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
**: Mandatory fields*	

9. Click **Add.**
   Once the server is added successfully, the path will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the server path from the list.
11. Click **Save**.
    The device is onboarded successfully.

Arbor

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Arbor** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Arbor server to be onboarded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Arbor server.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Arbor server device.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.

Vendor Specific Details - Field Description Table

Fields	Description
***Base URL**	Enter the base URL where the Arbor service is hosted.
***HSM Username**	Enter the username used to access the HSM device where the SSL/TLS certificates are stored.
***API Token**	Enter the API token to authorize the communication between AppViewX and the Arbor.
***HSM Password**	Enter the secure password used to access the HSM device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

8. Click **Save**.
   The Arbor device is onboarded successfully.

CISCO

The CISCO device can be on-boarded by four server types,

- UCS
- CUCM
- ISE
- IOS

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **CISCO** logo from the Vendors list.
   The **CISCO** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

   a. Select the **Server Type = UCS**, and enter the details of the fields mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type from the dropdown (UCS).
***Server name**	Enter the server name, a unique name for the device addition.
***IP address/ FQDN**	Enter the valid IP address or FQDN for device communication and integration with CISCO.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Cisco server.
***SSH Port**	Enter the SSH port number. Default value is 22.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

b. Select the **Server Type = CUCM**. All the fields mentioned above (in step a) will be displayed along with the additional fields as below:

Server Details - Field Description Table

Fields	Description
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

c. Select the **Server Type = ISE**. All the fields mentioned above (in step a) will be displayed along with the additional fields as below:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
ERS API Port	The Cisco Identity Services Engine (ISE) API uses ERS and OpenAPI port for communication. These port requirements can be modified during the installation or configuration of the ISE, depending on the network and security requirements. The default value for ERS API Port is **9060**. The default value for Open API Port is **443**.
Open API Port	
Proxy Required	The checkbox is not selected (false) by default. To enable communication through proxy servers select the checkbox (true).
Cert sync	Select the required cert sync. The possible options are • Managed (*default selection*) • Monitored • Ignored

d. Select the **Server Type = IOS**. All the displayed fields are as mentioned in **step b**.

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • Manual entry • Credential List - AppViewX • Credential List - BeyondTrust • Credential List - Thycotic **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the assigned username. (This field is displayed for Manual entry only)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password**	Enter the secure password. (This field is displayed for Manual entry only)
***Privilege Password**	Enter the privilege password for using the privilege mode.
**: Mandatory fields*	

7. Click **Save**.

Note: The CISCO device can be configured through the Import option, by downloading the .csv or .xlxs templates, Additional columns (ERS API Port and Open API Port) have been added for CISCO ISE. These can be left blank; the default values, 9060 and 443 respectively will be considered.

Dell

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Dell** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type has default value **iDRAC** (Integrated Dell Remote Access Controller).
***Server name**	Enter the name of the designated Dell iDRAC server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) of the device being onboarded. It is used for device communication and integration with the server.
***HTTPS Port**	Enter the valid HTTPs port number that is required to remotely access iDRAC through firewall.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the SAP server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select value *sudo* to execute with root privileges using sudo access or choose *none*. The RACADM utility requires sudo privilege to access iDRAC. **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
**: Mandatory fields*	

8. Click **Save**.
   The Dell iDRAC device is onboarded successfully.

HP-ILO

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **HP** logo from the Vendors list.
5. In the **Server details** section, select/enter the details as follows

Server Details - Field Description Table

Fields	Description
***Server Type**	The value is set to ILO.
***Server name**	Enter the name of the designated HP server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
HTTPS Port	Enter the HTTPS port number used for secure communication.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the HP server.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Multiple devices can be configured for the same vendor.

The device is onboarded successfully.

IBM

Websphere (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Websphere (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
***IP address**	Enter the IP address of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. In the **Service account credentials** section, select/enter the details as indicated below. These credentials are used by the WebSphere application server to perform various tasks, such as accessing files, interacting with the operating system, and communicating with other applications and services.

Service account credentials - Field description table

Fields	Description
***Username**	Enter the designated username for authentication.
***Password**	Enter the secure password.
**: Mandatory fields*	

8. In the **WSadmin credentials** section, select/enter the details as indicated below. These credentials are used to authenticate the wsadmin tool with the WebSphere Application Server so that it can execute administrative commands and access the necessary resources.

WSadmin credentials - Field description table

Fields	Description
WSadmin User name	Enter the designated WSadmin username for authentication.
WSadmin Password	Enter the secure password for WSadmin.
WSadmin directory path	Enter the file location / directory path where the WSadmin tool is stored.

9. Click **Add**.
   The WSadmin details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the WSadmin details from the list.
11. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Temporary Push Location	Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files

12. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the database in Oracle Linux that contains the private key and an associated certificate. *Example*: /etc/pki/java/cacerts
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the database in Oracle Linux that contains the CA certificates..
Trust store password	Enter the trust store password to access the keystore location.

13. Click **Add**.
    The certificate details are listed in the table.
14. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
15. Click **Save**.
    The device is onboarded successfully.

Websphere (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server details - Field Description Table

Fields	Description
***Server Type**	Select the **Websphere (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Windows server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device. If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List- Appviewx*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only if **Communication mode = Gateway**)

Windows gateway details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, select/enter the details as indicated below. (This section is displayed only if **Communication mode = SSM**)

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. In the **WSadmin credentials** section, select/enter the details as indicated below. These credentials are used to authenticate the wsadmin tool with the WebSphere Application Server so that it can execute administrative commands and access the necessary resources.

WSadmin credentials - Field description table

Fields	Description
WSadmin User name	Enter the designated WSadmin username for authentication.
WSadmin Password	Enter the secure password for WSadmin.
WSadmin directory path	Enter the file location / directory path where the WSadmin tool is stored.

10. Click **Add**.
    The WSadmin details are listed in the table.
11. *(optional step)* Click the delete icon, if you want to delete the WSadmin details from the list.
12. In the **Directory** section, enter the details as indicated below.

Directory section - Field description table

Fields	Description
WSadmin directory path	Enter the file location / directory path where the WSadmin tool is stored.

13. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the database in Oracle Linux that contains the private key and an associated certificate. *Example*: /etc/pki/java/cacerts
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the database in Oracle Linux that contains the CA certificates..
Trust store password	Enter the trust store password to access the keystore location.

14. Click **Add**.
    The certificate details are listed in the table.
15. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
16. Click **Save**.
    The device is onboarded successfully.

Data Power

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Data Power** from the dropdown field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Server name**	Enter the name of the designated IBM server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
***Resr Port**	Retain the value 22; it is the default port used for the communication.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List- Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
Is Https?	Select the checkbox to enable the secure mode.

8. Click **Save**.
   The device is onboarded successfully.

Domino

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Domino** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List- Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory**	Enter the directory/path where the application is installed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: /Installation_dir/domain-registry.xml

8. In the **Windows gateway details** section, enter the details as indicated below.

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

9. Click **Save**.
   The device is onboarded successfully.

MQServer (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQServer (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. SSH is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device. If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
Region	Enter the geographic region of the AWS instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

8. Click **Add**.
   The certificate details are listed in the table.
9. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. Click **Save**.
    The device is onboarded successfully.

MQServer (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQServer (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
Region	Enter the geographic region of the AWS instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only when **Communication mode** = **Gateway**).

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

9. Click **Add**.
   The certificate details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

IBMClient (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server details - Field description table

Fields	Description
***Server Type**	Select the **IBMClient (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

8. Click **Add**.
   The certificate details are listed in the table.
9. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
10. Click **Save**.
    The device is onboarded successfully.

IBMClient (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server details - Field description table

Fields	Description
***Server Type**	Select the **IBMClient (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below.

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. Click **Add**.
   The certificate details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

MQClient (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQClient (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated IBM server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
*: Mandatory fields	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only when **Communication mode** = **Gateway**).

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

9. Click **Add**.
   The certificate details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

JBoss

Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Click the + **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Linux** radio button.
***Server name**	Enter the name of the designated JBoss Linux server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the JBoss server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.
   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
Temp Directory	Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

8. Click **Save**.
   The JBoss Linux device is onboarded successfully.

Windows

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Windows** radio button.
***Server name**	Enter the name of the designated JBoss Windows server.
***Hostname**	Enter the hostname of the windows server that is to be onboarded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the JBoss server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If the **Communication mode = Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
**: Mandatory fields*	

If the **Communication mode = SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

8. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

9. Click **Save**.
   The JBoss Windows device is onboarded successfully.

Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Linux** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Linux server that is to be onboarded
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the Linux server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Linux server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the Linux server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Service account credentials** section, select/enter the details as indicated below. These credentials are used by the Linux application server to perform various tasks, such as accessing files, interacting with the operating system, and communicating with other applications and services.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Service account credentials - Field description table

Fields	Description
***Username**	Enter the designated username for authentication.
***Password**	Enter the secure password.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
Discover Formats	The Discover Formats fields contains all the possible certificate formats that are applicable to the 'Default' scan type. The formats include KBD(*.kbd), PEM(*.crt), PEM(*.cer), PEM(*.pem), DER(*.der) DER(*.cer), PKCS#7(*.p7b), PKCS#7(*.p7c), PKCS#12(*.p12), PKCS#12(*.pfx), JKS(*.JKS), JKS(*.keystore). To delete certificate format from the scan, click the 'x' icon in the respective cert type. To delete all the certificate format from the scan, click 'Clear' on the top-right of the field.
**: Mandatory fields*	

9. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Certificate Directory	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
Scan Type	Select any of the following: • *Default* - System scans for all certificate formats and adds them in the certificate inventory. • *Aggressive* - System scans for all keystore files with non-standard SSL extensions.
***Operation**	Enter the temporary or intermediate directory/path where certificates and keys are stored in the Apache server. *Example*: /inter/files
**: Mandatory fields*	

10. Click **Add**.
    The certificate location will be listed in the table.
11. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
12. Click **Save**.
    The Linux device is added successfully.

Microsoft IIS

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft IIS** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft IIS server.
***Hostname**	Enter the hostname of the Microsoft IIS server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Microsoft IIS server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft server device.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Gateway credential* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If **Gateway credential** is selected no other fields are displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). **Note:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote • LocalSystem **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***FQDN**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**. Enter the FQDN of the local system on which the Windows Gateway Agent will be installed.
***Port**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**. Enter the port number of the local system on which the Windows Gateway Agent will be installed.
***Select gateway**	**Note:** This field is not displayed when **Windows Gateway Mode** = **Integrated**. From the following options, select the gateway: • New • Existing

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

8. In the **Certificate location details** section, enter the details as indicated below.

Certificate Location Details - Field Description Table

Fields	Description
***Location type**	Select to the checkbox for *Certificate store* or *Centralized file system* or both as the location type.
***Certificate location**	Enter the directory or path where the certificate is stored. *Example*: C:\Cert\folder

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password vault**	Select any of the preconfigured password vault values. None is selected by default.
**: Mandatory fields*	

9. In the **Folder credential details** section, enter the details as indicated below.

Folder Credential Details - Field Description Table

Fields	Description
***Folder credentials**	Select from • Use gateway credential • New • Use device credential (disabled by default)
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Credential List - CyberArk* **Note:** If **Credential list - Appviewx** or **Credential list - CyberArk** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

10. Click **Save**.
    The Microsoft IIS device is onboarded successfully.

Microsoft PC

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click the **Server** tab.
3. Click the  **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft PC** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft PC server.
***Hostname**	Enter the hostname of the Microsoft PC server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Microsoft server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft server device.

Credentials - Field Description Table

Fields	Description
Credential Type	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
Username	Enter the designated username for authentication.. (field displayed for manual entry only)
Password	Enter the secure password. (field displayed for manual entry only)

7. Enter/Select the **Windows gateway details**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). **Note:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. Click **Save**.
   The Microsoft PC device is onboarded successfully.

Microsoft Server

Microsoft Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the ADC tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The Device details page is displayed.
4. Select **Microsoft Server** logo from the Vendors list. The following screen is displayed.
5. In the **Server Details** section button, enter/select details as mentioned below.

Server Details - Fields Description Table

Field Name	Description
Server Type	Select Server Type as **Microsoft Server**.
***Server name**	Enter the name of the designated Microsoft server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Microsoft server. Gateway is the preferred communication mode.
Host name	Enter the hostname of the server to be onboarded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Name	Description
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list. • Manual entry • Credential List - AppViewX • Credential List - CyberArk • Credential List - Hashicorp
***Username**	Enter the server name
Password	Select the data center from the dropdown list.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Credential List - cloudAccount

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Name	Description
	Note: If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext **Note:** Click the  (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2 **Note:** Click the  (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Enter/Select the **Windows gateway details**.

> **Note:** This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). **Note:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. In the **Certificate details** section, select/enter the details as follows. (This section is only displayed when **Communication mode = SSM**).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
***Keystore Credential Type**	Select the type of credential from the dropdown list. • Manual entry • Credential List - Thycotic **Note:** If **Credential list - Thycotic** is selected, the ***Keystore Credential Name** dropdown field is displayed. Select any of the preconfigured credential values.
Certificate location	Enter the directory/path where the application is installed. *Example*: C:\Microsoft\ADFS\
Certificate Password	Enter the certificate password. This field is only displayed for Keystore Credential Type = Manual entry)
**: Mandatory fields*	

9. Click **Add.**
   Once the server is added successfully, the path will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the server path from the list.
11. Click **Save**
    The device is onboarded successfully.

ADFS Server

The ADFS server can now be on-boarded into the AppViewX inventory. To onboard the ADFS server,

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the ADC tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The Device details page is displayed.
4. Select **Microsoft Server** logo from the Vendors list. The following screen is displayed.
5. In the **Server Type** radio button, select/enter the details below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Fields Description Table

Field Name	Description
Server Type	Select Server Type as **ADFS Server**.
***Server name**	Enter the name of the designated Microsoft ADFS server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Microsoft ADFS server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Microsoft server. Gateway is the preferred communication mode. (SSM is disabled by default)
Host name	Enter the hostname
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. (This option is disabled by default). • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials Section - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Credential List - AppViewX • Credential List - CyberArk • Credential List - Hashicorp
***Username**	Enter the server name

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Name	Description
Password	Select the data center from the dropdown list.
**: Mandatory fields*	

7. In the **Windows gateway details** section, select/enter the details as follows.

Windows Gateway Details - Field Description Table

Field Name	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. Click **Save**
   The device is onboarded successfully

The ADFS Server device can also be onboarded by the import functionality using the standard .xlxs and .csv templates available.

To onboard the ADFS server into the AppViewX inventory using the import functionality:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
2. Click the **Server** tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Click the **Import** button. The Import details page is displayed.
4. Click on the **CSV** or **XLSX** icons in the **Uploader Info** section. The sample templates are downloaded and saved at the default file location.
5. Open the CSV or XLSX templates, enter the relevant information for onboarding the ADFS server, and save the file.

> **Note:** Ensure all the mandatory and relevant fields are entered in the .csv or .xlsx template.

6. Click the upload icon in the **Import** section, and select the .csv or .xlsx file from the file dialog box. The status of the uploaded file is displayed in the **File Histories** section.

Microsoft SQL

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft SQL** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft SQL server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Microsoft SQL server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the Microsoft SQL server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft SQL server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following features: • Server addition using the **import** feature • Endpoint CSR generation
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, enter the details as indicated below. This section is displayed only if **Communication mode** = **SSM**.

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. Click **Save**.
   The Microsoft SQL device is onboarded successfully.

MySQL

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **MySQL** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated MySQL server that is to be onboarded
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the MySQL server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the MySQL server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the MySQL server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the MySQL server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the directory/path where configuration files are stored. *Example*: /tmp/files
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the directory/path where configuration files are stored. *Example*: /tmp/files
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Proxy required	Select the checkbox to enable the secure proxy service.

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
**: Mandatory fields*	

9. Click **Add**.
   The certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
11. Click **Save**.
    The MySQL device is added successfully.

NGINX

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Nginx** (Green N icon) from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Nginx server to be onboarded.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Nginx server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Nginx server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Nginx server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access • *None* **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

8. Click **Save**.
   The Nginx device is onboarded successfully.

Oracle

Weblogic (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server type**	Select **Weblogic (Linux)**.
***Server name**	Enter the name of the designated Oracle server.
***IP address**	Enter the valid IP address of the server being onboarded.
Data center	Select the desired data center from the dropdown list. It holds all the SSL related information that is to be retrieved from the server.
***SSH Port**	Enter the SSH port number. 22 is the default port used for the SSH communication mode.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Weblogic Installation directory	Enter the path where the weblogic installation file is saved. *Example:*/WL_installation_directory/domain-registry.xml

8. Click **Add**
   The Weblogic Installation directory is added successfully in the table.
9. *(optional step)* Click the (Delete) icon, if you want to delete the directory location from the table, or add more Weblogic Installation directories.
10. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the database in Oracle Linux that contains the private key and an associated certificate. *Example*: /etc/pki/java/cacerts
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the database in Oracle Linux that contains the CA certificates..
Trust store password	Enter the trust store password to access the keystore location.

11. Click **Add**
    The keystore location is added successfully in the table.
12. *(optional step)* Click the (Delete) icon, if you want to delete the certificate location from the list, or add more keystore locations.
13. Click **Save**.
    The Oracle Weblogic (Linux) device is on-boarded successfully.

Weblogic (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click the **Server** tab.
3. Click the  **(Add)** icon.
4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server type**	Select **Weblogic (Windows)**.
***Server name**	Enter the name of the designated Oracle server.
Communication Mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Oracle server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the Oracle Weblogic (Windows) server that is to be onboarded. This field is not mandatory if Communication mode is SSM.
Data center	Select the desired data center from the dropdown list. It holds all the SSL related information that is to be retrieved from the server.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. In the **Vendor Specific Details** section enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Weblogic Installation directory**	Enter the path where the weblogic installation file is saved. *Example:*/WL_installation_directory/domain-registry.xml
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
***Weblogic Installation directory**	Enter the path where the weblogic installation file is saved. *Example:*/WL_installation_directory/domain-registry.xml
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the database in Oracle Linux that contains the private key and an associated certificate. *Example*: /etc/pki/java/cacerts
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the database in Oracle Linux that contains the CA certificates..
Trust store password	Enter the trust store password to access the keystore location.

10. Click **Add**
    The keystore location is added successfully in the table.
11. *(optional step)* Click the (Delete) icon, if you want to delete the certificate location from the list, or add more keystore locations.
12. Click **Save**.
    The Oracle Weblogic (Windows) device is on-boarded successfully.

iPlanet

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details section - Field Description Table

Fields	Description
***Server type**	Select **iPlanet**.
***Server name**	Enter the name of the designated Oracle server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***IP address**	Enter the valid IP address of the server being onboarded.
Data center	Select the desired data center from the dropdown list. It holds all the SSL related information that is to be retrieved from the server.
***SSH Port**	Enter the SSH port number. 22 is the default port used for the SSH communication mode.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials section - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
***WADM User name**	Enter the username for the WADM CLI (Command line interface) utility. WADM defines all the commands that are supported for configuring and administering the server.
***WADM Password**	Enter the password for the WADM CLI utility.
***WADM directory path**	Enter the file location/directory path to where the WADM utility is stored.
**: Mandatory fields*	

8. In the **Certificate Details** section enter the details as follows.

Certificate Details- Field Description Table

Fields	Description
Database path	Enter the file location/directory path of the database where the certificates are stored.
Password	Enter the password for the certificates database.

9. Click **Add**
   The database path is added successfully in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the database path from the list, or add more accordingly.
11. Click **Save**.
    The Oracle iPlanet device is on-boarded successfully.

Other Devices

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Other Devices** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server Type**	The server type has a fixed value **Other devices**.
***Server name**	Enter a unique name of the designated server to be onboarded.
***IP address/ FQDN**	Enter the valid IP address of the device to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the VMware server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Click **Save**.
   The device is onboarded successfully.

RabbitMQ

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **RabbitMQ** logo from the Vendors list.
   The RabbitMQ server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the server name.
***IP address/ FQDN**	Enter the valid IP address or FQDN
Data center	Select the desired data center from the dropdown list.
Communication mode	Select the required communication mode. The possible options are: • SSH • SSM
***SSH Port**	Enter the SSH port number

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This field is displayed only if the Communication mode selected is SSH.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. This option is **disabled** by default. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Credential List - AppViewX • Credential List - CyberArk • SSH
***Username**	Enter the username.
***Password**	Enter the password.
**: Mandatory fields*	

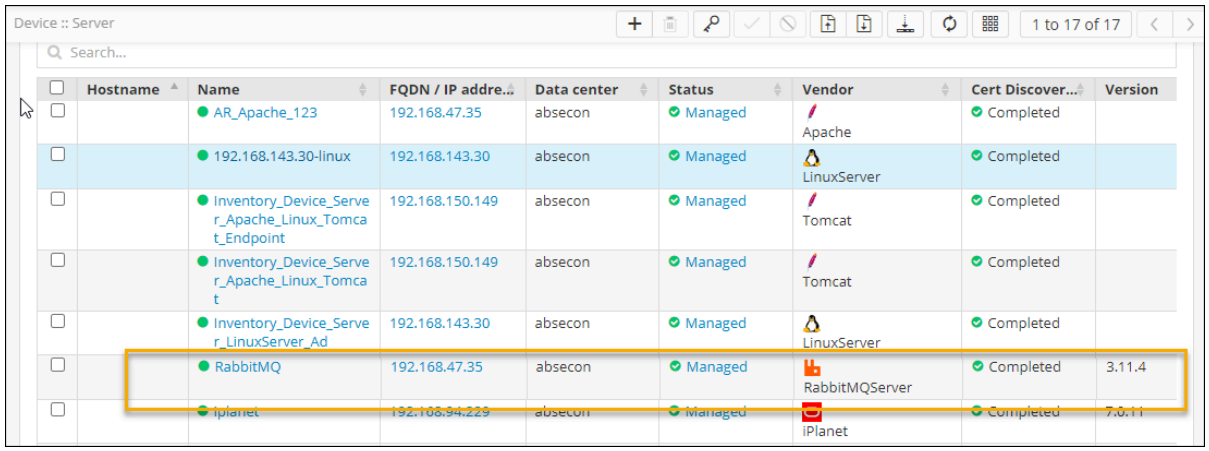
7. In the **Vendor Specific Details** section enter the details as follows.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the path where the config file is saved. *Example:*etc/rabbitmq/rabbitmq.config
**: Mandatory fields*	

8. Click **Save**.
   The device is on-boarded successfully and the version number in the **Version** column will contain the value **3.11.4**.



SAP

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **SAP** logo from the Vendors list.
   The **SAP** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type from radio button options. • ABAP • WebDispatcher • Java (Disabled by default)
***Server name**	Enter the name of the designated SAP server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the SAP.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the SAP server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select default value *sudo* to execute with root privileges using sudo access. **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
***Client ID**	Enter the following details: • Client ID • Web Service User ID • Web Service Password • Web Service Port The following fields are required to invoke the web service to bind the certificate into the selected profile. The values entered in the fields are used to frame and invoke the API with the credential.
***Web Service User ID**	
***Web Service Password**	
***Web Service Port**	
Is Https?	Select the checkbox to frame the API with http or https.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

8. In the **SAP SID Details** section, enter details as mentioned below.

SAP SID Details - Field Description Table

Fields	Description
SAP SID Details	Enter the three digit character code SAP System Identification (SAP SID). It corresponds to the identifier for an SAP system. Enter the values in upper case only.
*: Mandatory fields	

9. Click **Save**.
   The SAP device is added successfully.

VMware

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **vmware** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type as **VMware** from the dropdown list.
***Server name**	Enter the name of the designated VMware server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the VMware.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the VMware server.
***HTTPS Port**	Enter the valid HTTPs port number that is required to remotely access VMware.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
***Base URL**	Enter the base URL that is to be appended with the API.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: /policy/api/v1
**: Mandatory fields*	

8. Click **Save**.
   The VMware device is added successfully.

Deleting Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the **Delete** icon in the command bar.
   The **Delete** confirmation pop-up window is displayed.
5. Click **Yes** on the confirmation pop-up.
   The server will be removed from the inventory

Import Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

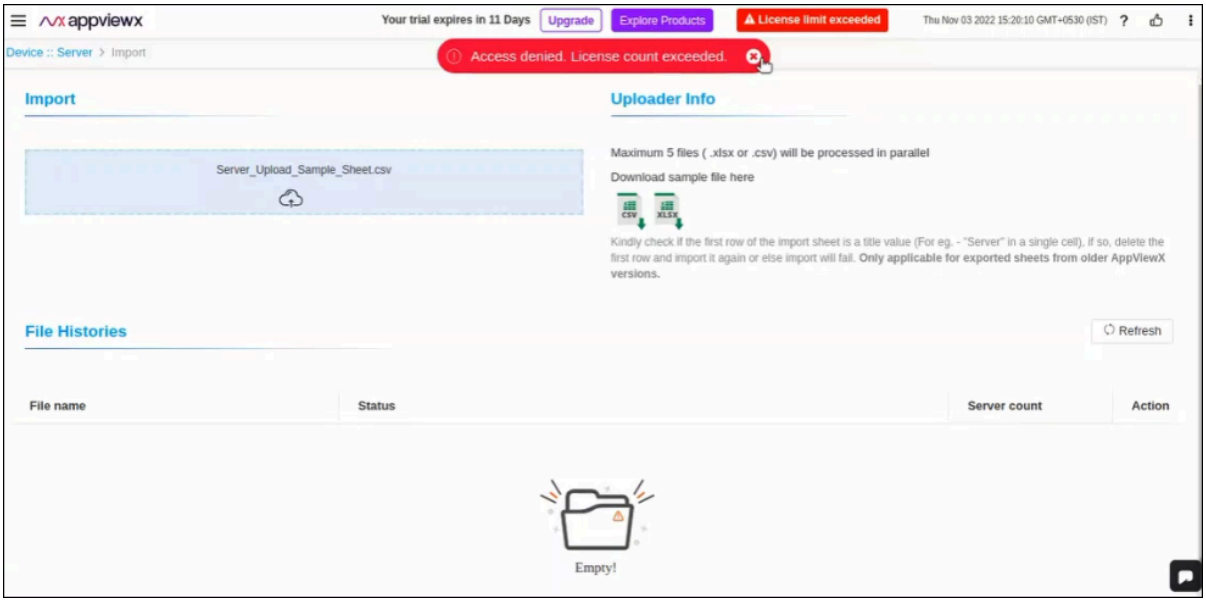
4. Click the (**Import**) icon in the command bar.
   You will be redirected to the import server page.
5. Download the sample <.csv> or <.xls> file.
6. Update the details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Click the **Browse** and **Upload** button.
8. Upload the files.
   Sever details provided in the sheet will be added to the server inventory.

License Enforcement

AppViewX has enabled a feature to set a limit for the licensed certificates. If the number of certs exceeds this limit then the additional certs added into the inventory will be moved into the **Monitored** status.



- A red indicator labelled **License Limit Exceed** is displayed on the title bar of the page, if the limit has exceeded.
- A pop-up message **Access denied. License count exceeded** is displayed on the click of the **Save** button while adding a new server device.

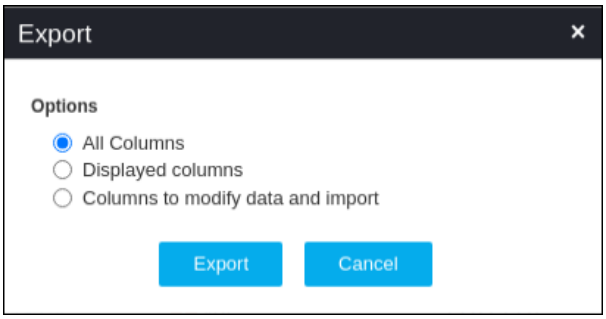
Export Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple servers of the same kind, select the check-boxes for each one.

> **Note:** If the desired server device is not listed on the screen, run a search.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click the  (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up, select the type of information you want to export and click the **Export** button.



   a. **All Columns** - Select this option if you want to export all information about the server.
   b. **Displayed columns** - Select this option if you want to export only the information that is visible on the server screen. This is useful if you need to compare values or settings for different servers and do not have any need to see the less important data.
   c. **Columns to modify data and import** - Select this option if you are exporting device details to make modifications and then re-import the data into the Device Inventory.
6. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
   Server details will be downloaded as an Excel `<.xls>` file.

Manage Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. To start managing the device, click the  (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   - The "Config fetch" will be triggered and the server will get managed.
   - The server status is changed to Manage.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Unmanage Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the Command bar at the top of the screen.
5. Click the **Yes** button from the confirmation popup message that is displayed.
   Server device status is changed to UnManaged in Server inventory.

Fetch Config for Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name.

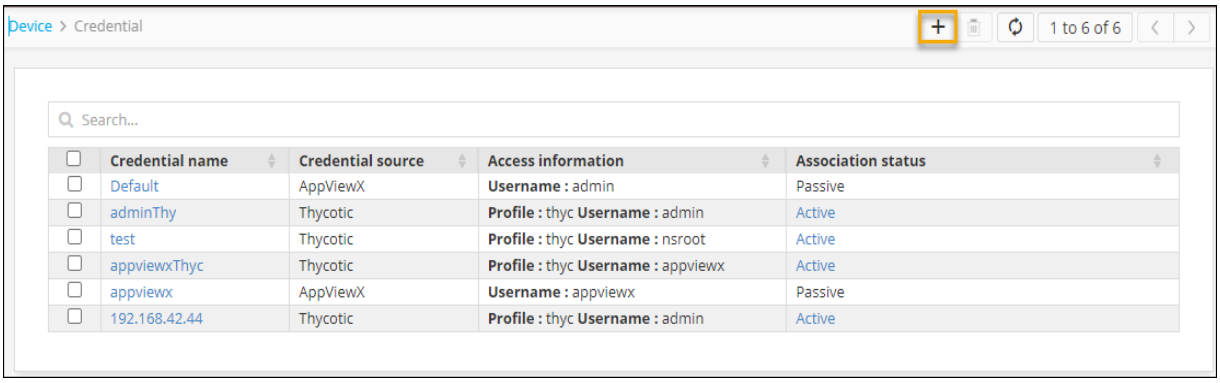
> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the server.** The configuration will be fetched from the server.

Add Credentials

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Credentials**) icon in the command bar.
   The Credentials page is displayed. If credentials have been set up, a list of credential names with details will be displayed in a table as shown below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



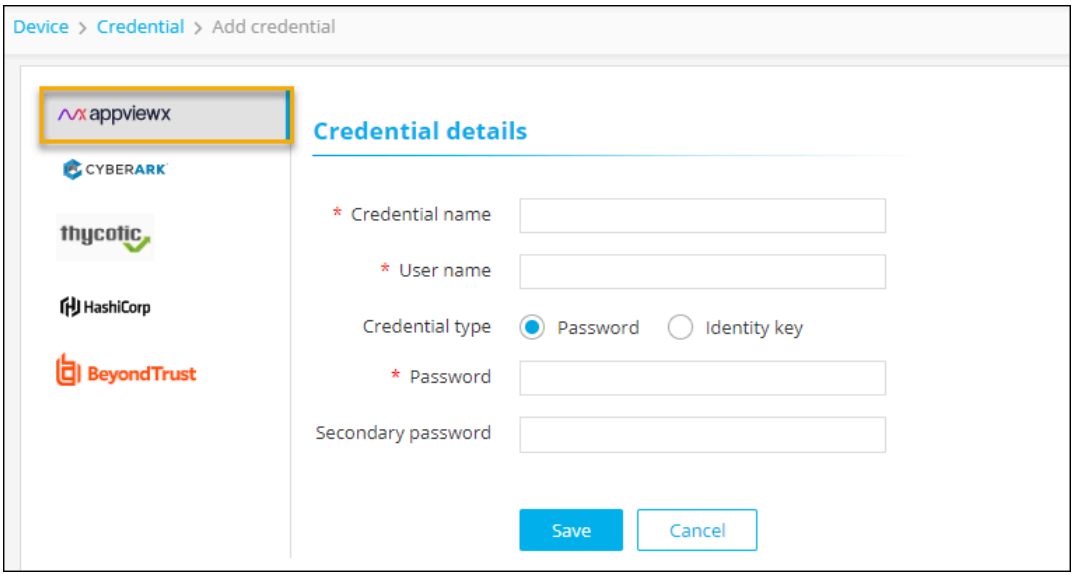
4. To add a new credential, click the plus or + (**Add**) icon in the command bar of the Credentials page.
   The Add Credential page is displayed with default credentials fields for AppViewX.

> **Note:** For details of fields in AppViewX and other vaults refer to the sections below.

AppViewX

AppViewX is shipped with a built-in integration with HashiCorp Vault for software level security to secure the private keys and device credentials onboarded to the product.

To configure credential details for the AppViewX enter the fields described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

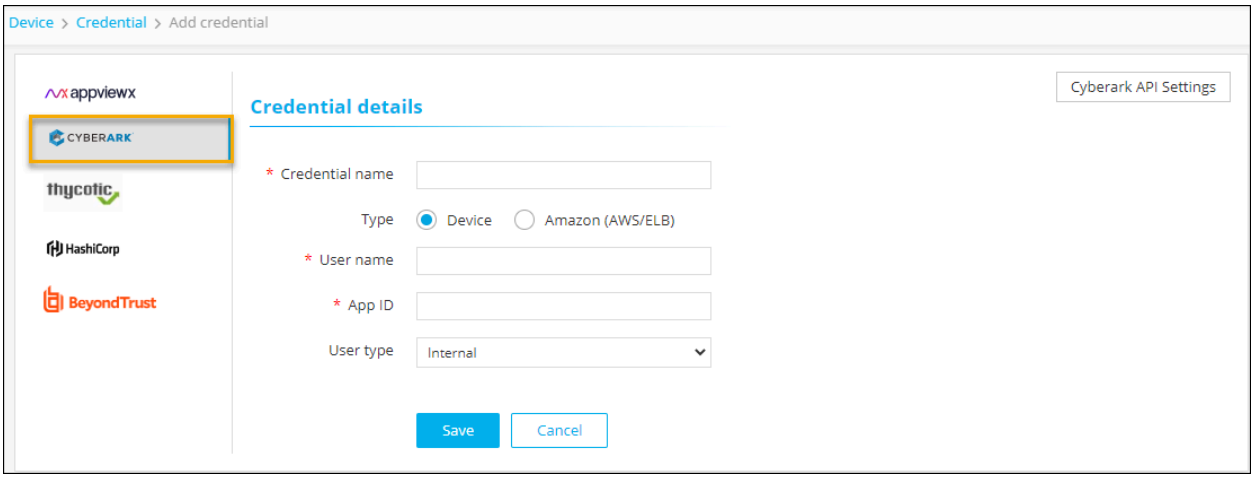
Field Description for AppViewX Credentials

Fields	Description
***Credential name**	Name for the credential for the users to identify it.
***User name**	User name used for device onboarding.
Credential type	Select the type of authentication from one of the following: • Password • Identity key
***Password**	Password configured at the time of device onboarding. **Note:** This field is displayed only when the **Credential type** is selected as **Password**.
Secondary password	Additional password enabled by vendors for specific operations. **Note:** This field is displayed only when the **Credential type** is selected as **Password**.
***Identity key**	Credentials (private key in the **.pem** or **.txt** format) for enabling device communication via SSH. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
Passphrase	Key to protect the private key files. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
All * marked fields are mandatory.	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Cyberark

To configure credential details for the CyberArk vault enter the fields described in the table below.



Field Description for Cyberark Credentials

Fields	Description
***Credential name**	Name for the credential for the users to identify it.
Type	To retrieve a credential from the CyberArk vault, select one of the following options: • Device (default) • Amazon (AWS/ELB)
***User name**	User name that has been added in CyberArk. **Note:** This field is displayed when the **Device** type is selected.
***App ID**	App ID that has been authorized to provide access to CyberArk and retrieve credentials. **Note:** This field is displayed when the **Device** type is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Cyberark Credentials (continued)

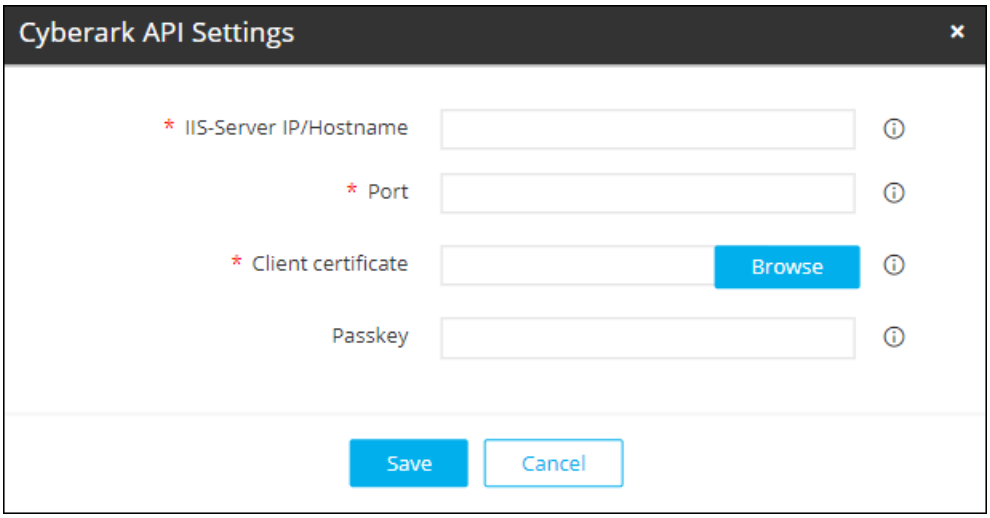
Fields	Description
User type	From the dropdown list menu, select one of the following: • Internal (user created directly in the device) • External (user created in the Active Directory) **Note: *Server IP Address** field is displayed when the **User type** is selected **External**.
***Server IP Address**	Server IP Address has to be entered if the user has created external active directory. **Note:** This field is displayed when the User type is selected as **External**.
***AWS IAM username**	User name that has been added in CyberArk. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***App ID**	Reference ID provided by CyberArk for the corresponding application. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***AWS access key ID**	Access key ID generated from the AWS management console. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Cyberark Credentials (continued)

Fields	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

To configure credential details for the CyberArk vault, from the top right corner of the page, click **CyberArk API Settings**.



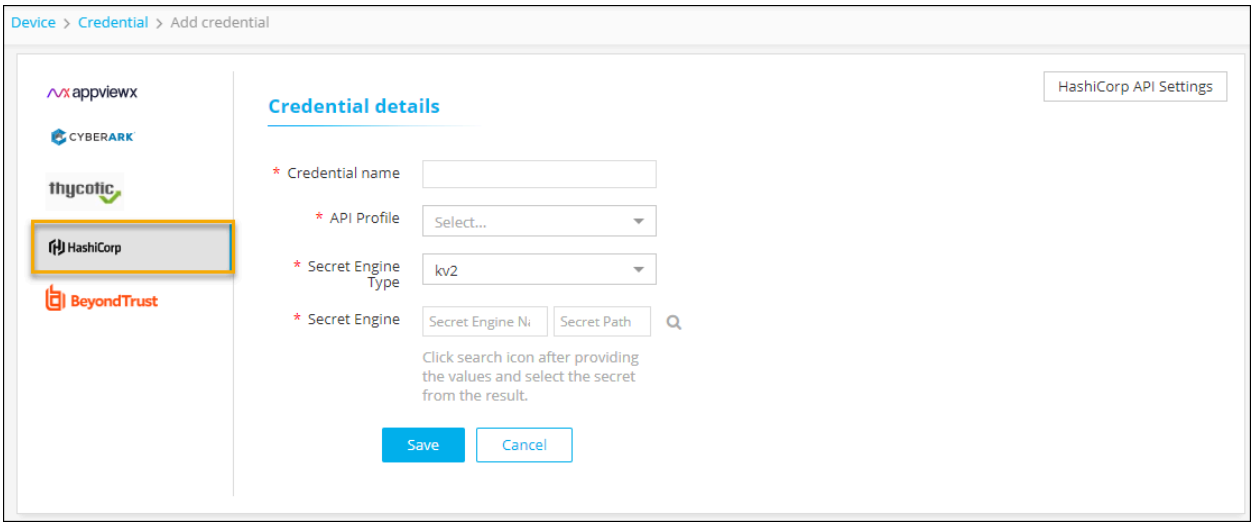
Field Description for Cyberark API Settings

Fields	Description
***IIS-Server IP/Hostname**	Hostname or IP address of the CyberArk application.
***Port**	Port number on which CyberArk is running.
***Client certificate**	Upload the Client Certificate needed to authenticate the CyberArk API service.
***Passkey**	Enter the passkey for Client Certificates uploaded in the .pfx format.
Note: The asterisk (*) symbol indicates a mandatory field.	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HashiCorp

To add credentials for HashiCorp Vault enter the fields described in the table below.



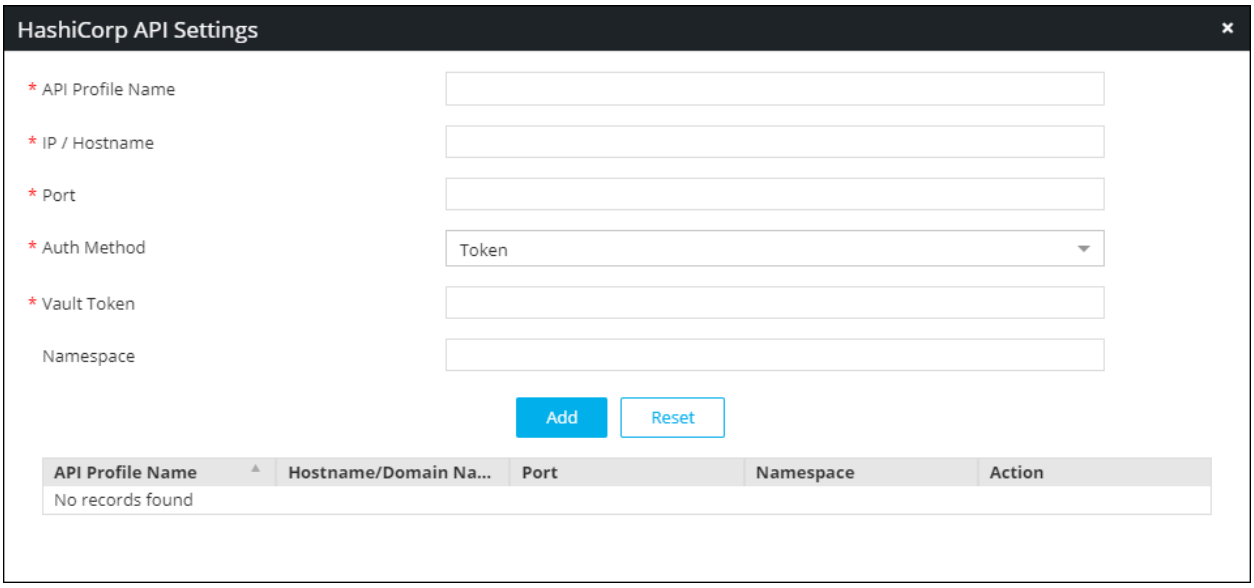
Field Description for HashiCorp Credentials

Fields	Description
***Credential name**	Unique name for the credential for the users to identify it.
***API Profile**	Select the API profile from the dropdown list which is configured in HashiCorp API settings.
***Secret Engine**	Type path and click enter. It will suggest a list of secrets and the desired secret can be selected.

Note: The asterisk (*) symbol indicates a mandatory field.

To set API Credentials: From the top right corner of the page, click **HashiCorp API Settings**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for HashiCorp API Settings

Field	Description
***API Profile Name**	Enter a unique API profile name.
***IP/Hostname**	Enter the HashiCorp vault hosted IP address or hostname.
***Port**	Enter the port in which the HashiCorp vault is running.

***Auth Method**	From the dropdown list list, select either **Token/AppRole.**
	
	• If **Token** is selected, enter the **Vault Token** for the authentication.
	• If **AppRole** is selected, enter the following:
	  • Enter the **RoleID**
	  • Enter the **SecretID**

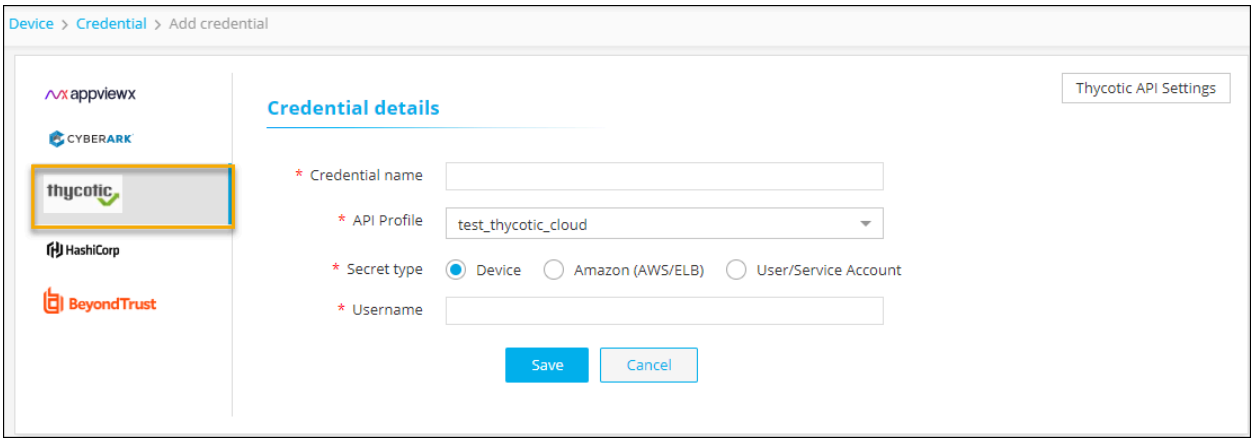
Namespace	Enter a namespace.

Note: The asterisk (*) symbol indicates a mandatory field.

Thycotic

To add credentials for Thycotic secret enter the fields described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



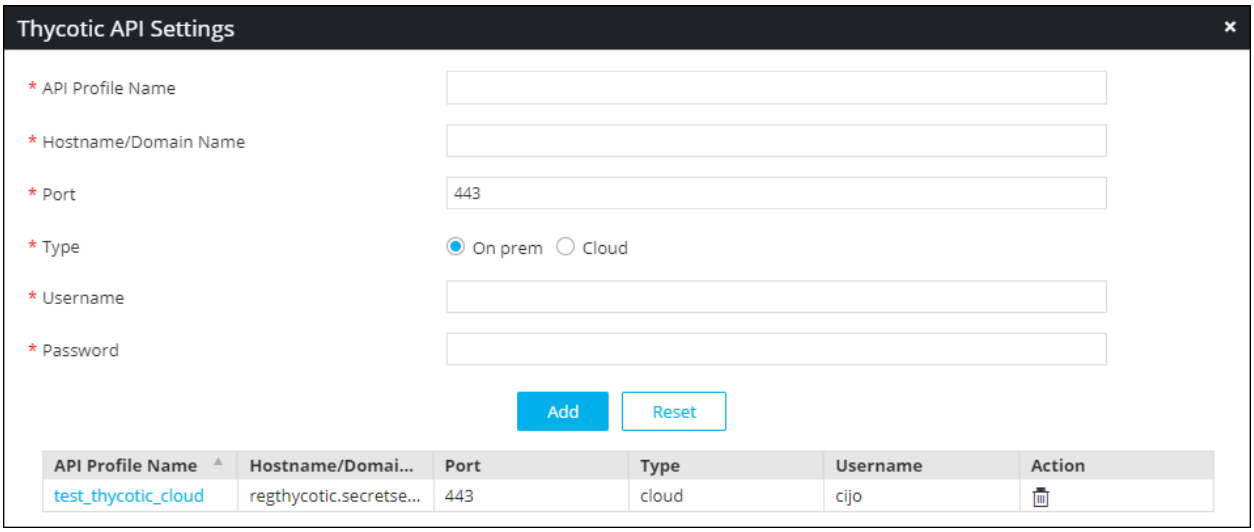
Field Description for Thycotic Credentials

Fields	Description
***Credential name**	Reference name for Thycotic in AppViewX.
***API Profile**	If you have more than one Thycotic Server added as profiles, select the respective profile while adding credentials.
***Secret Type**	Select secret type as Device or Amazon (AWS/ELB) or User/Service Account.
Username	Enter the username of the secret if you selected the Secret Type as Device.
AWS IAM Username	Enter the AWS IAM username if you selected the Secret Type as Amazon.

Note: The asterisk (*) symbol indicates a mandatory field.

To set API Credentials: From the top right corner of the page, click **Thycotic API Settings**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Thycotic API Settings

Fields	Description
***API Profile Name**	Reference name for the vault in AppViewX.
***Hostname/Domain Name**	Enter the Hostname of the Thycotic Secret Server if it is hosted in an on-prem environment or the Domain name of the Thycotc Secret Server if it is the cloud version.
***Port**	Port number of the Thycotic Secret Server.
***Type**	Select if Thycotic Secret Server is hosted in an On prem or Cloud environment.
***Username**	Username of Thycotic Secret Server.
***Password**	Password of Thycotic Secret Server.

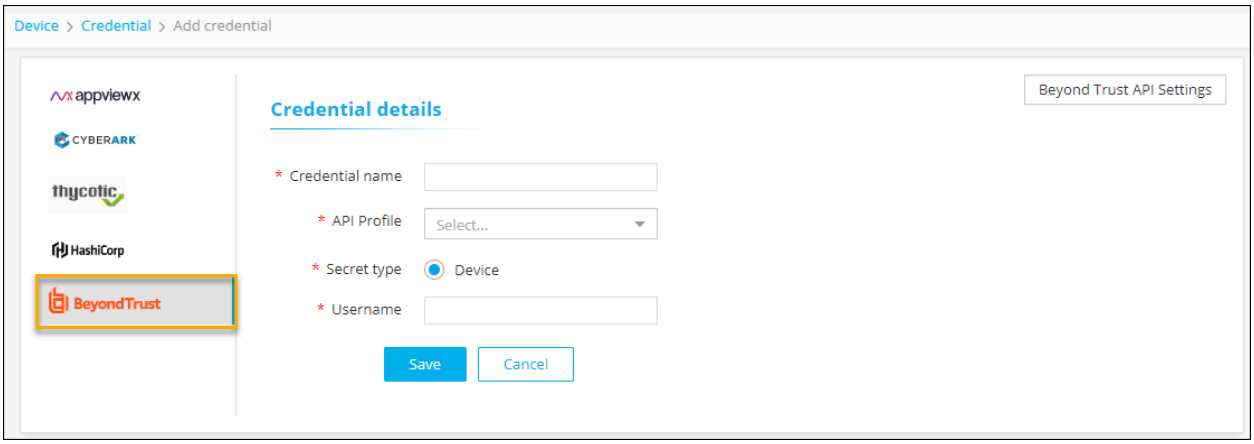
Note: The asterisk (*) symbol indicates a mandatory field.

Note: You can add multiple Thycotic Secret Servers as different Profiles. Each Thycotic Secret Sever will be added to the Thycotic API settings page.

BeyondTrust

To add credentials for BeyondTrust Vault enter the fields described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



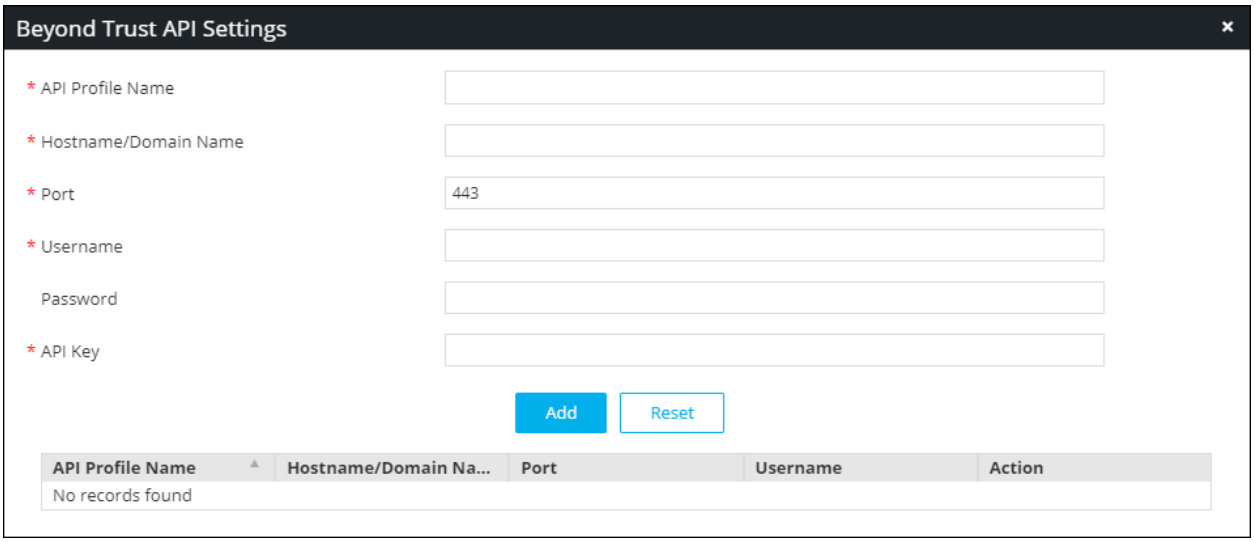
Field Description for Beyond Trust Credentials

Fields	Description
***Credential name**	Reference name for BeyondTrust in AppViewX.
***API Profile**	If you have more than one BeyondTrust Server added as profiles, select the respective profile while adding credentials.
***Secret Type**	Select the secret type as Device. Only secrets associated with any device can be added with this secret type. i.e., Secret should contain the device name.
Username	Enter the username of the secret if you selected the Secret Type as Device. When this secret is used in any device, respective device name will be automatically send as one of the argument when AppViewX fetches credential from Vault.

Note: The asterisk (*) symbol indicates a mandatory field.

To set API Credentials: From the top right corner of the page, click **BeyondTrust API Settings**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Beyond Trust API Settings

Fields	Description
***API Profile Name**	Reference name for the vault in AppViewX.
***Hostname/Domain Name**	Enter the Hostname of the BeyondTrust Secret Server if it is hosted in an on-prem environment or the Domain name of the BeyondTrust Secret Server if it is the cloud version.
***Port**	Port number of the BeyondTrust Secret Server.
***Username**	Username of BeyondTrust Secret Server.
Password	Password of BeyondTrust Secret Server.
***API Key**	It is the security key provided for authentication.

Note: The asterisk (*) symbol indicates a mandatory field.

Note: You can add multiple BeyondTrust Secret Servers as different Profiles. Each BeyondTrust Secret Server will be added to the BeyondTrust API settings page.

Enabling Vault as a Service

Vault as a service refers to the provision of Vault, a popular tool for securely storing and accessing sensitive information. It implies that all the vaults and credentials from the platform can be in all the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

applicable places. For example, if a new credential type feature is supported in the platform, then those credentials will be available to all the vendors in the Server addition page. You do not have to manually make changes for supporting the same in the respective module. The following credentials are now made available to all vendors on the Server device addition page:

- CyberArk
- Thycotic
- HashiCorp
- BeyondTrust

Vault as a service enables the following capabilities:

- Fetches all available credential store from platform.
- Removes the Static Credential type drop down List maintained from Web.
- Consumes the retrieved vaults from platform at required places.
- Vaults are automatically listed in consumption places (e.g. Server device addition)when added in Platform.
- Sets the access list based on user-selected credential type from the available vaults.
- Supports all the vault services of the imported vendors servers.

Device Setting

AKAMAI CPS

During enrollment using server device as endpoint, Akamai has a long list of details that are mandatorily required for the enrollment request. Adding these fields along with the CSR parameters will make the enrollment form too big with many details to be filled out. Since these are fixed values and only have to be filled once, the other mandatory fields are made available in the global device settings page. The details saved on the global setting page are based on the combination of the fields **Validation Type**, **Secure Network**, and **Vendor Certificate Type** that are available on the enrollment page.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **Akamai** logo from the Vendors list.
   The Akamai Vendor Specific Details configuration screen is displayed.
5. Enter the fields in the respective sections described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Description of fields on the Vendor Specific Details page.

Fields	Description
General Information	
***Validation Type**	Select a validation type from the dropdown list for the endpoint. The default value is **Third-party**.
***Secure Network**	Select the secure network from the dropdown list for the endpoint. The default value is **Standard TLS**.
***Vendor Certificate Type**	Select a vendor certificate type from the dropdown list for the endpoint. The default value is **Third-party**.
Organization Information	
***Name**	Enter the organization's name.
***Address**	Enter the organization's address.
***Country**	Enter the organization's country code.
***City/Municipality**	Enter the organization's city or municipality.
***State/Province**	Enter the organization's state or province.
***Zip/Postal Code**	Enter the organization's zip or postal code.
***Phone Number**	Enter the organization's phone number.
Admin Contact Information	
***First name**	Enter the administrator's first name
***Last name**	Enter the administrator's last name
***Phone number**	Enter the administrator's phone number
***Email**	Enter the administrator's email
Tech Contact Information	
***First name**	Enter the technical contact's first name
***Last name**	Enter the technical contact's last name
***Phone number**	Enter the technical contact's phone number
***Email**	Enter the technical contact's email

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
* (asterisk): *Mandatory fields*	

6. Click **Update**.
   The vendor details are saved successfully.

Configuring Firewall

- Add Firewall
- Delete Firewall
- Import Firewall
- Export Firewall
- Manage Firewall
- Unmanage Firewall
- Fetch Config for Firewall

Add Firewall

Adding a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the + (**Add**) icon.
4. Enter the *General information, Credentials, Secondary device information* in the device details form.
   You can configure multiple device details for the same vendor.
5. Once the server is added successfully you are redirect to the device server inventory. The status of the server can be viewed in the Status column

AppViewX has enabled a feature to set a limit for the licensed certificates. If the number of certs exceeds this limit then the additional certs added into the inventory will be moved into the **Monitored** status.

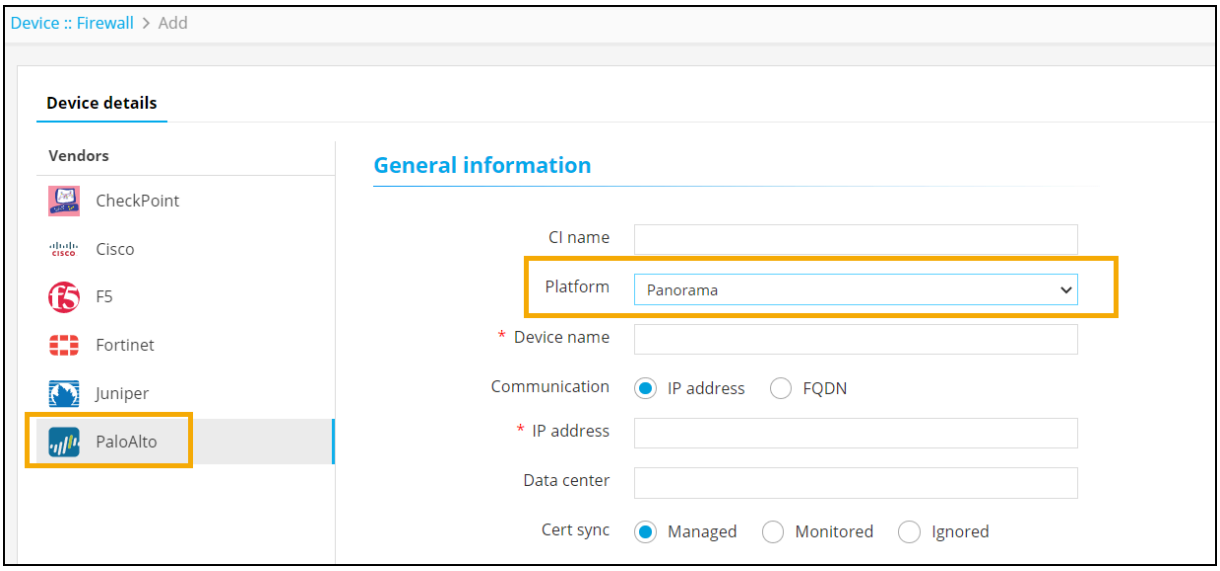
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- A red indicator labelled "**License Limit Exceed**" appears on the title bar of the page, if the limit has exceeded.
- A pop-up message "**Access denied. License count exceeded.**" is displayed on the click of the Save button while adding a new server device.
- All the new on-boarded server certs (Server/ADC/Firewall/WAF Device config sync) into the inventory will be mapped to the**Monitored** state.

Configuring Palo Alto Firewall

To push certificates to Palo Alto firewalls that are being managed through **Panorama**, you need to first configure the Palo Alto firewall.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the + (**Add**) icon.
4. On the **Device :: Firewall > Add** page, under **Device Details**, select the **Vendor** as **Palo Alto**.



5. Enter the required field information to configure the Palo Alto firewall and click **Save**.

Certificate Push all Palo Alto Firewalls using Panorama platform

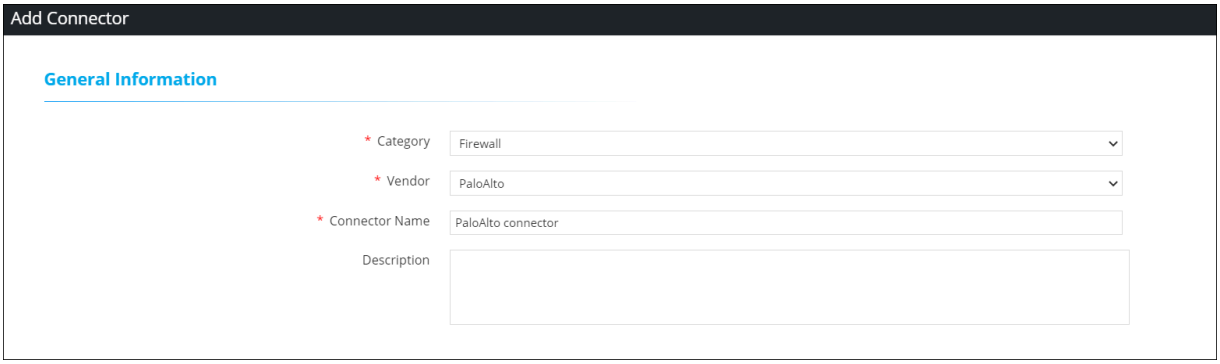
To push certificate(s) to the configured Palo Alto firewall:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. In the Server Certificates inventory, search for the certificate to be pushed to the **Palo Alto** firewall.

> **Note:** You can enroll any new server certificate from the inventory and push it to the Panorama device, which in turn pushes the certificate to the managed firewall device.

2. Select a certificate.
3. Click **Add Connector**.
4. In the **Add Connector** window, under the **General Information** section, select the required field information.



The following table describes the field information in this section:

Field Description for General Information

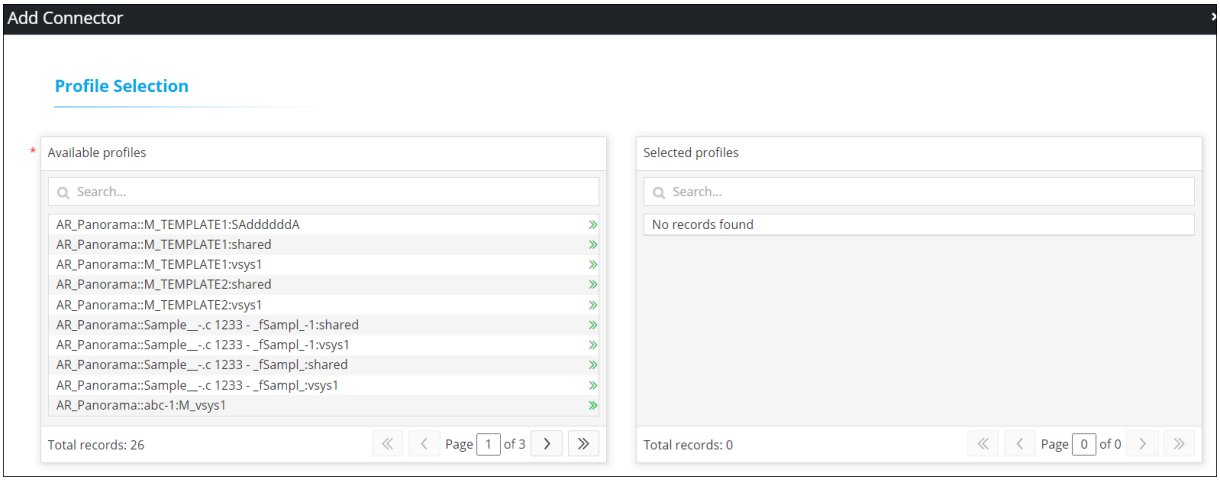
Fields	Description
***Category**	Select the Category as Firewall.
***Vendor**	Select the Vendor as Palo Alto. **Note:** The values in this field populate based on the Category selected.
***Connector Name**	Displays the connector name based on the vendor selected in the previous field.
Description	Enter a description.

Note: The asterisk (*) symbol indicates a mandatory field.

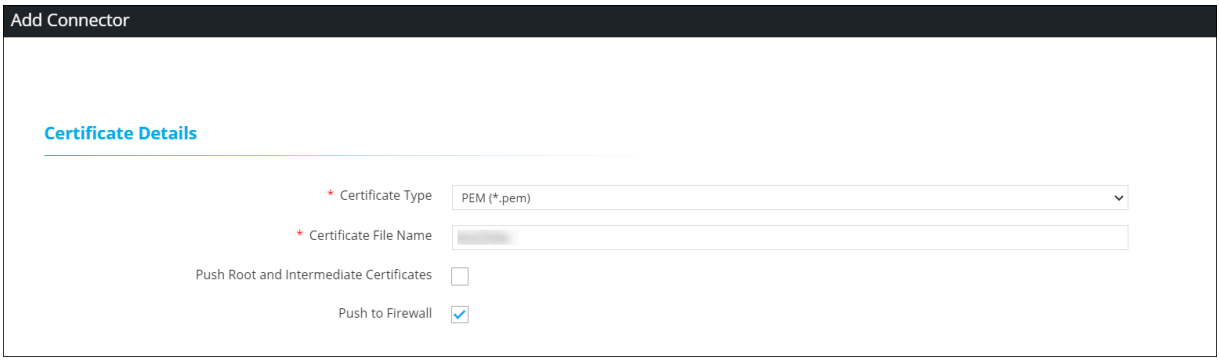
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Profiles Selection** section will be auto-populated based on the values entered in fields in the General Information section with the profiles containing the Panorama template stack name. The profiles are displayed in the following format:

Device::Template_Stack::Template::shared/vsys



5. To select a profile to be pushed to the Firewall, click the arrow button next to the profile name.
6. In the **Certificate Details** section, enter or select the required field information.



Field Description for Connector Certificate Details

Fields	Description
***Certificate Type**	Select the Certificate Type from the options available in the dropdown.
***Certificate File Name**	Enter the certificate file name.
Push Root and Intermediate Certificates	Select this checkbox to push the root and intermediate certificate along with the server certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

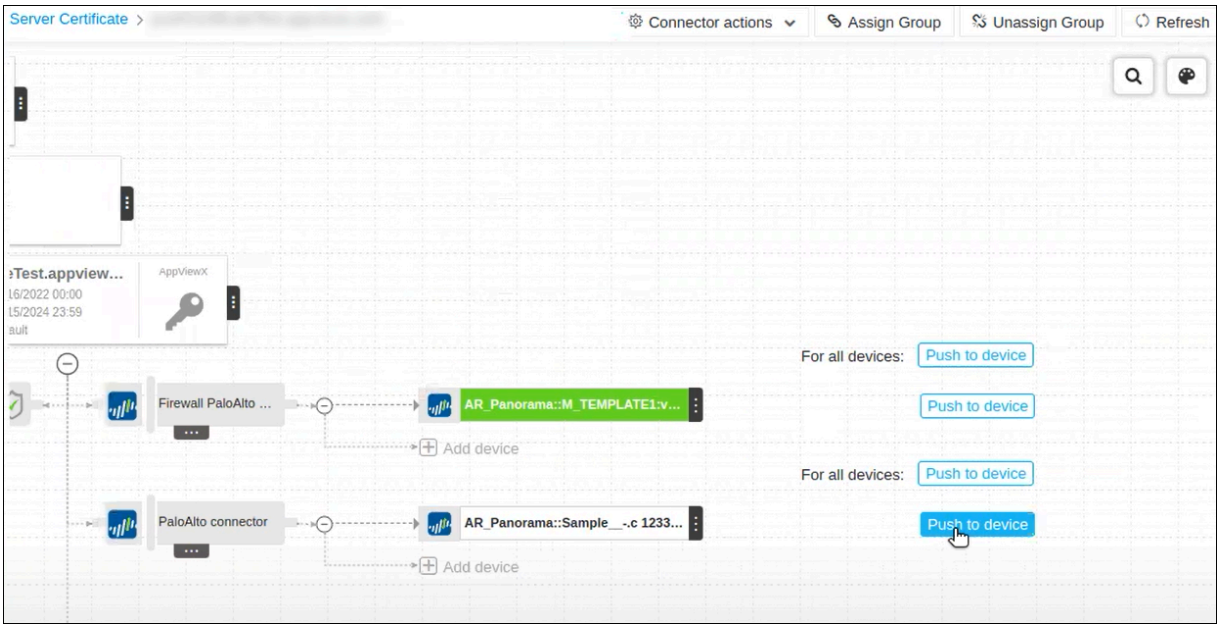
Fields	Description
Push to Firewall	Select this checkbox to push the certificate to the firewall.

Note: The asterisk (*) symbol indicates a mandatory field.

7. Click **Save**.

   You will be redirected to the Certificate Holistic View.

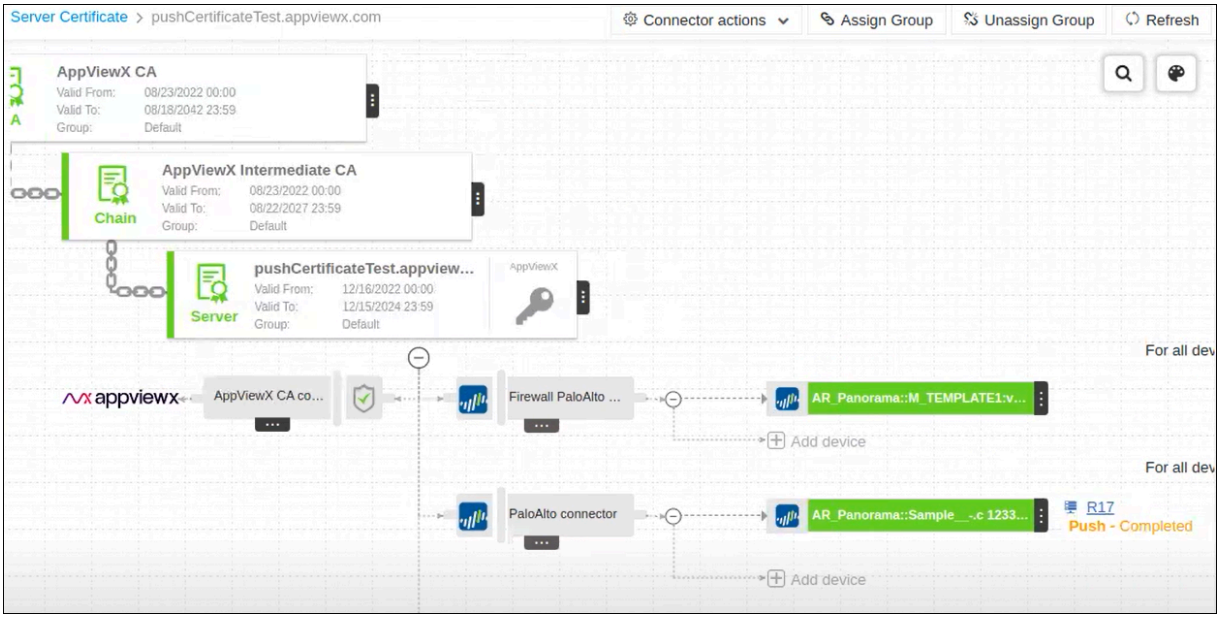
8. Click **Push to Device** for the newly added connector.



9. Click **Approve**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The certificate is pushed to the Panorama platform and also associated with the Palo Alto firewall.



Delete Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Delete**) icon in the command bar.
   The **Delete** confirmation popup window is displayed.
5. Click **Yes**.
   The firewall will be removed from the device inventory.

Import Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: If the desired server device is not listed on the screen, run a search.

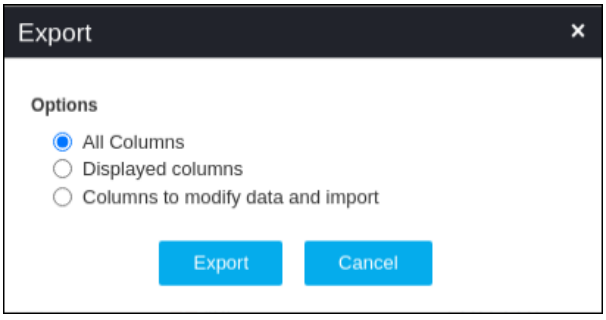
4. Click the  (**Import**) icon in the command bar.
   You will be redirected to the import firewall page.
5. Download the sample <.csv> or <.xls> file.
6. Update the details.
7. Click the browse and upload button.
8. Upload the files.
   Firewall details will be updated to the firewall inventory.

Export Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple firewalls, select the check-boxes for each one.

Note: If the desired server device is not listed on the screen, run a search.

4. Click the  (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up screen that is displayed, select the type of information you want to export and click the **Export** button.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. **All Columns** - Select this option if you want to export all information about the firewall.
b. **Displayed columns** - Select this option if you want to export only the information that is visible on the firewall screen.
c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the firewall Inventory.

6. On the screen that opens, select the location where you want the firewall details file to go, then click **Save**.
   Firewall details will be downloaded as an Excel `<.xls>` file.

Manage Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. To start managing the firewall, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   - Config fetch will be triggered and the firewall will get managed.
   - Firewall status is changed to **Manage** in Firewall inventory.

Unmanage Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the command bar at the top of the screen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click the **Yes** button from the confirmation popup message that is displayed.
   Firewall device status is changed to UnManaged in Firewall inventory.

Fetch Config for Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the firewall.** The configuration will be fetched from the server.

Configuring Cloud

- Add Cloud
- Delete Cloud
- Import Cloud
- Export Cloud
- Manage Cloud
- Unmanage Cloud
- Fetch Config for Cloud

Add Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the (**Add**) icon.
   The **Device details** page is displayed.
4. Enter the *Basic Information, Key Information, Additional Attributes* in the device details form.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click the **Add** button.
   - You can configure multiple device details for the same vendor.
   - Once the cloud device is added successfully you will redirect to the cloud inventory.
   - The status of the cloud can be viewed in the Status column.

> **Note:** With the introduction of the **Cert License Enforcement**; Server Auto discovery of EC2 instances will be on-boarded with certs status as **Monitored**, even if managed state is configured in the Cloud account configuration.

Delete Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the  (**Delete**) icon in the command bar.
   The **Delete** confirmation popup window is displayed.
5. Click **Yes**.
   The cloud will be removed from the device inventory.

Import Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the  (**Import**) icon in the command bar.
   You will be redirected to the import cloud page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Download the sample <.csv> or <.xls> file.
6. Update the details.
7. Click the browse and upload button.
8. Upload the files.

   Cloud details will be updated to the firewall inventory.

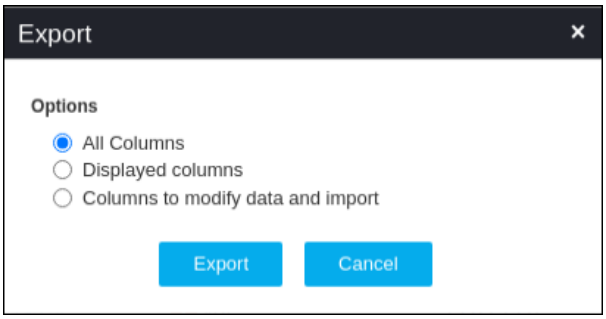
Export Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.

   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the **Export** icon in the command bar at the upper right of the screen.
5. On the **Export** pop-up screen that is displayed, select the type of information you want to export:



   a. **All Columns** - Select this option if you want to export all information about the cloud.
   b. **Displayed columns** - Select this option if you want to export only the information that is visible on the cloud screen.
   c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the cloud inventory.
6. On the screen that opens, select the location where you want the cloud details file to go, then click **Save**.

   Cloud details will be downloaded as an Excel `<.xls>` file.
7.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Manage Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. To start managing the cloud, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   - Config fetch will be triggered and the cloud will get managed.
   - Cloud status is changed to **Manage** in Cloud inventory.

> **Note:** With the introduction of the **Cert License Enforcement**; Server Auto discovery of EC2 instances will be on-boarded with certs status as **Monitored**, even if managed state is configured in the Cloud account configuration.

Unmanage Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   Cloud device status is changed to UnManaged in Cloud inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fetch Config for Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the  (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the cloud.** The configuration will be fetched from the server.

Configuring WAFs

- Adding a WAF Device
- Delete a WAF Device
- Import a WAF Device
- Export a WAF Device
- Manage a WAF Device
- Unmanage a WAF Device
- Fetch Config for WAF Devices

Adding a WAF Device

- Barracuda
- CloudFlare
- F5
- Imperva Securesphere

Barracuda

1. Go to (**Menu**) > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click the **WAF** tab.
3. Click the + **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Barracuda** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
Platform	Select the platform from the dropdown field • Azure • AWS • On-Prem
***Device name**	Enter a unique name for the device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the device to be onboarded.
***Rest port**	Enter the rest port number.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Barracuda. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Barracuda.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. In the **Secondary device information** section, select/enter the details as follows.

Fields	Description
Secondary / Alternate device	Select either *Auto-detect* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** select/enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. (*Optional step*) Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

CloudFlare

1. Go to (**Menu**) > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **Device details** page is displayed.

4. Select **Cloudflare** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
***Account name**	A user defined unique name to identify the server. No special characters other than '-' , '_' , '.' , '*' , '|' , '!' and spaces are not allowed.
Data center	Enter the data center routing. It holds all the SSL related information that is to be retrieved from the Cloudflare device.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Cloudflare.
***Token based Authentication**	Select the checkbox to enable the token based authentication.
API Token	Enter the API token if the token based authentication is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	This field will be visible if the Credential Type is selected as **Manual entry and token based authentication is disabled** . Enter the designated username for Cloudflare.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry and token based authentication is disabled** . Enter the designated password to access Cloudflare.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

7. Click **Save**.
   The device is onboarded successfully.

F5

1. Go to (**Menu**) > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **f5** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
Platform	Select the platform from the dropdown field. ASM is the default value.
***Device name**	Enter a unique name for the device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the device to be onboarded.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Barracuda. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Barracuda.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
***Token based authentication**	Select the checkbox to enable the token based authentication.
**: Mandatory fields*	

7. In the **Secondary device information** section, select/enter the details as follows.

Fields	Description
Secondary / Alternate device	Select either *Auto-detect* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** select/enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. (*Optional step*) Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

Imperva Securesphere

1. Go to (**Menu**) > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Imperva Securesphere** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
Platform	Select the platform from the dropdown field. AWS is the default value.
***Device name**	Enter a unique name for the device to be onborded.
Communication	Select from *IP address* and *FQDN*.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the device to be onboarded.
***Rest port**	Enter the rest port number.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Proxy Required	Enable this field if the device communication needs to happen via a proxy. The proxy details configured in general settings will be used for communication.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Access type**	Select the method to access the Barracuda. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Barracuda.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

7. In the **Secondary device information** section, select/enter the details as follows.

Fields	Description
Secondary / Failover / Sync group	Select either *Ignore* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** select/enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. (*Optional step*) Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

Delete a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Delete**) icon in the command bar.
   The **Delete** confirmation popup window is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click **Yes**.
   The firewall will be removed from the device inventory.

Import a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the  (**Import**) icon in the command bar.
   You will be redirected to the import page.
5. Click **Browse** to navigate to the location of the file to be uploaded.
6. Once the file is selected, click **Upload**.
7. Click **Submit**.

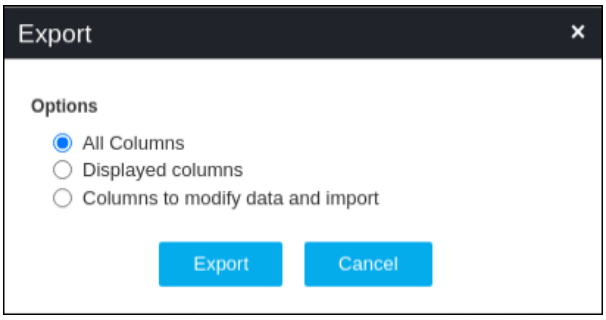
Export a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple devices, select the check-boxes for each one.

> **Note:** If the required device is not listed on the screen, run a search.

4. Click the  (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up screen that is displayed, select the type of information you want to export and click the **Export** button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



a. **All Columns** - Select this option if you want to export all information about the firewall.
b. **Displayed columns** - Select this option if you want to export only the information that is visible on the firewall screen.
c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the firewall Inventory.

6. On the screen that opens, select the location where you want the firewall details file to go, then click **Save**.
   Device details will be downloaded as a **.xls** file.

Manage a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. To start managing the device, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   • Config fetch will be triggered and the device will get managed.
   • Device status is changed to **Manage** in the inventory.

Unmanage a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. Click the  (**Unmanage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation popup message that is displayed.
   Device status is changed to **UnManaged** in the inventory.

Fetch Config for WAF Devices

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. Click the  (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the device(s).**
   The configuration will be fetched from the server.

Certificate Reports

Once the certificates are discovered and managed/monitored in AppViewX, those certificates can be viewed as the reports in dashboards. For some of the reports, email notifications can be enabled as well provided with the other functionality as downloading the report/data.

> **Note:** Default reports will contain data only if there is at least one relevant certificate present for that report in the inventory. Otherwise, it displays pop-up message as **No Records Found**.

- SMTP Configuration
- Troubleshooting SMTP
- Fetch All Default Reports
- Job Scheduler

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Types of Scheduled Jobs
- Device and Certificate Synchronization
- CRL Certificate Revocation Check
- Configuring Report Settings and Schedule
- Report Routing
- Validation Settings
- Revocation Check Routing
- Securing CERT+

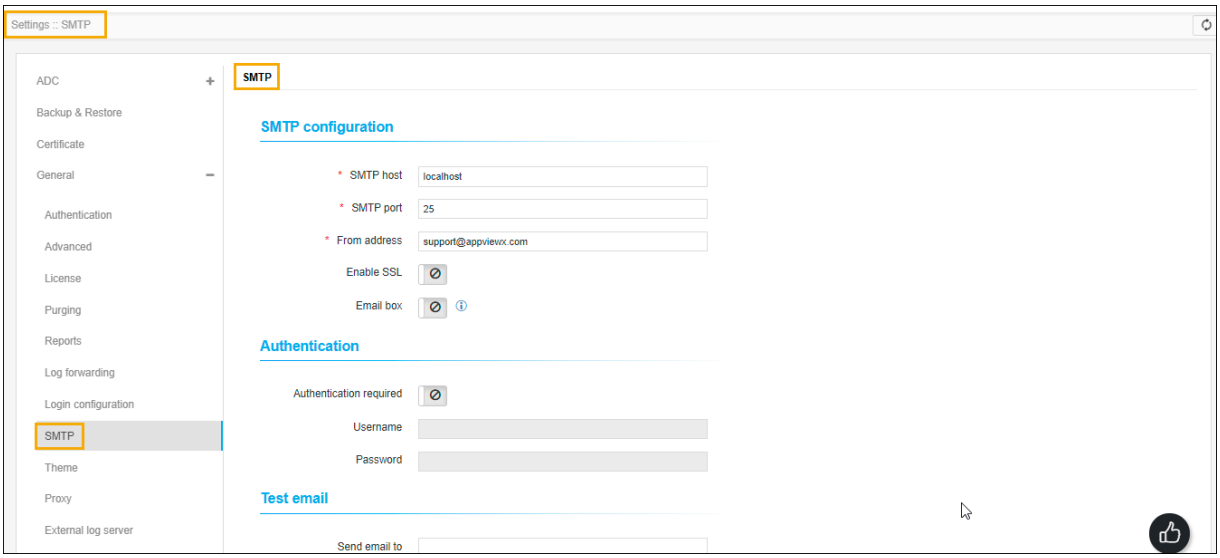
SMTP Configuration

To get the certificate reports sent as a mail, we will have to first configure SMTP

1. Log in to the AppViewX application with valid credentials.
2. Click on the menu button.

   The left navigation pane is displayed.
3. Click **Settings.**

   The **Settings** page is displayed.
4. Expand the General menu and then click **SMTP.**



5. Refer to the fields in the table below to update the information on the SMTP page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

SMTP Page - Field Description Table

Name	Type	Description	Error Message
* SMTP host	Text	The server that will send the email.	Enter valid Hostname/ IP address <x.x.x.x>.
* SMTP port	Text	Port to connect to the email server.	• Port can contain only numbers. • Enter a port number between 0-65535.
* From address	Text	Mail address from which mail is to be received by the user.	• Please enter a valid email.
Enable SSL	Toggle button	To enable/disable SSL while sending mail.	NA
Email box	Toggle button	Enabling this setting will use IMAP for the mailbox.	NA
* Email	Text	Email for IMAP. Mandatory if Email box is enabled.	• Please enter a valid email.
Password	Text	Password for IMAP. Mandatory if Email box is enabled.	This field is mandatory.
* Hostname	Text	The hostname for IMAP. Mandatory if Email box is enabled.	• Enter valid Hostname/ IP address <x.x.x.x>.
Authentication required	Toggle button	To enable/disable Authentication required.	NA
* Username	Text	The username if authentication required. Mandatory if Authentication required is selected as true.	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

SMTP Page - Field Description Table (continued)

Name	Type	Description	Error Message
* Password	Text	Mandatory if Authentication required is selected as true.	NA
* Send email to	Text	Test email to check if able to send mail after configuring the above settings. Mandatory if you want to test.	Enter a valid email.

Note: The asterisk (*) symbol indicates a mandatory field.

Troubleshooting SMTP

Error Message	Possible Cause	Possible Solution
Please provide a valid value.	Anyone of the mandatory fields is invalid or is missing.	Provide valid values for all mandatory fields.
E-Mail sending was unsuccessful.	• If trying to test, no/valid email is not provided in the ‘send email to’ field. • Credentials and field values may be incorrect.	• If trying to test, provide a valid email in the ‘send email to’ field. • All the credentials and fields should be correct.
Service unavailable. Try after some time.	avx_subsystems or avx_platform_gateway is not running.	Restart the plugin.

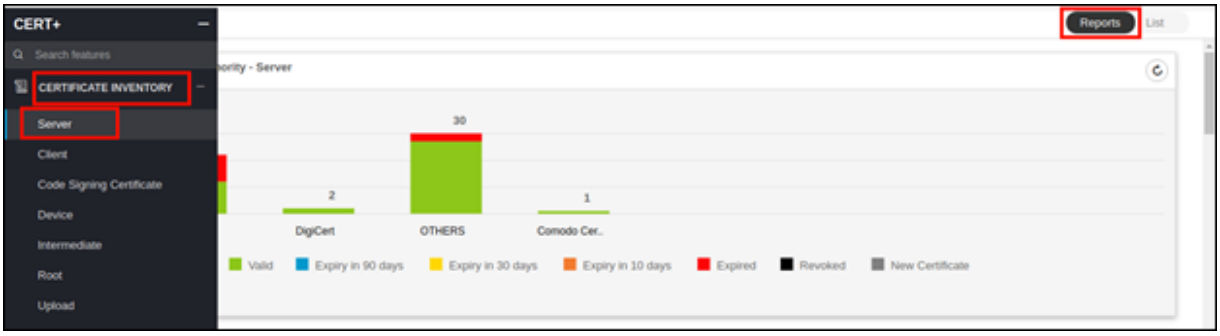
Fetch All Default Reports

All Reports will be present separately for each certificate category. To view Reports for certain certificate categories, follow the steps given below.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server** or **Client** or **Code Signing Certificate**.
2. In the top right corner, click **Reports** tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The respective report page is displayed.



Job Scheduler

Overview

This topic describes the basic functionality of the job schedulers available in CERT+. These cron jobs are scheduled in the background to check, monitor, audit the certificates in inventory. The AppViewX Platform cron job checks the certificate cron job every 15 minutes and looks for the changes and triggers the job at a scheduled time.

The Cron job frameworks are,

- Check
- Monitor
- Audit

Check

- Each Cron Job is executed for the batch of certificates (depending on the job) asynchronously and on successful completion, the status is updated in the database.
- All Cron jobs executed asynchronously based on the scheduled time.
- Each Cron job is bound to the internal business logic to update the status in the database.

Monitor

- Cron jobs are scheduled at recurring intervals and customized to run the job multiple times in a day or months.
- Audit Logs are captured in the logging subsystem.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Audit

- The auditing is enabled subsystem-wise (ADC+ and CERT+) based on internal business logic.
- Notification logs and Audit logs are captured for each internal business logic.

Types of Scheduled Jobs

List of Scheduled jobs for the certificates:

- Device and Certificate synchronization
- Certificate compliance check
- Certificate polling request
- CRL Certificate Revocation Check
- CRL Download Monitor Job
- Certificate Revoke Status Check From CA
- Auto Regenerate Certificates
- Delete Expired Certificates
- Auto-Renew Certificates
- Certificate Expiry Status Check
- Periodic CRL Update for AppViewX and Custom CAs
- CA Connector Validity Updater
- Certificate Vulnerability Check
- Certificate CAA Record Check
- Certificate Transparency Check
- Certificate Validation Check.

Device and Certificate Synchronization

This periodical running job synchronizes the data such as certificates and objects used for application connectors from devices to AppViewX. The device includes ADC, Servers, Firewall, WAF, Cloud, and MDM.

- **Check** -
  - The cron job is executed to synchronize the inventory certificates from the managed device inventory.
  - The device inventory is categorized as ADC, Server, WAF, Firewall, Cloud, MDM, and so on.
  - The <config fetch> is executed and the certificates are fetched from the managed devices.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Monitor** - The scheduled job is monitored and triggered by default daily at 03:00 A.M.
- **Audit** - Audit logs are captured in internal business logic.

Certificate Compliance Check

A compliance check is the process of review and analysis of the implemented controls to check that the implemented controls and their outputs meet the certificate policy requirements. It checks the compliance for all the certificates in the inventory. If the policy is changed the compliance will be in pending status till this job is executed.

- **Check**
  - The cron job is executed to check the compliance status for all certificates in the inventory.
  - If the policy is changed the compliance will be in pending status till this job is executed.
  - Once the job is completed, the **compliance report** is updated in the **server and client** certificates dashboard.
- **Monitor** - The scheduled job is monitored and triggered by default daily at 05:00 A.M.
- **Audit** - The internal business logic for compliance checks is captured via audit logs and notification logs.

Certificate Polling Request

This job gets triggered only during the performance of CLM actions. Once the CSR gets submitted to the Certificate Authority, until the signed certificate is received from the certificate authority, the polling request job gets triggered to collect the certificate in the response.

CRL Certificate Revocation Check

To download the CRL for all the certificates in the inventory and validate with the downloaded CRL record. You can change the revocation status in the inventory.

- **Check**
  - The cron job is executed to download CRL data for all the certificates available in the inventory.
  - Once CRL is downloaded compare and change the revocation status in the inventory.
- **Monitor** - The scheduled job is monitored and triggered by default daily every 6 hours.
- **Audit** - The internal business logic for certificate revocation check is captured via audit logs and notification logs in the logging module.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CRL Download Monitor Job

To monitor the certificates in inventory and download the CRL for the newly added certificate. Make sure that the below actions are completed for the CRL download monitor job.

- **Check** - The cron job is executed to monitor the certificates in inventory to download the CRL for the newly synchronized certificate.
- **Monitor** - The scheduled job is monitored and triggered by default every 5 minutes.
- **Audit** - The internal business logic for the certificate download monitor job is captured via audit logs and notification logs in the logging module.

Certificate Revoke Status Check From CA

For all the certificates managed or monitored in the inventory, this job will be performed periodically at the configured duration. Based on this check, the certificate status in the inventory will be updated with either revoked or others.

Note: This feature is supported only for Digicert CA.

- **Check** - The cron job is executed to check only the certificate revoke status from the CA Portal.
- **Monitor** - The scheduled job is monitored and triggered by default every 15 minutes.
- **Audit** - The internal business logic to check the certificate revoke status from the CA portal is captured via audit logs and notification logs in the logging module.

Auto-Regenerate Certificates

This job is triggered periodically to check whether the regeneration action to be triggered for the certificates in the inventory that are enabled with Regenerate Automatically in the CA connector, based on whether the certificate is reached the time to trigger the regenerate action.

- **Check** - The cron job is executed for auto regeneration of certificates at a scheduled time.
- **Monitor** - The scheduled job is monitored and triggered by default daily at 02:00:00 A.M.

Note: Auto generates for the certificate available in the inventory, enabled with Auto regenerate action in the CA connector when the threshold is reached, as mentioned in the CA connector form, the auto regenerate will be triggered.

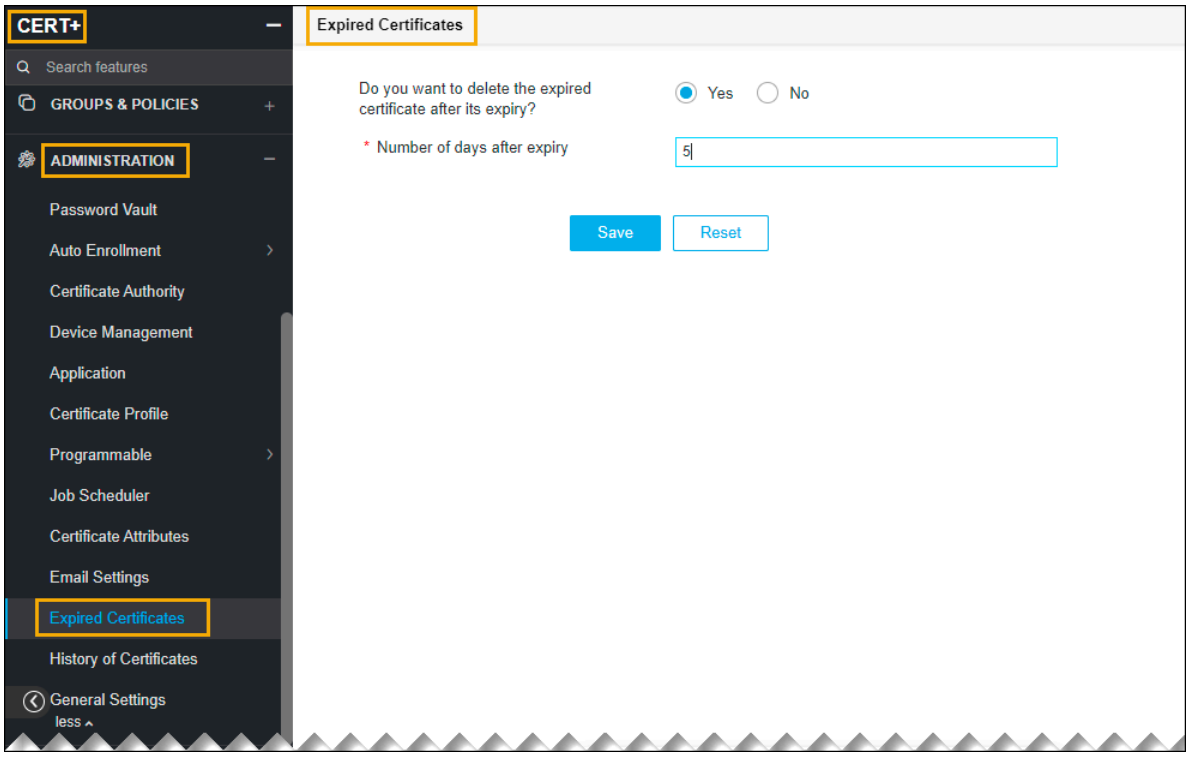
- **Audit** - The internal business logic of auto-regenerates certificates is captured via audit logs and notification logs in the logging module.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Delete Expired Certificates

This is a periodical job to check and delete the expired certificates available in the inventory. This job will be triggered only when this action is enabled in “Expired Certificates”.

- **Check** - The cron job is executed to delete the expired certificates in the inventory. To enable the delete expiry certificate function, do the following steps:
  1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
  2. Enable **Yes** to delete the expired certificates.



Note: Once enabled, automatically the expiry certificate will be deleted.

- **Monitor** - The scheduled job is monitored and triggered by default daily at 03:00:00 A.M.
- **Audit** - The internal business logic of auto regenerate certificates are captured via audit logs and notification logs in the logging module.

Auto-Renew Certificates

This job is triggered periodically to check whether the renewed action to be triggered for the certificates in the inventory that are enabled with Renew Automatically in the CA connector, based on a certificate is reached the time to trigger the renew action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Check** - To auto-renew certificates if it is scheduled.
- **Monitor** - The scheduled job is monitored and triggered by default daily every 6 hours.
- **Audit** - The internal business logic of auto-renew certificates is captured via audit logs and notification logs in the logging module.

Certificate Expiry Status Check

This job is triggered periodically to update the expiry status for all the certificates in the inventory.

- **Check** - The cron job is executed to check the expiry status of all the certificates available in the inventory.
- **Monitor** - The scheduled job is monitored and triggered by default daily 20 minutes every 5 hours.
- **Audit** - The internal business logic to check the expiry status is captured via audit logs and notification logs in the logging module.

Periodic CRL Update for AppViewX and Custom CAs

To do the CRL rotation for AppViewX and Custom CA. The CRL is regenerated, any expired certificates are removed from the CRL.

- **Check** - The cron job is executed to rotate CRL for AppViewX and Custom CA so that the CRL is regenerated, any expired certificates are removed from the CRL.
- **Monitor** - The scheduled job is monitored and triggered by default daily at 05:00:00 A.M.
- **Audit** - The internal business logic to update the CRL is captured through audit logs and notification logs in the logging module.

CA Connector Validity Updater

It allows to check the validity offered by CA and update the same in CA connector and policy.

- **Check** - The cron job is executed to check the validity offered by the External CA and update the same in CA connector and Certificate policy.
- **Monitor** - The scheduled job is monitored and triggered by default on every Sunday at 06:00:00 A.M.
- **Audit** - The internal business logic to update the CA connector and Policy is captured via audit logs and notification logs in the logging module.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Vulnerability Check

This is a periodical running job to update the vulnerability report data available in the dashboards Server endpoint security. It allows checking the vulnerability in the device such as Toodles, Heart bleed, and Roca.

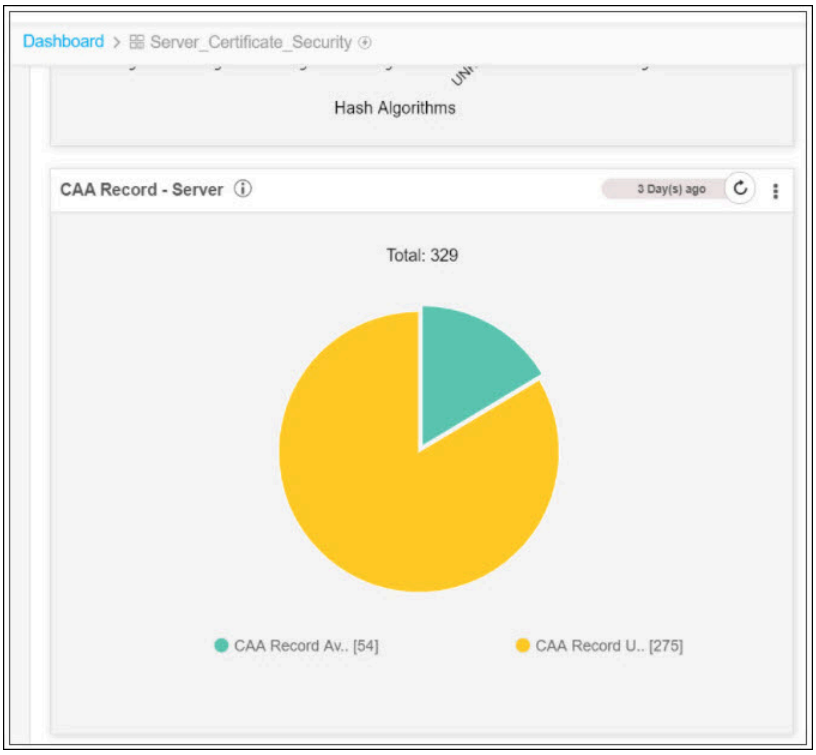
- **Check** -
  - The cron job is executed to check the certificates and their device association
  - There is internal business logic to check the Poodle, Heart bleed, and Roca vulnerabilities for the associated device.
  - Once the job is completed the “Vulnerability reports” are updated in “Server_Endpoint_Security”, “Client_Endpoint_Security”.
  - The ROCA vulnerability is a cryptographic weakness that allows the private key of a key pair to be recovered from the public key in keys generated by devices with the vulnerability.
  - The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
  - The Poodle vulnerability lets an attacker eavesdrop on communication encrypted using SSLv3. The vulnerability is no longer present in the Transport Layer Security protocol (TLS), which is the successor to Secure Socket Layer (SSL).
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Saturday.
- **Audit** - The internal business logic to check the vulnerability of the device. It is captured via audit logs and notification logs in the logging module.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate CAA Record Check

A Certification Authority Authorization (CAA) record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.CAA records allow domain owners to declare which certificate authorities are allowed to issue a certificate for a domain. They also provide a means of indicating notification rules in case someone requests a certificate from an unauthorized certificate authority. If no CAA record is present, any CA is allowed to issue a certificate for the domain. If a CAA record is present, only the CAs listed in the record(s) are allowed to issue certificates for that hostname.



- **Check** -
  - The cron job is executed to check the CAA record for all the certificates in the inventory.
  - Once the job is completed, the CAA report is updated in the server_certificate_security dashboard.
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Monday.
- **Audit** - The internal business logic to check the CAA records for all the certificates are captured through audit logs and notification logs in the logging module.

Certificate Transparency Check

This is a periodical running job to update the certificate transparency report data available in the dashboard Server certificate security. It allows checking the certificate transparency for all certificates in the inventory (Google CT project). The Certificate Transparency safeguards the certificate issuance process by monitoring and auditing HTTPS certificates.

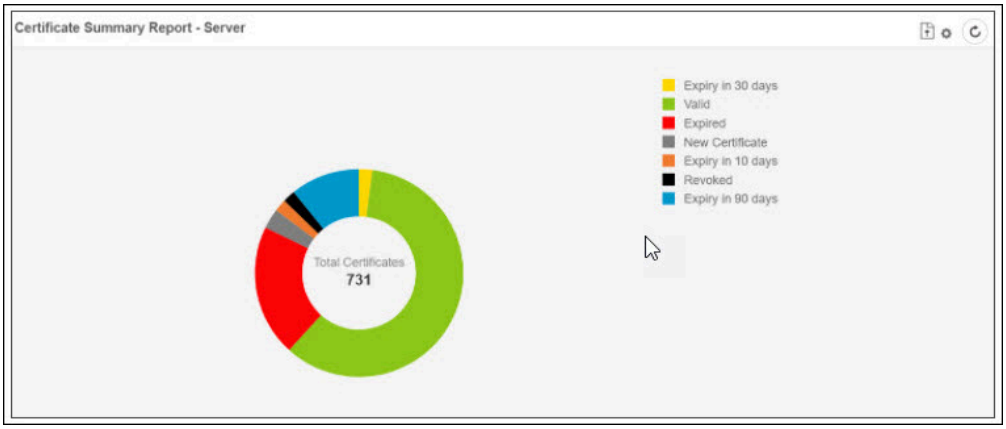
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- **Check**
  - The cron job is executed to check the Certificate transparency for all certificates in the inventory.
  - The internal business logic uses the Google CT project (Open source) to identify the violation
  - Once the job is completed, the CT and CAA reports are updated in the server_certificate_security dashboard.
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Sunday.
- **Audit** - The internal business logic to check the CT for all the certificates is captured via audit logs and notification logs in the logging module.

Certificate Validation Check

This is a periodical running job to validate the chain of trust information for all the certificates in the inventory. Based on this validation, the certificate validation report will be updated with the latest data in the server certificate dashboard.



- **Check**
  - The cron job is executed to check the validation for all certificates in the inventory.
  - Once the job is completed, the certificate summary report is updated in the Server Certificate and Client Certificate Dashboard.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Monday.
- **Audit** - The internal business logic to check the CT for all the certificates is captured through audit logs and notification logs in the logging module.

Configuring Report Settings and Schedule

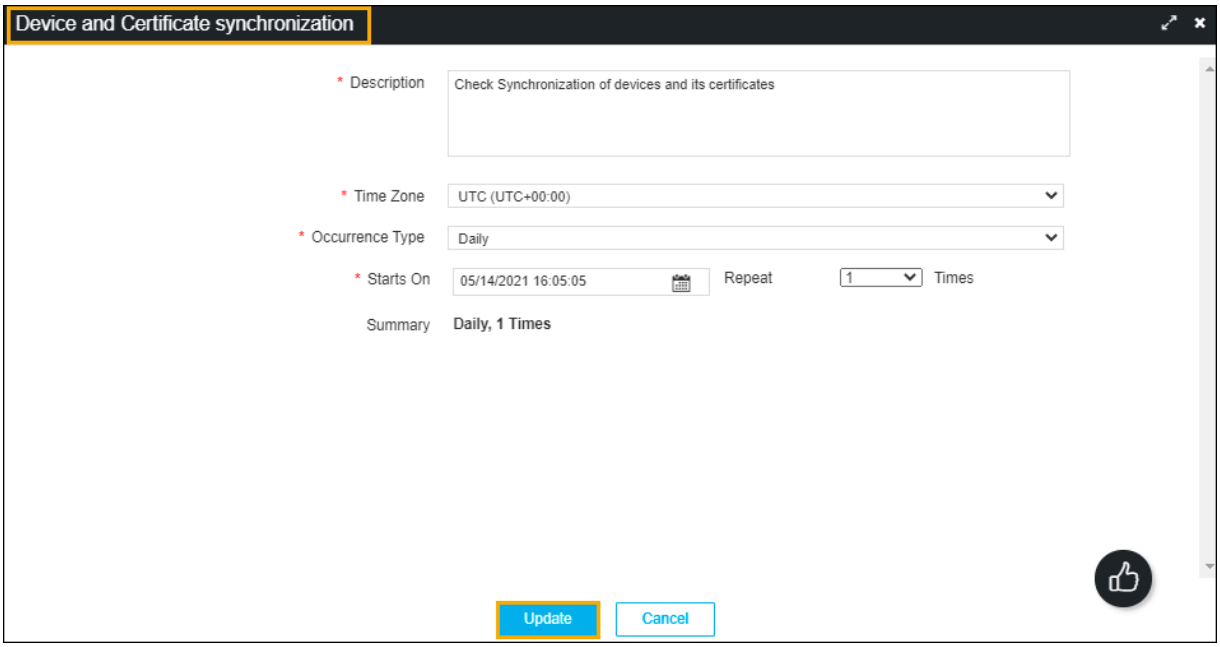
The running time of the reports to collect the data can be configured per the organization level using the Job Scheduler. To configure the Job Scheduler,

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Job Scheduler.**
   The **Job Scheduler** home page is displayed.



2. Click on the desired task name in the list to modify the configuration of the job running time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The following table describes the options available on the task page:

Task Page - Field Description Table

Fields	Description
* **Description**	Enter the task description in this field. **Note:** You can enter a maximum of 2000 words in the field.
* **Time Zone**	Allows setting the correct time according to your region. **Note:** By default, the dropdown list shows time in UTC.
* **Occurrence Type**	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
* **Start On**	Set the start date and time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Repeat	The number of times the job schedulers to be completed. **Note:** You can repeat this activity maximum of six times.
Summary	Displays the occurrence type and frequency of the job scheduler.

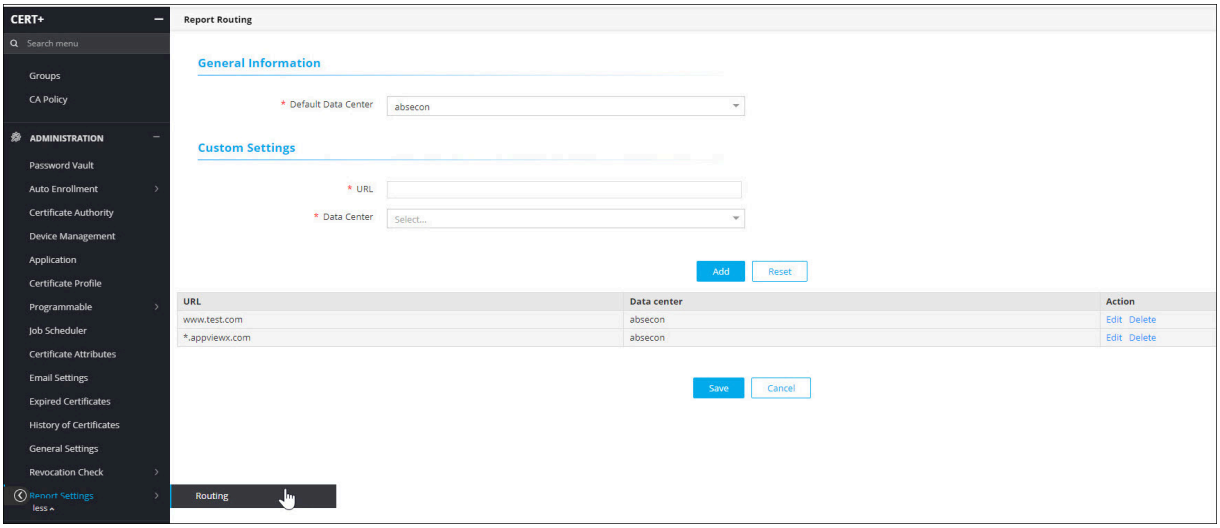
3. After configuring the details, click **Update**.
   The job scheduler details are saved.

Report Routing

This functionality is applicable only to the following reports:

- Validation report
- Vulnerability report
- CAA report

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Report Settings** > **Routing** or **Code Signing**.
   The **Report Routing** page is displayed.



2. Enter the following fields:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Revocation Routing Page - Fields Description

Fields	Description
General Information	
Default Data Center	This is the default data center through which all validation requests are routed.
Custom Settings	
URL	Type the URL of the certificate for which you want to perform the revocation check.
Data Center	Select the data center of the URL from the dropdown list. Selecting this value will overwrite the default data center.
Note: The asterisk (*) symbol indicates a mandatory field.	

3. Click **Add.**
   The table is refreshed with a row entry of the newly added URL and the data center.
4. Click **Save.**
   - A message that certificate report settings routing is saved successfully is displayed.
   - On saving, any report validation such as validation checks or CAA record check is routed through the data center configured on this page.

> **Note:** To perform a bulk operation on certificate URLs, you can specify a wild card character with their domain name, for example, if you want to specify a data center to all the AppViewX certificates at one go, then use wild card character as in *.appviewx.com and select the data center from the dropdown list.

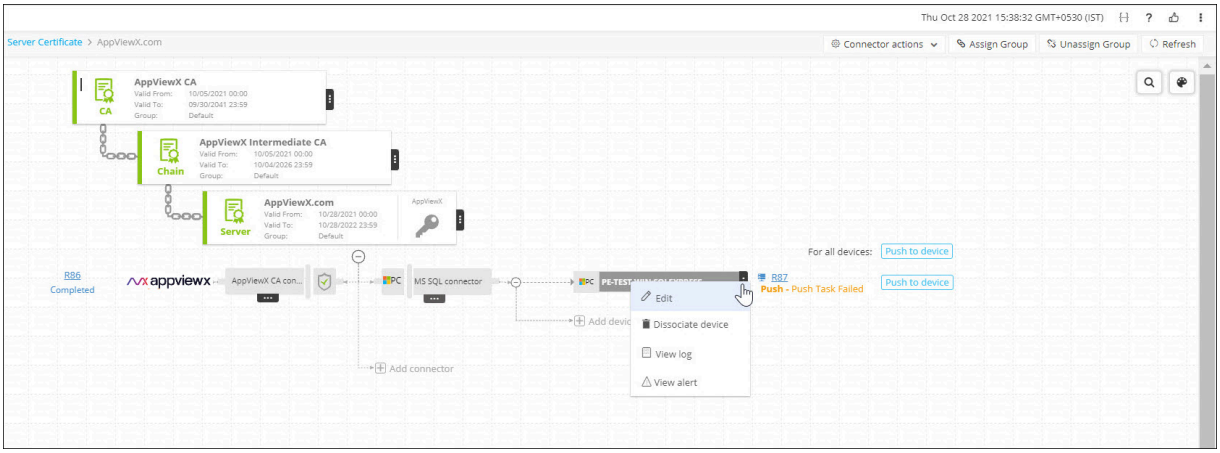
5. Click **Add**.
6. To edit the certificates, then use the **Edit** option.

Validation Settings

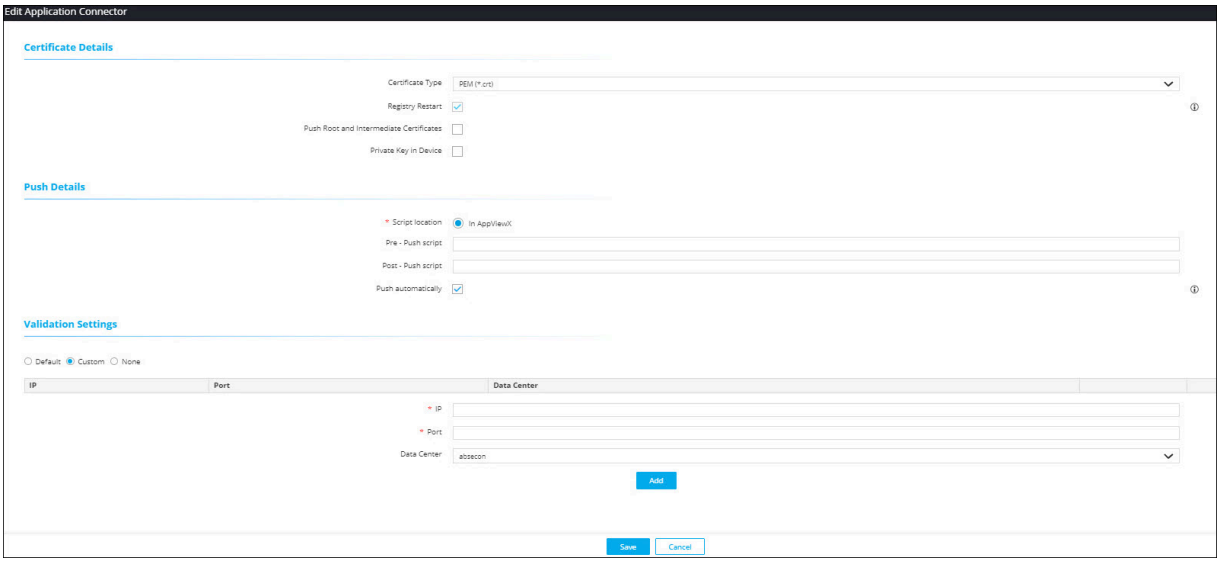
This is an extended feature of Report Routing.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server** or **Client** or **Code Signing**.
2. Click the **Common Name** link to view the certificate in the holistic view.
3. Hover the mouse over the (**More**) icon of the application connector and click **Edit.**



The **Edit Application Connector** page is displayed.



4. Select **Custom** option.
5. In the **Validation Settings** section, select the data center from the dropdown list.

   This ensures that for any validation check, this is treated as high priority.

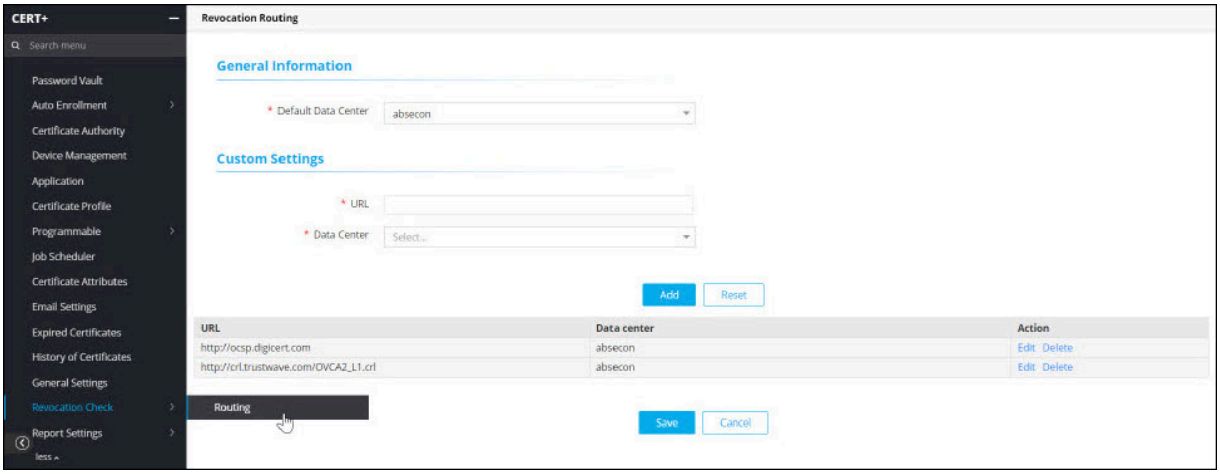
Revocation Check Routing

This functionality is applicable to:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Revocation check job
- On demand revocation check

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Revocation Check** > **Routing** .
   The **Revocation Routing** page is displayed.



2. Enter the following fields:

Revocation Routing Page - Fields Description

Fields	Description
General Information	
***Default Data Center**	This is the default data center through which all validation requests are routed.
Custom Settings	
***URL**	Specify the URL for which you want to run the revocation check job or the on-demand revocation check by selecting the certificate from the holistic view. To run the revocation check job, copy and paste the URL from the **CRL distribution points** field of the **Certificate details** window. To run the on demand revocation check, copy and paste the URL with ocsp extension from the **Authority information access** field of the **Certificate details** window. **Note:** For on demand revocation checks, if you have configured two URLs with .crl and .ocsp extensions and for any reason the job fails

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	on .ocsp, then the revocation check is triggered on the URL with .crl extension. If the job is successful and the certificate is revoked, then the certificate is displayed on the **Certificate Inventory** page with a black icon against it. If the job failed, then go to **Administration > Logging > Certificate** and check the log message.
***Data Center**	Select the data center of the URL from the dropdown list. Selecting this value will overwrite the default data center.
Note: The asterisk (*) symbol indicates a mandatory field.	

3. Click **Add**.
   The table is refreshed with the added URL and the data center.
4. Click **Save**.
   - A message that certificate revocation check routing is saved successfully is displayed.
   - The table is refreshed with a row entry of the newly added URL and the data center.

Securing CERT+

CERT+ Certificate Lifecycle Management (CLM) offers capabilities to discover and manage certificates on devices and self-service certificate enrollment for users. CERT+ also acts as a Key Escrow for keys discovered and enrolled.

Typically, the private keys are stored by the devices handling SSL termination, and an SSL management tool retrieves them during certificate renewal. The tools and devices store them in their storage in the original format, which can be reused. If there is an attack on the device or tool storage, the private keys will be given away, which can be used to host an array of attacks.

AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using the AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Thus, even if the hackers get the database, they will not be able to get the private keys. Only a maze of jumbled up characters will be visible to them, which does not make any sense and hence, rendering the attack useless.

Auto Enrollment Protocols

Auto-enrollment protocols are standardized enrollment mechanisms accepted across a wide range of enterprise systems for device and application certificate enrollment. Systems leveraging Auto-enrollment protocols typically expect minimum to no admin intervention. Network devices such as routers-switches, DevOps tools, and Enterprise Mobility Management platforms are typical examples of such systems.

- ACME
- EST
- Microsoft Intune
- SCEP
- CMP
- EST Client Authentication in Cloud Connectors
- Direct Requests

ACME

ACME is **Automated Certificate Management Environment**, which is a certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire certificates and associated CA certificates. Architecturally, the ACME service (agent) is located between a CA and a client.

- There should be a plugin/pod (avx_vendor_cert_acme_agent) up and running for ACME in AppViewX.
- This ACME plugin works in the HPPTS gateway (The default gateway is used in Appviewx with port 31443)
- It is highly recommended to turn OFF the **Approval Required** flag in **Menu > Inventory > Certificate > Policy** page.
- A valid agent settings should be available in **Menu > Inventory > Certificate > Settings**.
- Configuring ACME
- Validating ACME

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring ACME

In order to carry out client certificate enrollments using the ACME protocol, the administrator or a privileged user must initially configure the ACME server agent using the AppViewX portal. Once the ACME server agent is successfully set up through the portal, a URL will be generated. Clients can then utilize this URL to submit enrollment requests to AppViewX via the ACME protocol.

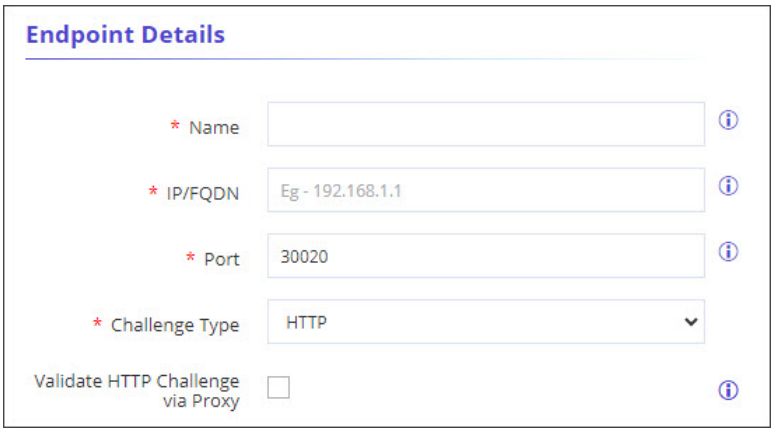
To set up the ACME server agent,

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **ACME**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The **Auto Enrollment : ACME** page displayed with tabs for **General Setting** and **EAB Setting**
3. Select the **General Setting** and configure the **Endpoint Details** as follows:

   Prerequisites for entering the IP/FQDN field:

   - The "Cloud Connector Name" (in the Add Cloud connector page) must be the same as the FQDN name entered.
   - The CC should have the reachability to the Endpoint.
   - If entering the IP the ensure that single cloud connector is used.

   The fields for Endpoint Details are as follows:



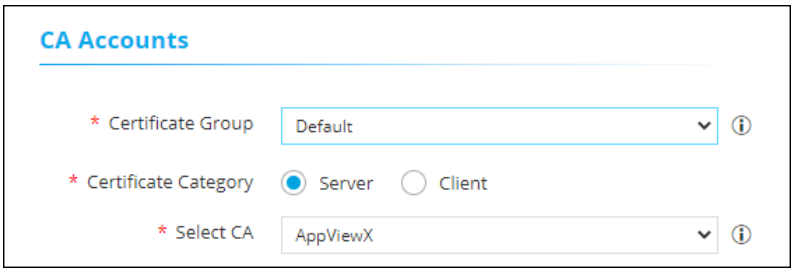
Endpoint Details - Field Description Table

Fields	Description
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable Characters: A-Z, a-z, 0-9, '.', '_', '-'

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***IP/FQDN**	In the On-Prem setup, enter the FQDN/IP address of the AppViewX cloud connector. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***Port**	HTTP gateway port of the AppViewX node. Port will accept only numerical values between 0 to 65535. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only port 443.
***Challenge Type**	Select the one of the following challenge type: • DNS • HTTP
Validate HTTP Challenge via Proxy	This field is enabled when Challenge Type = HTTP. If **enabled** the communication with the ACME client to fetch the http challenge token is via the proxy details provided in the General Settings
**: Mandatory fields*	

4. Configure the **CA Accounts** details as follows:



The fields for CA Accounts section are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

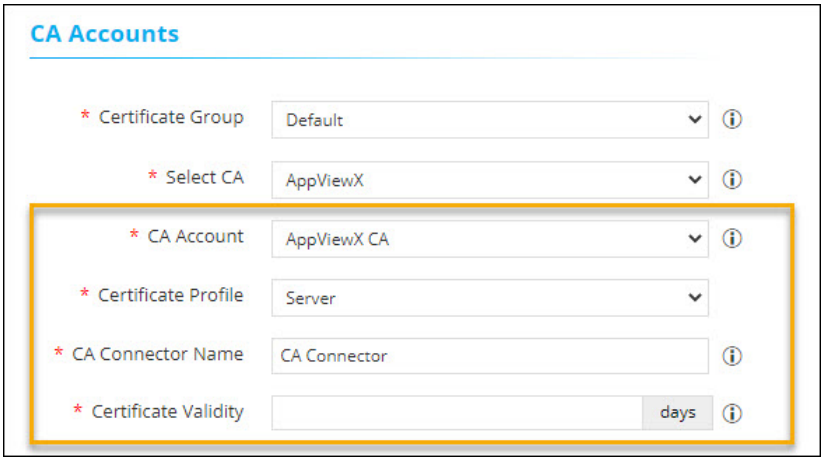
CA Accounts - Field Description Table

Fields	Description
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Certificate Category**	Select a specific certificate type (Server / Client) to be enrolled.
***Select CA**	Select the required CA from the available options: • AppViewX • AppViewX PKIaaS • Amazon Private CA • Comodo Certificate Manager • DigiCert • DigiCert MPKI • Ejbca • Entrust • Entrust MPKI • Globalsign • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Lets Encrypt • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust The certificate will be enrolled under the selected CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The **Vendor Specific Details** section is displayed after the **CA Accounts** section only for the following selected CA • DigiCert • EJBCA • Entrust • Entrust MPKI • MS Enterprise • Nexus
**: Mandatory fields*	

When **AppViewX** is selected as CA,



The fields for AppViewX CA are as follows:

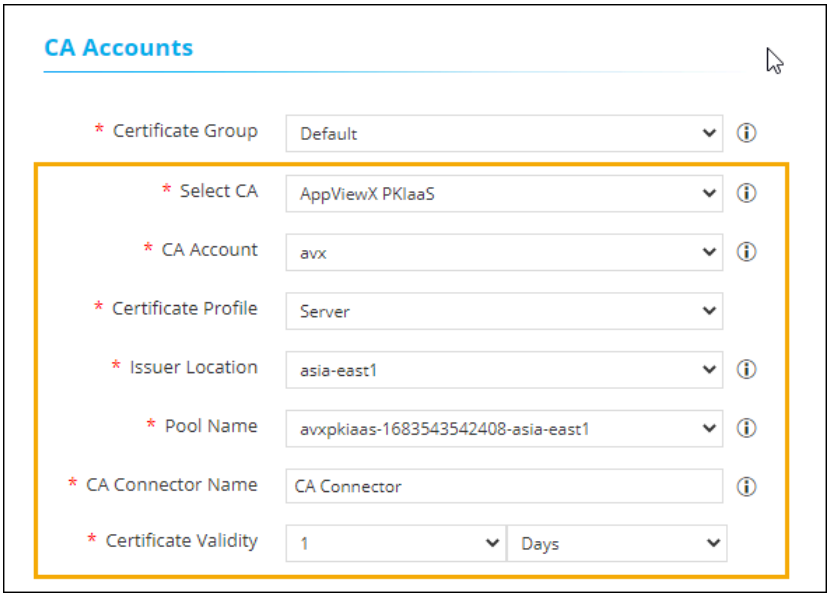
Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **AppViewX PKIaaS** is selected as CA,



The fields for AppViewX PKIaaS CA are as follows:

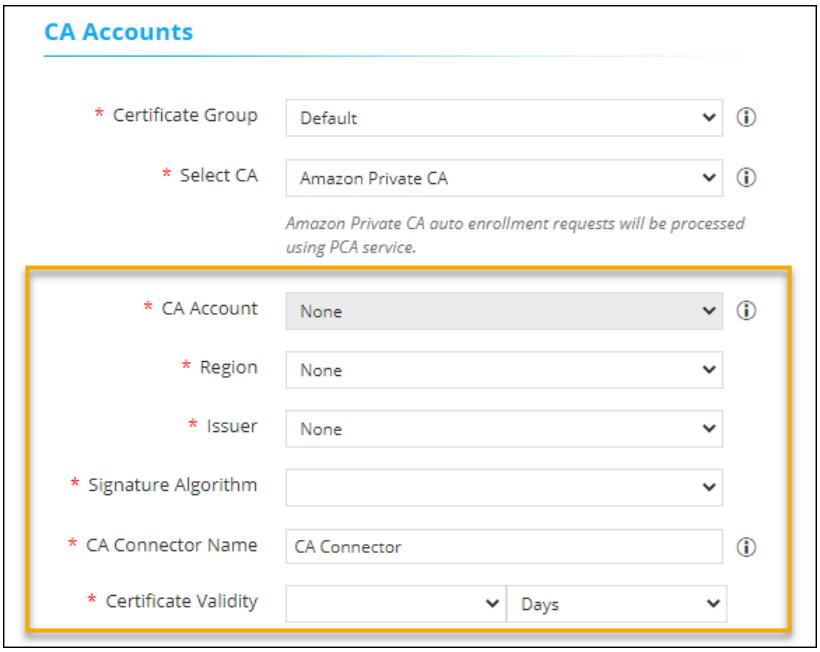
Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Amazon Private CA** is selected as CA,



The fields for Amazon Private CA are as follows:

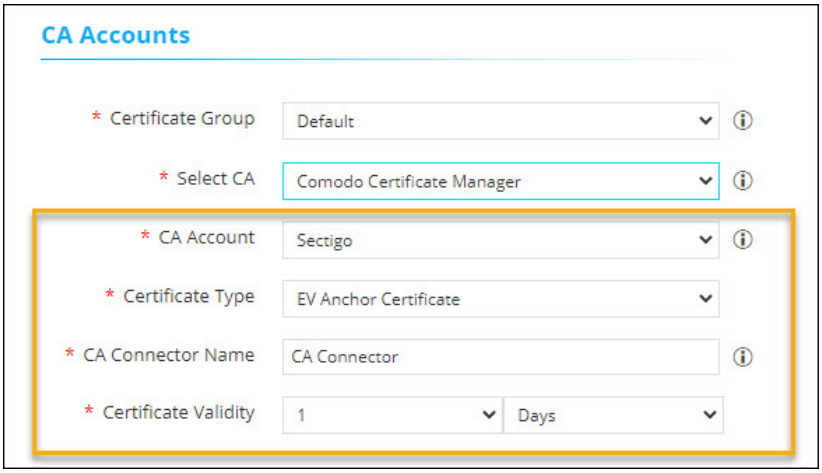
Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Region**	Select a region from the dropdown list.
***Issuer**	Select the issuer from the dropdown list.
***Signature Algorithm**	Select the Signature Algothirm from the dropdown list. The available options are: • SHA256WITHECDSA • SHA384WITHECDSA • SHA512WITHECDSA • SHA256WITHRSA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• SHA384WITHRSA • SHA512WITHRSA
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Comodo Certificate Manager** is selected as CA,



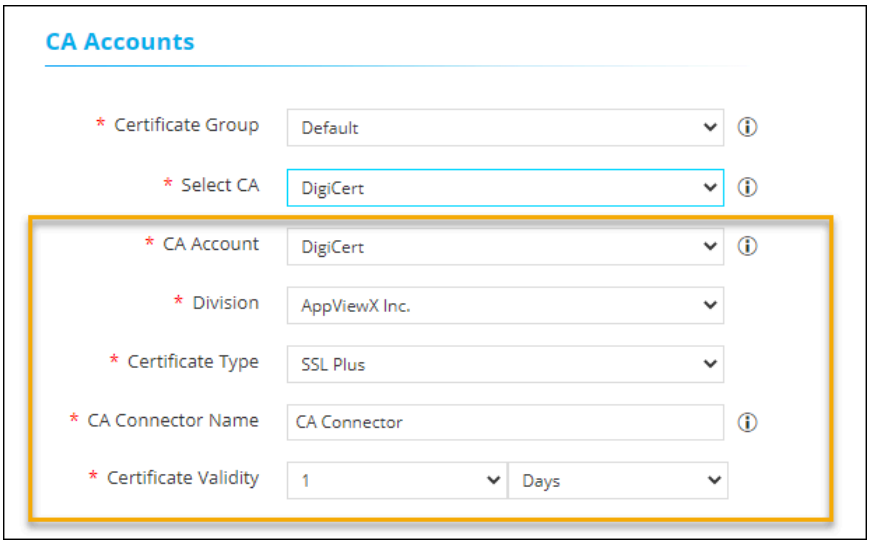
The fields for Comodo Certificate Manager CA are as follows:

Details for Comodo Certificate Manager CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Cert Type**	Select certificate type to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **DigiCert** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

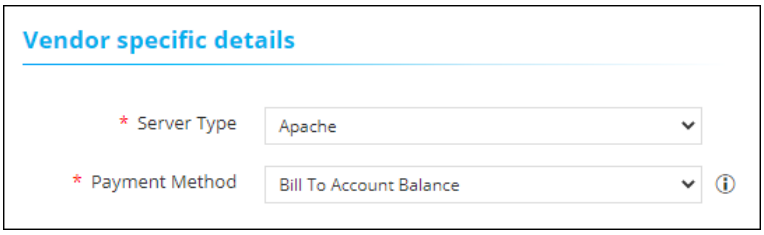


The fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Division**	Select the division associated with the CA account.
***Cert Type**	Select certificate type to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.



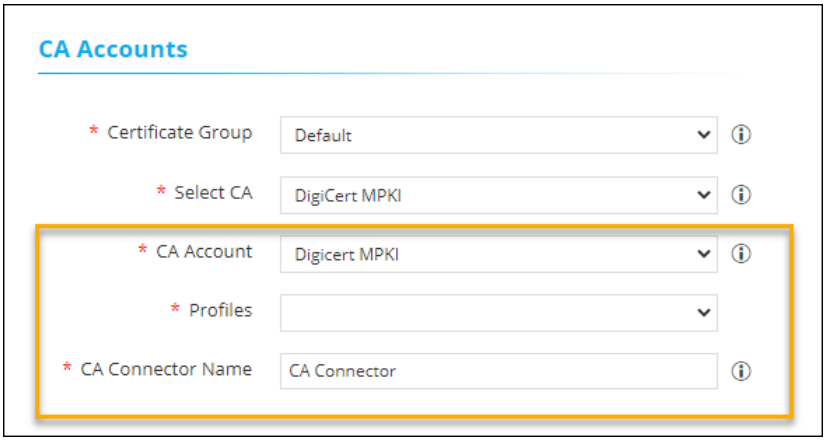
The fields for Vendor specific details are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
**: Mandatory fields*	

When **DigiCert MPKI** is selected as CA.



The fields for DigiCert MPKI CA are as follows:

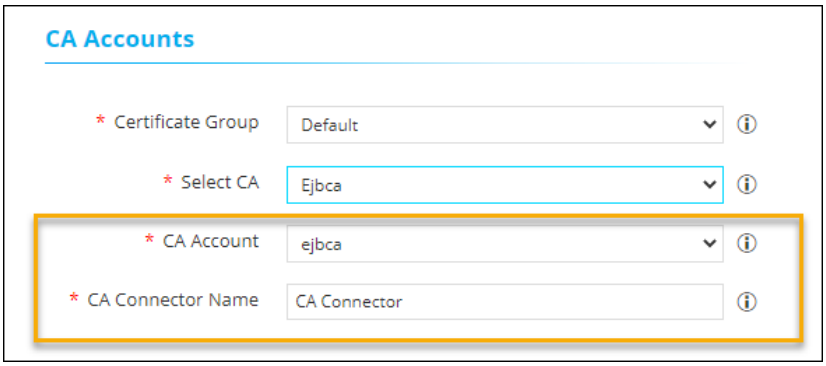
Details for DigiCert MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Profiles**	Select a profile associated with the CA account.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Based on the DigiCert MPKI account configuration Custom Attributes section may also be displayed on the endpoint configuration page.

When **EJBCA** is selected as CA,

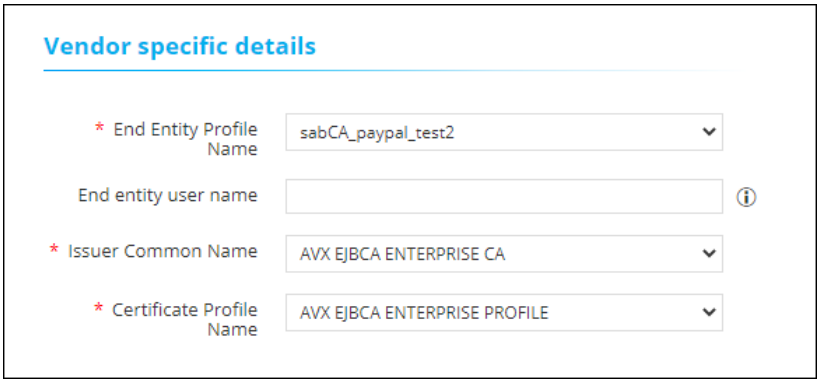


The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section.



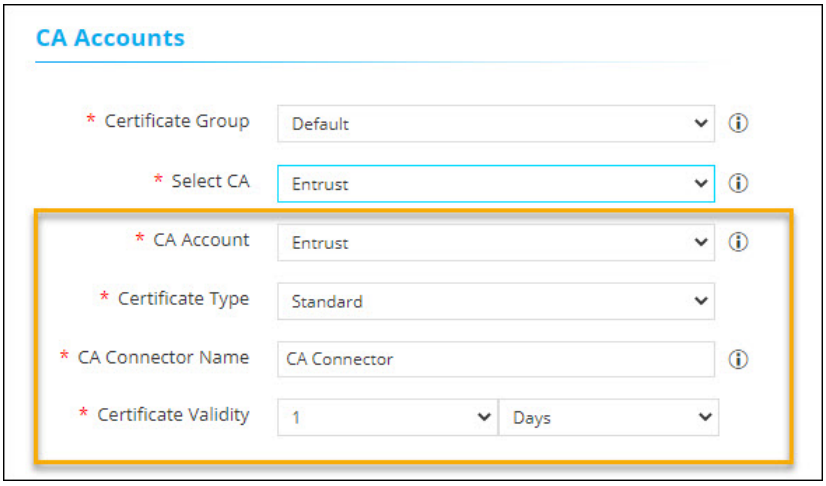
The fields for Vendor specific details are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
**: Mandatory fields*	

When **Entrust** is selected as CA,



The fields for Entrust CA are as follows:

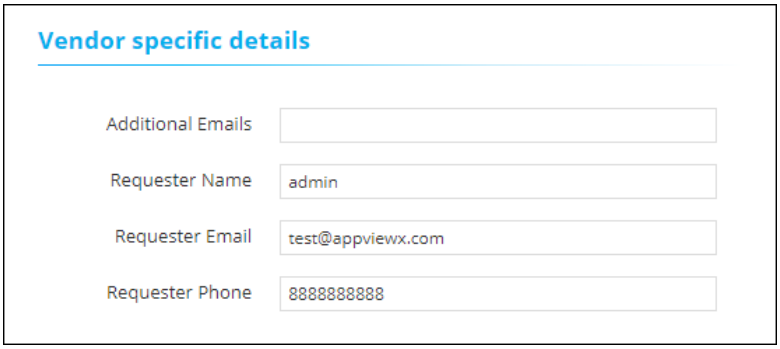
Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select a valid cert type associated with the CA account. If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

If the selected CA is Entrust, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section.



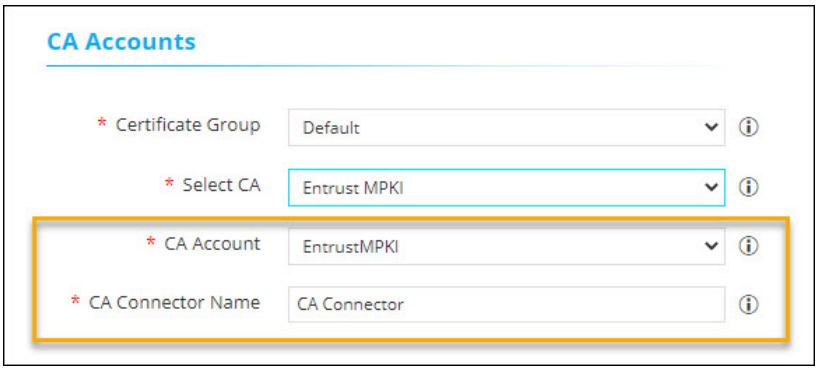
Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the demo details
Requester Email	Enter a valid eamil id
Requester Phone	Enter the 10-digit phone number.
**: Mandatory fields*	

When **Entrust MPKI** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

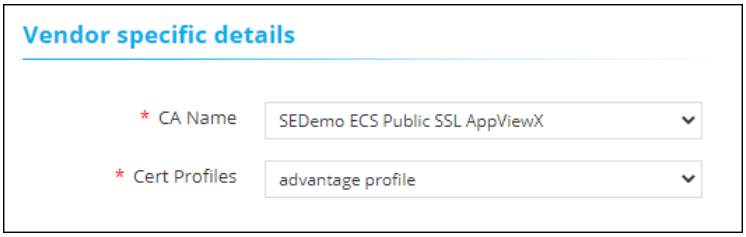


The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section.



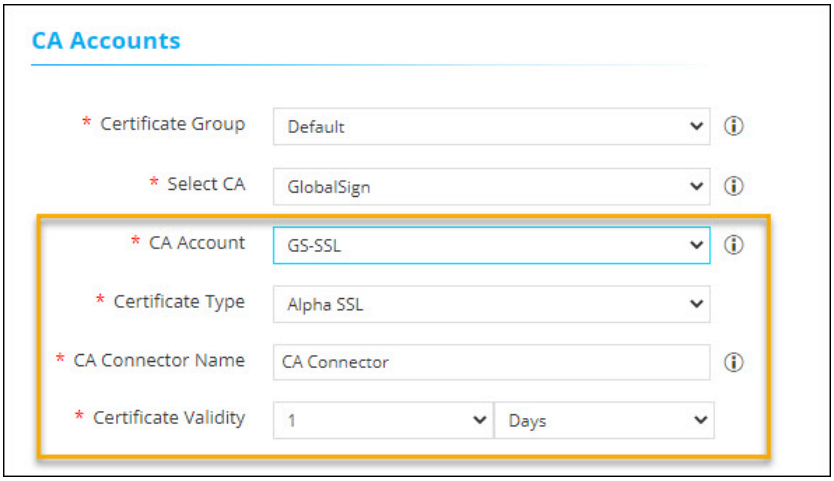
The following table provides the field description for Vendor specific details:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
**: Mandatory fields*	

When **GlobalSign** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

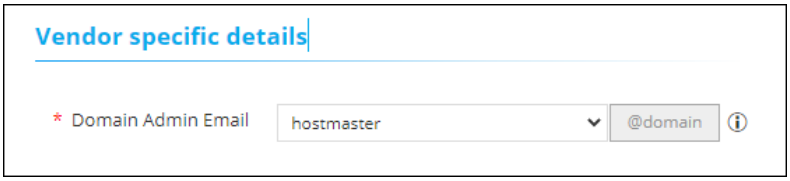


The fields for GlobalSign CA are as follows:

Details for GlobalSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Alpha SSL or Domain SSL**



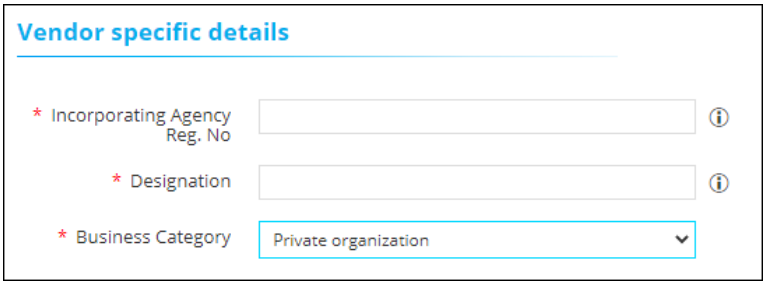
Vendor Specific Details for GlobalSign CA - Field Description Table

Fields	Description
***Domain Admin Email**	Select the email id to receive the approval requests from GlobalSign CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

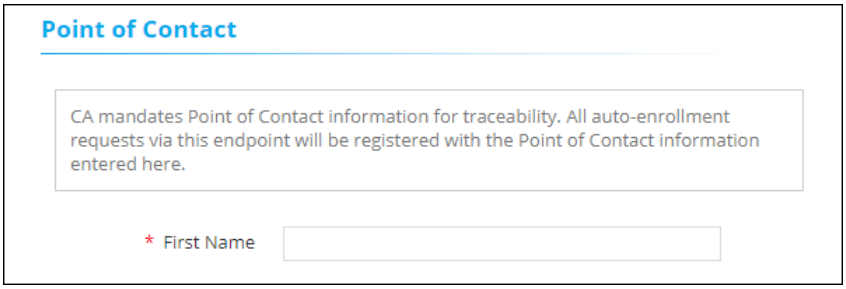
The following fields are displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Extended SSL**



Vendor Specific Details for GlobalSign CA - Field Description Table

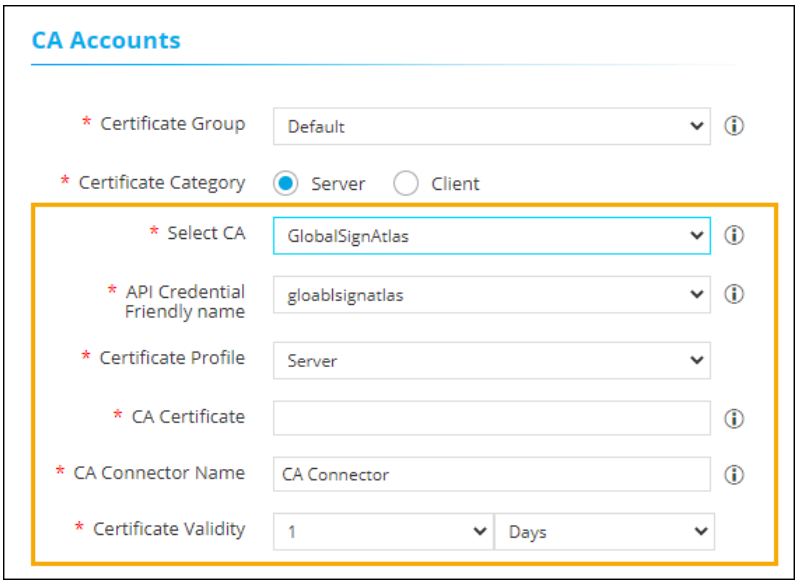
Fields	Description
***Incorporating Agency Reg. No**	Enter the Registration number of the incorporating agency.
***Designation**	Enter the designation of the requester.
***Business Category**	Select the type of business (private org., government entity, or business entity
**: Mandatory fields*	

:The following field is displayed in the **Point of Contact** section as per the selected CA if the **Select CA =GlobalSign**, and the **Certificate type = Organization SSL** . The CA mandates the point of contact information (**First Name**) for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.



When **GlobalSign Atlas** is selected as CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



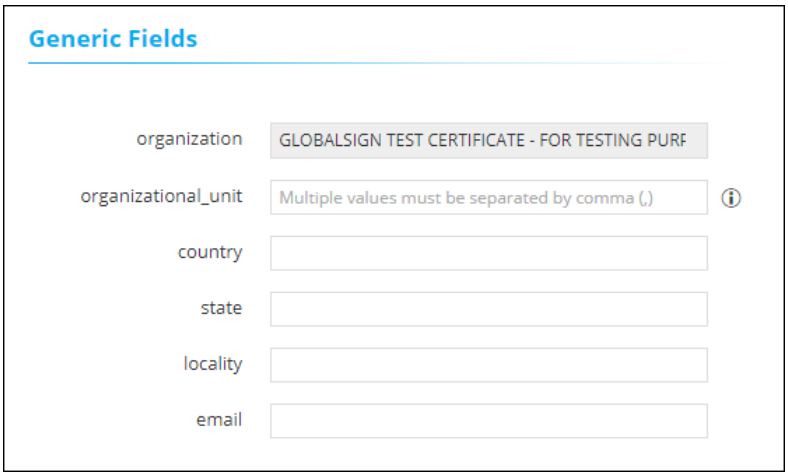
The fields for GlobalSign Atlas CA are as follows:

Details for GlobalSign Atlas CA - Field Description Table

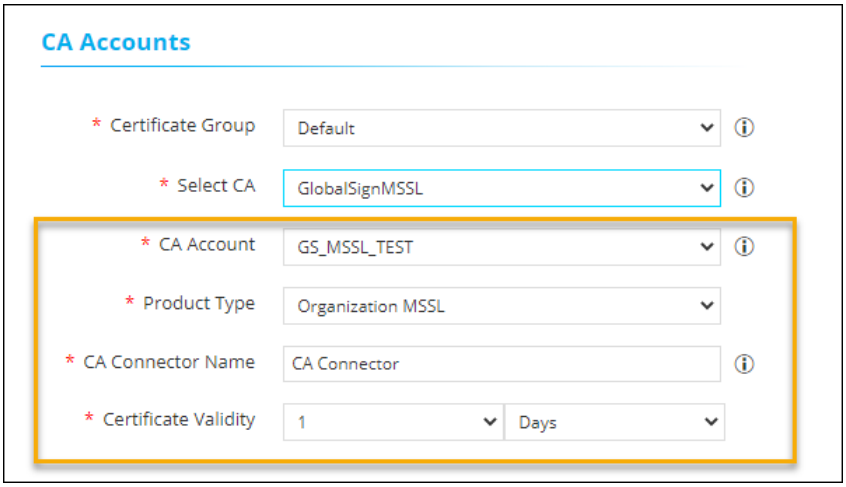
Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



When **GlobalSign MSSL** is selected as CA.



The fields for GlobalSign MSSL CA are as follows:

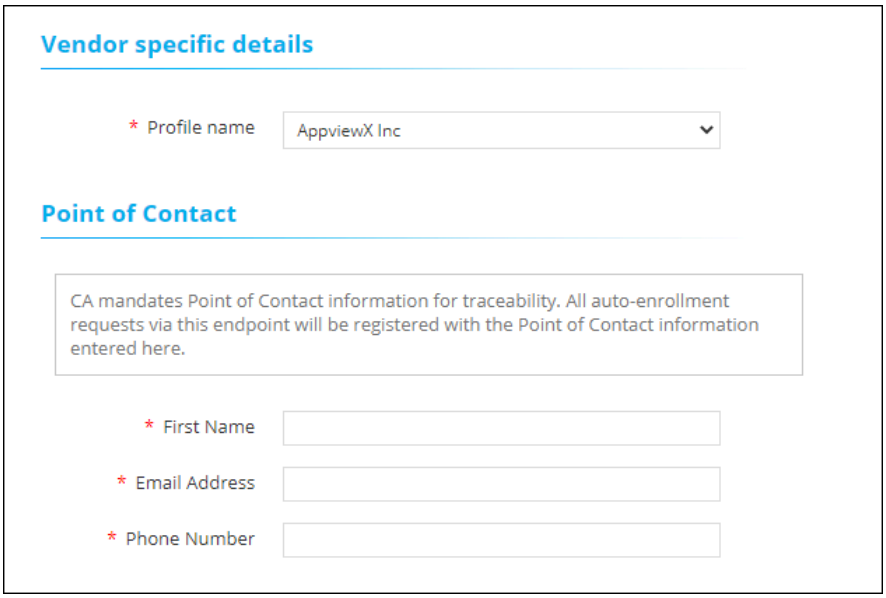
Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

The following field is displayed in the **Vendor Specific Details** and **Point of Contact** section as per the selected CA:



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
**: Mandatory fields*	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.

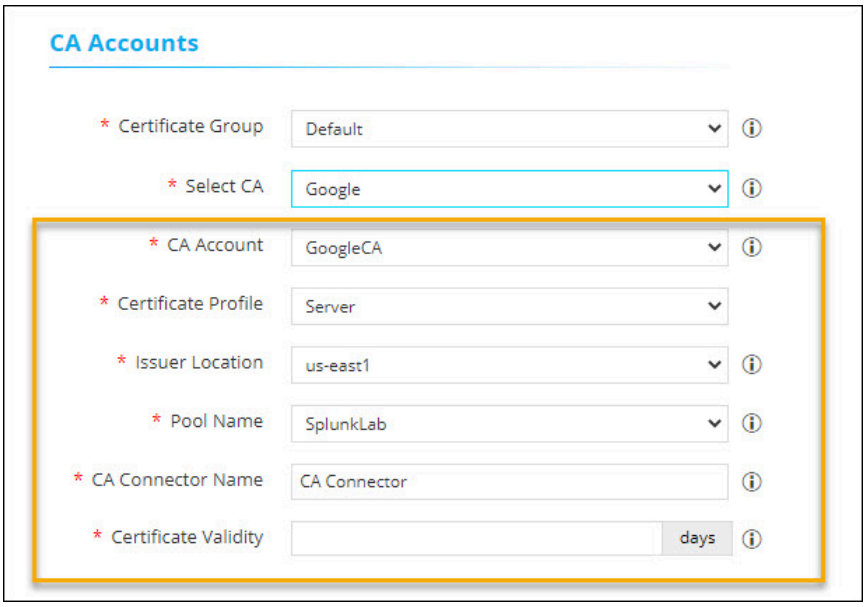
Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Phone Number**	Enter the valid phone number.
**: Mandatory fields*	

When **Google** is selected as CA,



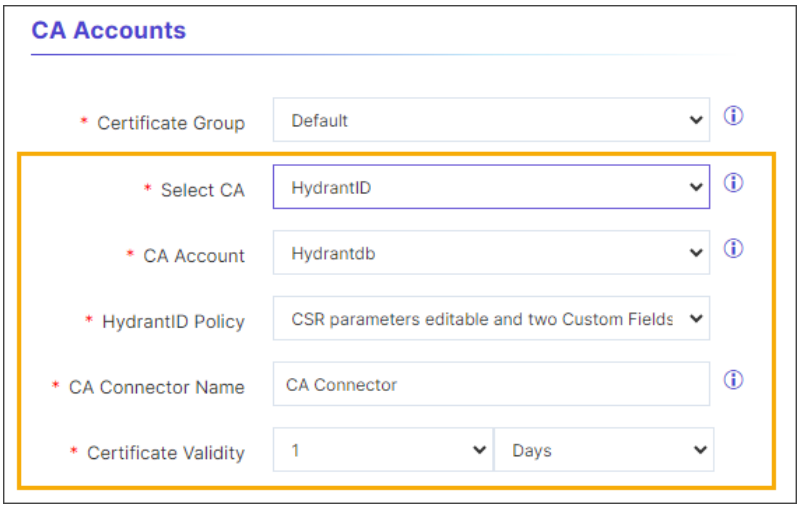
The fields for Google CA are as follows:

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Issuer Location**	Select the issuer location associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **HydrantID** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



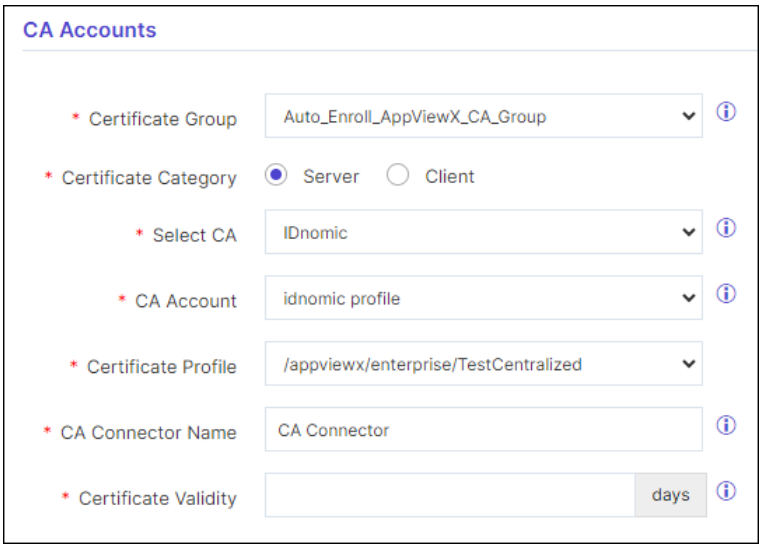
The fields for HydrantID CA are as follows:

Details for Lets HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **IDnomic** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

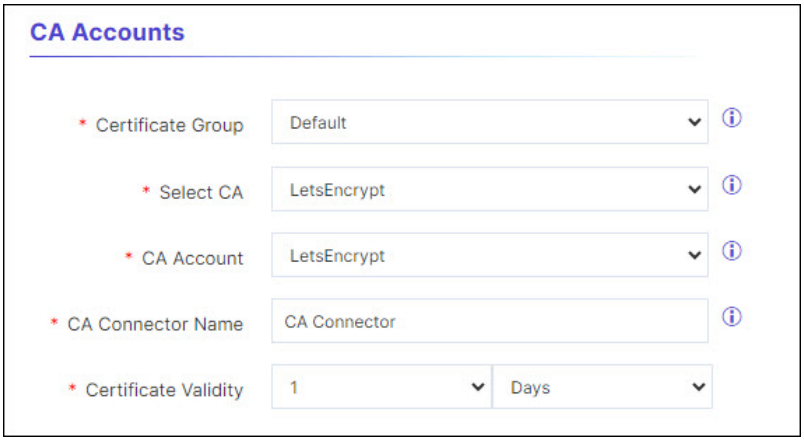


The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Lets Encrypt** is selected as CA,



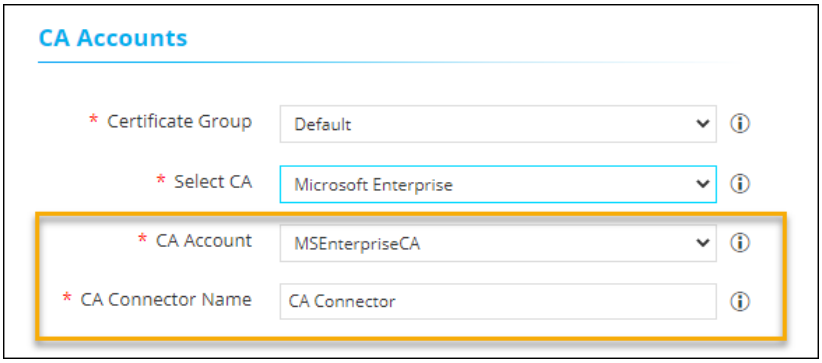
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for Lets Encrypt CA are as follows:

Details for Lets Encrypt CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Microsoft Enterprise** is selected as CA,



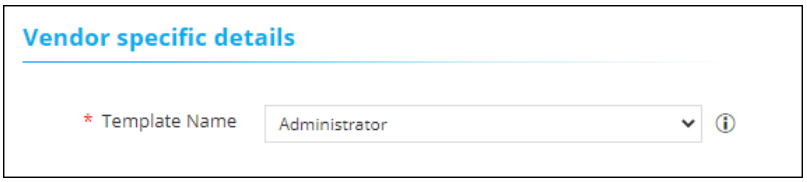
The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

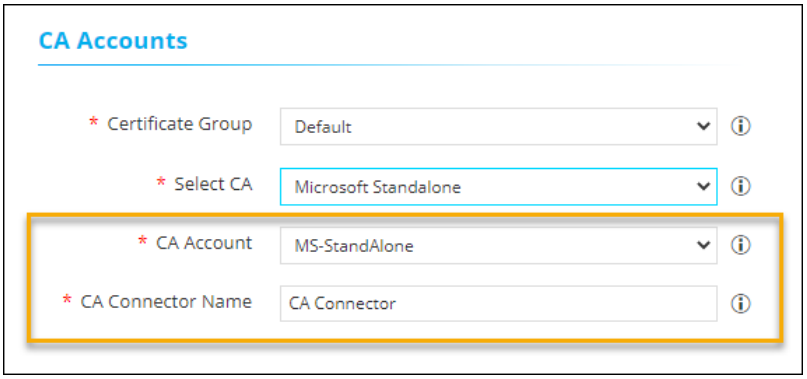
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Microsoft Enterprise, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section. Select a **Template Name** from the dropdown list. This value is based on the policy setting and its group association.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



When **Microsoft Standalone** is selected as CA,

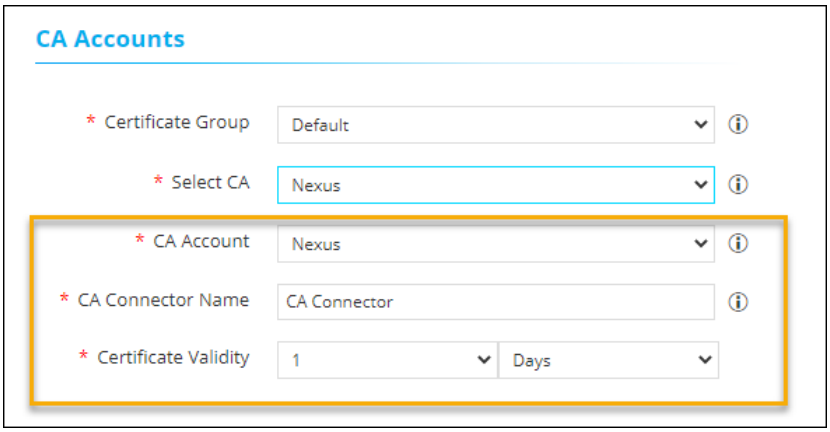


The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

When **Nexus** is selected as CA.



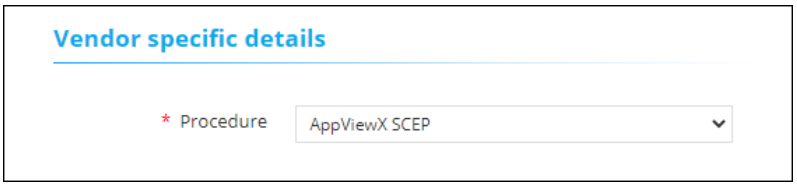
The fields for Nexus CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

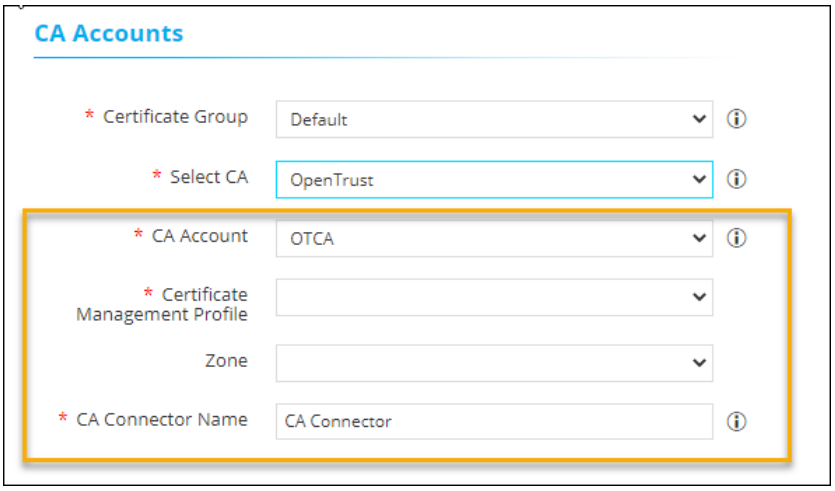
The following field is displayed in the **Vendor Specific Details** section as per the selected CA:



Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the Procedure based on the configurations made in the Certificate Authority Setting.
**: Mandatory fields*	

When **OpenTrust** is selected as CA.



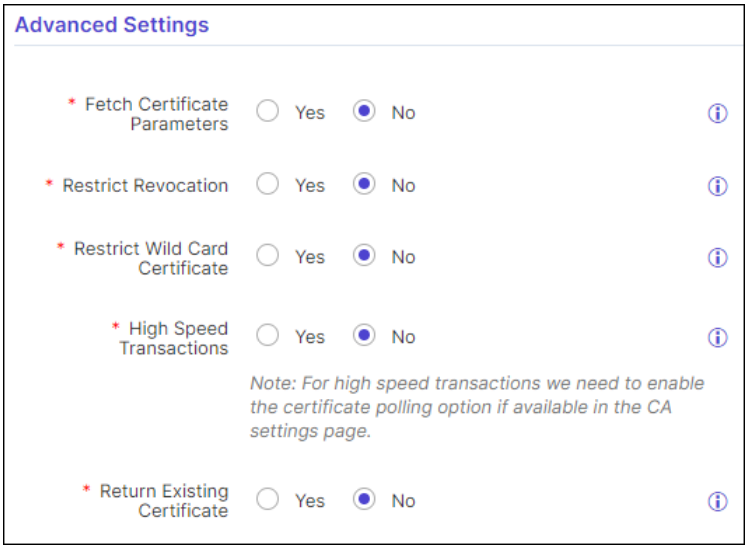
The fields for OpenTrust CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Management Profile**	Select one issuer certificate from the dropdown list. This issuer certificate will be used for signing the CSR by the certificate authority. **Note:** Only the issuer certificates available in the root or intermediate certificates inventory will be shown for selection.
Zone	Select the zone pertaining to the Certificate Management Profile
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

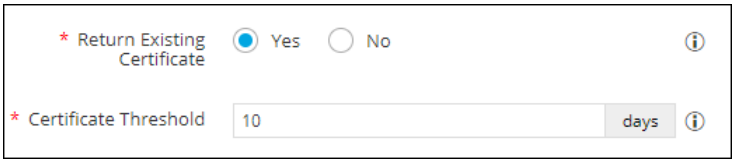
5. Configure the **Advanced Settings** details as follows:



The fields in the Advanced Settings section are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Advanced Settings - Field Description Table

Fields	Description
***Fetch Certificate Parameters**	Select Yes or No Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
***Restrict Revocation**	This option restricts the revocation of certificates through this endpoint. • If it is set to **No**, then the certificates are revoked through the ACME endpoint. • If this is set to **Yes** certificates cannot be revoked through the ACME end point.
***Restrict Wild Card Certificate**	This option restricts the issuance of wildcard certificates through this endpoint. The default value is set to “No”. • If it is set to **No**, then wildcard certificates are issued through the endpoint. There are no restrictions to certificate enrollment through the ACME endpoint. • If this is set to **Yes** then wildcard certificates are issued through the ACME endpoint. Choosing this option will not allow Common Name or DNS starting with *.
High Speed Transactions	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol’s Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed. 

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the option is disabled (**No**) then the AppViewX will do the default behavior of enrolling a new certificate for each request.
Certificate Threshold	This field is enabled only if **Return Existing Certificate = Yes.** Enter the number of days in this field. This value is used to Initiate a new certificate request if the certificate is nearing the expiry date i.e., if existing certificate validity is less than the entered value.

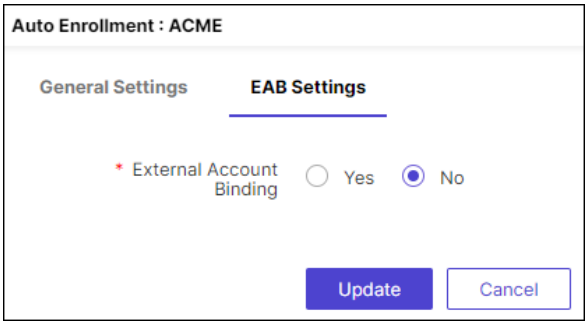
***External Account Binding**	The Certificate Authority operating the ACME server needs to provide the ACME client with a MAC Key and a Key Identifier using mechanisms outside of ACME (either through Email/SMS/ downloading or copying from the local login account). The key identifier must be an ASCII String. The MAC key will be provided in base64 URL encoded form to maximize the compatibility between non-ACME provision systems and ACME clients.
	• Select **Yes** to enable the External Account Binding (EAB). The following fields are enabled:
	  • EAB Algorithm
	  • EAB Generation Logic
	  • MAC Value
	  • Key Identifier
	• Select **No** to disable the EAB

EAB Algorithm	This dropdown list contains a list of preset algorithms that generate the MAC Value and the key identifier that are used for enrollment. The values are • HS256 • HS384 • HS512
EAB Generation Logic	This field has two options, **Generate Static** and **Generate Dynamic.** **Generate Static** - application would generate the Key Identifier and MAC Value and display the same in the respective fields. The MAC Value will be displayed with “asterisk” and Key Identifier as plain text and the option to copy the values will be provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Generate Dynamic option is grayed out. (This option will be enabled in the future product release.)
MAC Value	The MAC value as generated by the EAB Algorithm.
Key Identifier	The Key identifier value as generated by the EAB Algorithm.
**: Mandatory fields*	

6. To save the changes in the **General Setting** tab, click **Save**.
7. Select the **EAB Setting** tab and enter the details as shown below.

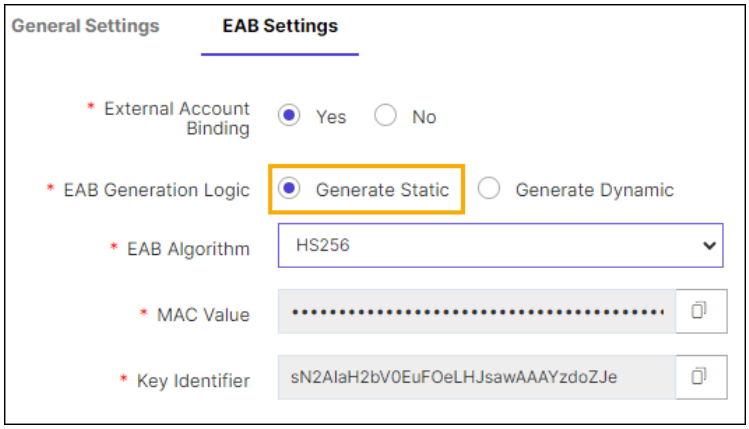


The fields in the EAB Settings tab are as follows:

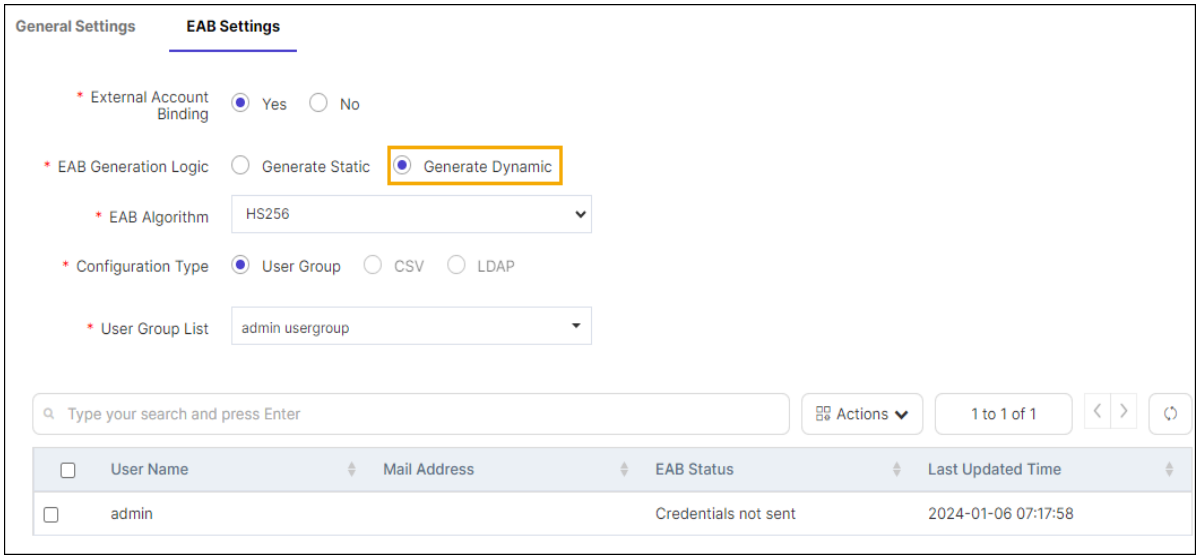
EAB Settings - Field Description Table

Fields	Description
***External Account Binding**	The Certificate Authority operating the ACME server needs to provide the ACME client with a MAC Key and a Key Identifier using mechanisms outside of ACME (either through Email/SMS/ downloading or copying from the local login account). The key identifier must be an ASCII String. The MAC key will be provided in base64 URL encoded form to maximize the compatibility between non-ACME provision systems and ACME clients. • Select **Yes** to enable the External Account Binding (EAB) or keep default **No** to keep it disabled.
***EAB Generation Logic**	This field has two options, **Generate Static** and **Generate Dynamic.** **Generate Static** - application would generate the Key Identifier and MAC Value and display the same in the respective fields. The MAC

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Value will be displayed with “asterisk” and Key Identifier as plain text and the option to copy the values will be provided. Use these values in the client. **Generate Dynamic** - based on the selected algorithm and other field values, the MAC value and Key Identifier are sent in an email to the selected user group.
When **Generate Static** is selected. 	
***EAB Algorithm**	This dropdown list contains a list of preset algorithms that generate the MAC Value and the key identifier that are used for enrollment. The values are • HS256 • HS384 • HS512
***MAC Value**	The MAC value as generated by the EAB Algorithm.
***Key Identifier**	The Key identifier value as generated by the EAB Algorithm.
When **Generate Dynamic** is selected.	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	
***EAB Algorithm**	This dropdown list contains a list of preset algorithms that generate the MAC Value and the key identifier that are used for enrollment. The values are • HS256 • HS384 • HS512
***Configuration Type**	Select the type of configuration as below: • **User Group** - enabled by default. • **CSV** - currently disabled • **LDAP Group** - currently disabled
***User Group List**	A dropdown with a list of available user groups with multi-select option. Select one or more user groups.
**: Mandatory fields*	

The **Generate Dynamic** option also displays a table with the configured values as follows:

Description for configured values of Generate Dynamic selection

Table Options	Description
User Name	Column to display the user name / user group. A checkbox is available next to the user name to perform actions described below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Table Options	Description
Mail Address	Column to display the mail address where the EAB details were sent.
EAB Status	Displays the status as follows • Activated • Deactivated • Credentials not sent
Last Updated Time	Column to display the date and time when the configuration was last updated.
Search	Type the user name/group, mail address, status etc to find or display desired values in the table.
Actions	The Actions dropdown field has the values below. Select the checkbox next to the user name and then click **Actions**. • **Activate** - Deactivated EAB credentials and ACME accounts are marked as activated. An activation email is sent to the user. • **Deactivate** - EAB details and ACME accounts are marked as deactivated. A deactivation email is sent to the user. • **Rotate** - New EAB credentials will be generated and shared to the user. The ACME accounts - Dynamic and Static, created with existing credentials are deleted. • **Resend** - Existing EAB details are resent to the users through email.
 **(Pages)**	Click the icon indicated by, for example **1 to 1 of 1** to change the number of items to display per page and use the right and left arrows to move pages.
 **(Refresh)**	Click the refresh icon to display the latest updated values.

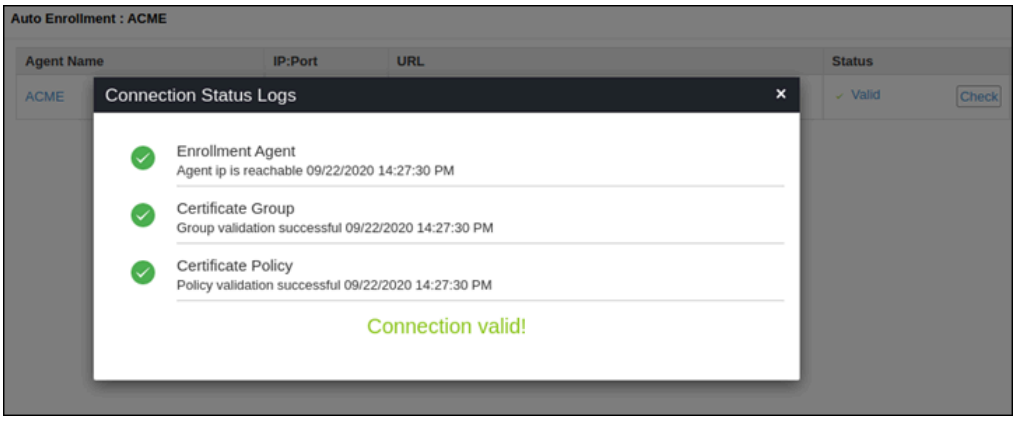
8. Click **Update**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Validating ACME

Once the ACME settings are added validation needs to be done to check whether the CA and Agent-related details are properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **ACME**.
2. On the **ACME** page, click **Check** from the Status column to validate the ACME setting that has been created.
   The ACME settings will be validated and the **Status** will be shown as either **Success** or **Failure**.



EST

EST stands for Enrollment over Secure Transport, it is a certificate management protocol targeting Public Key Infrastructure (PKI) clients which require digital certificates to prove their authenticity. EST also helps the clients in acquiring associated CA certificates. Some prerequisites and features are as follows:

- There should be an agent (avx_vendor_cert_est_agent) up and running for EST in AppViewX.
- This EST plugin can either be in HTTPS or HTTP, but it needs a gateway which supports client certificate authentication running in order to communicate with the client.
- It is highly recommended to keep the 'Approval Required' flag OFF in the **Menu -> Inventory -> Certificate -> Policy** page.
- The valid agent setting should be available in **Menu -> Inventory -> Certificate -> Settings**.

- Configuring EST
- Validating EST

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring EST

In order to carry out client certificate enrollments using the EST protocol, the administrator or a privileged user must initially configure the EST server agent using the AppViewX portal. Once the EST server agent is successfully set up through the portal, a URL will be generated. Clients can then utilize this URL to submit enrollment requests to AppViewX via the EST protocol.

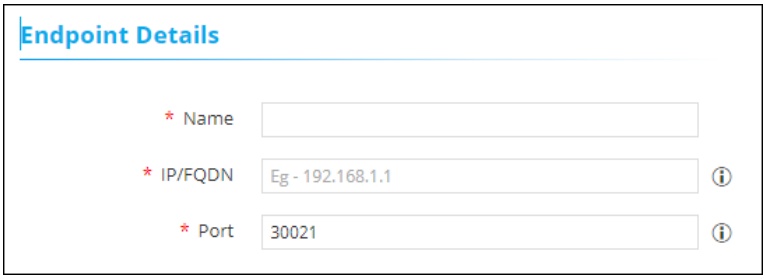
To set up the EST server agent,

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **EST**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
3. Configure the **Endpoint Details** as follows:

   Prerequisites for entering the IP/FQDN field:

   - The "Cloud Connector Name" (in the Add Cloud connector page) must be the same as the FQDN name entered.
   - The CC should have the reachability to the Endpoint.
   - If entering the IP the ensure that single cloud connector is used.

   The fields for Endpoint Details are as follows:



Endpoint Details - Field Description Table

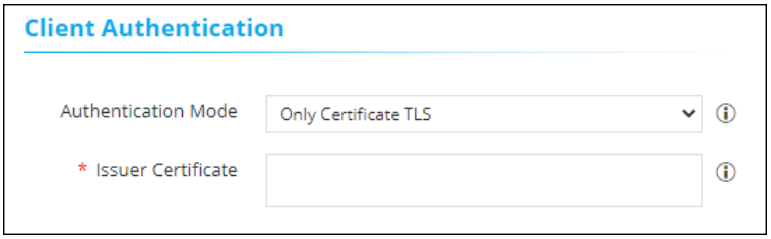
Fields	Description
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable Characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	Enter the FQDN/IP address of the AppViewX cloud connector. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, the FQDN/IP address

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

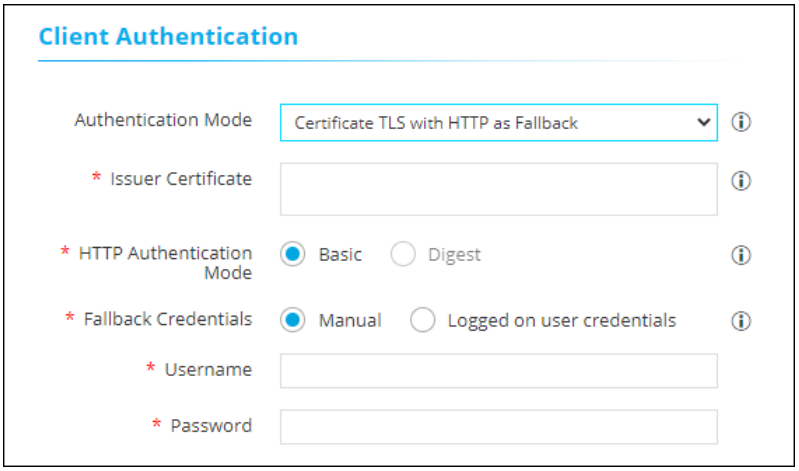
Fields	Description
	will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***Port**	The gateway port of the AppViewX node. Port will accept only numerical values between 0 to 65535. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only port 443.
**: Mandatory fields*	

4. Configure the **Client Authentication** details as follows:

Client Authentication = Only Certificate TLS



Client Authentication = Certificate TLS with HTTPs as fallback or **Both Certificate TLS and HTTPs**



The following table provides the field description for CA Authentication section:

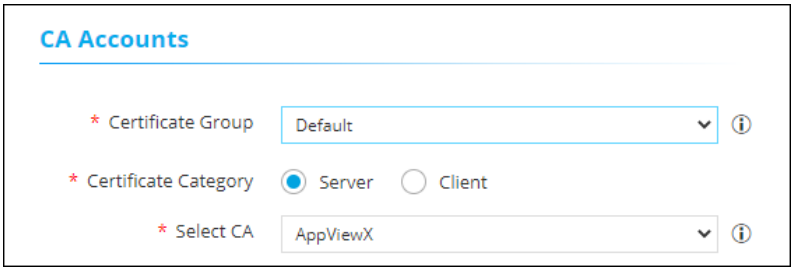
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

CA Authentication- Field Description Table

Fields	Description
Authentication Mode	Select any one authentication method to be carried out during communication with clients. • *Only Certificate TLS* - During client authentication, only certificate TLS based authentication will be performed. • *Certificate TLS with HTTPS fallback* - During client authentication, when the certificate TLS fails, HTTPs based authentication will b performed as fallback. • *Both Certificate TLS and HTTPs* - During client authentication, both certificate TLS and HTTPs authentication will be performed one after the successful completion of the other. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only *Certificate TLS with HTTPS fallback* as the Authentication mode.
***Issuer Certificate**	Select one or more issuer certificates which needs to be checked for the client certificate authentication.
***HTTP Authentication Mode**	Select the type of HTTP auth mode either Basic/Digest. • *Basic* - During Client authentication only the username and password values will be considered for HTTPs based authentication. • *Digest* - During Client authentication, along with username and password, nonce and realm values will also be supported.
***Fallback Credentials**	Select Manual/Logged on user credentials - based on the selection users can configure the credentials manually or save as credentials equivalent to the logged in user. • *Manual* - The Username and Password fields will be displayed to enter values. • *Logged on user credentials* - The Username and Password fields will not be displayed.
***Username**	Username for HTTP authentication.
***Password**	Password for HTTP authentication.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Configure the **CA Accounts** details as follows:



The fields for CA Accounts section are as follows:

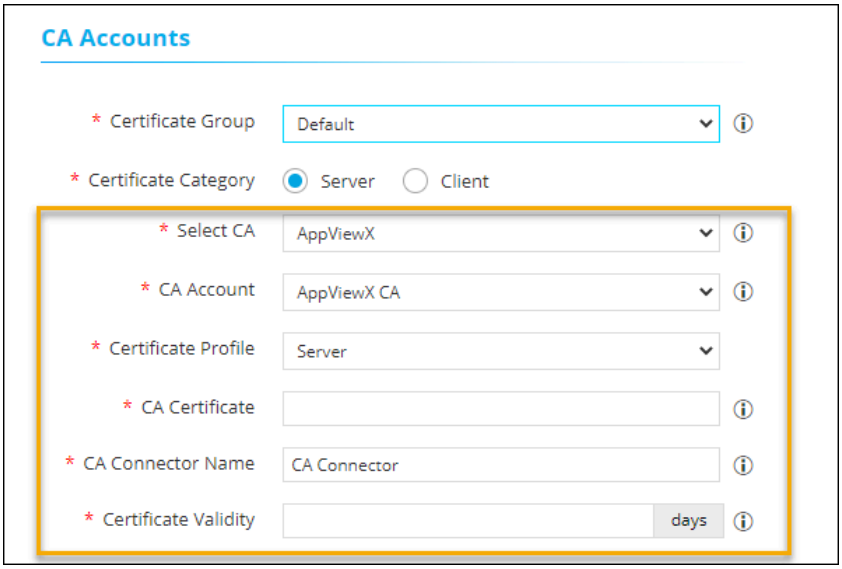
CA Accounts - Field Description Table

Fields	Description
Certificate Group	Select a specific group under which certificate needs to be enrolled.
Certificate Category	Select a specific certificate type (Server / Client) to be enrolled.
Select CA	Select the required CA from the available options. The certificate will be enrolled under the selected CA. The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • Amazon Private CA • DigiCert • DigiCert MPKI • Ejbca • Entrust • Entrust MPKI • GlobalSign Atlas • GlobalSign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs as follows: • Digicert • Ejbca • Entrust • Entrust MPKI • GlobalSign MSSL • MS Enterprise • Nexus
**: Mandatory fields*	

When **AppViewX** is selected as CA,



The fields for AppViewX CA are as follows:

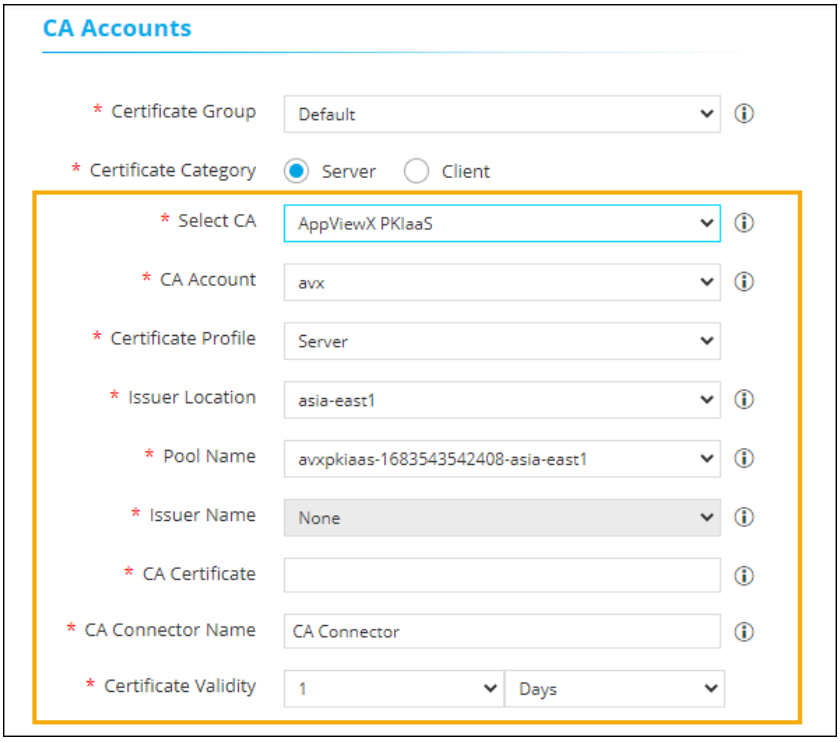
Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **AppViewX PKIaaS** is selected as CA.



The fields for AppViewX PKIaaS CA are as follows:

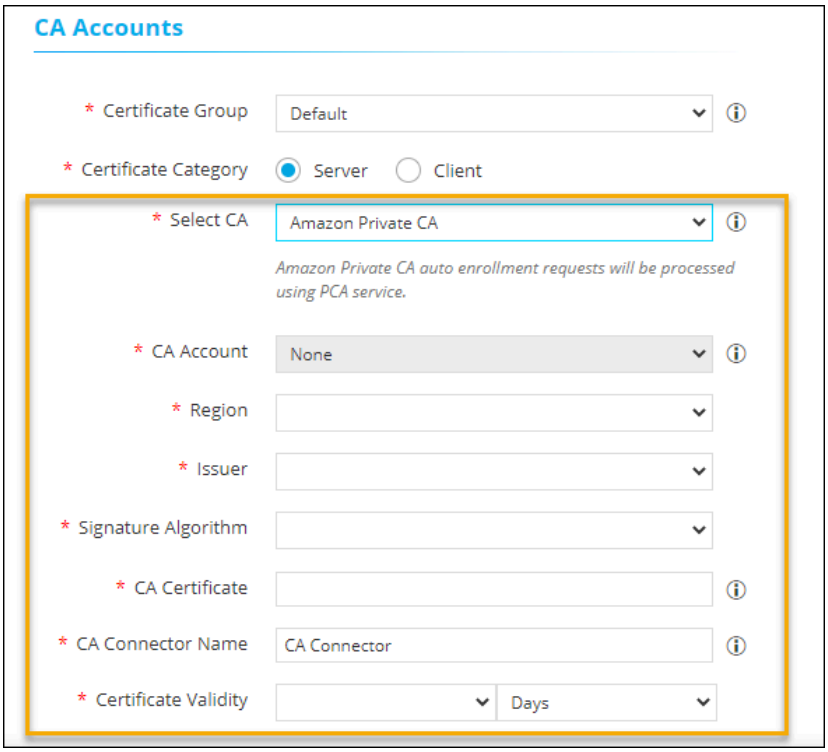
Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Amazon Private CA** is selected as CA.



The fields for Amazon Private CA are as follows:

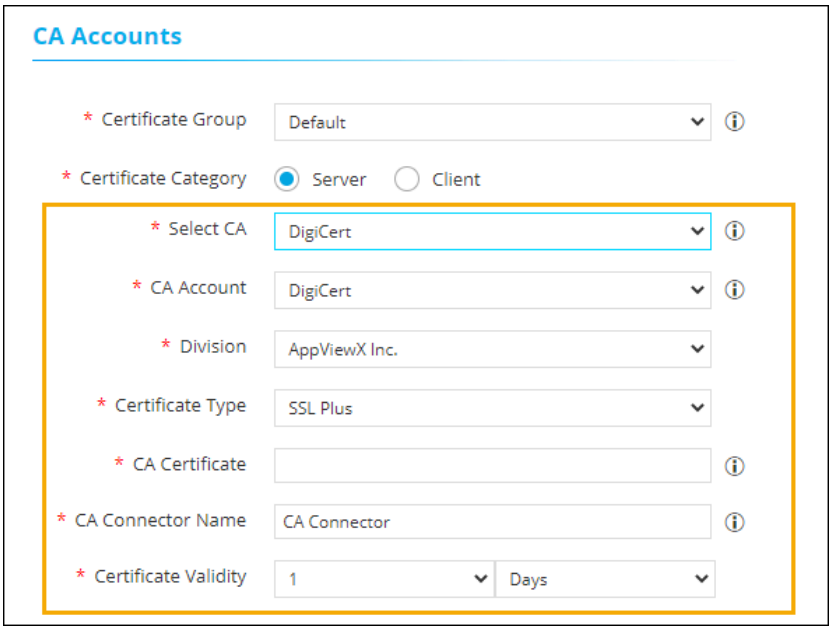
Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The dropdown list is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in years)
**: Mandatory fields*	

When **DigiCert CA** is selected as CA.



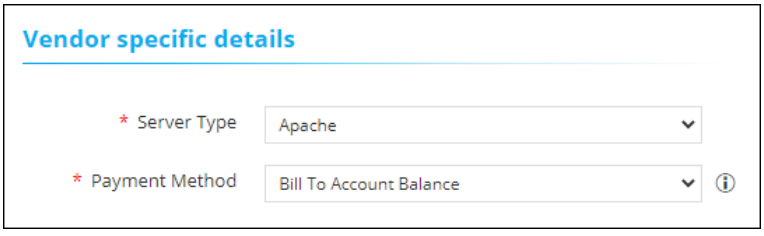
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid cert type associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.



The fields for Vendor specific details are as follows:

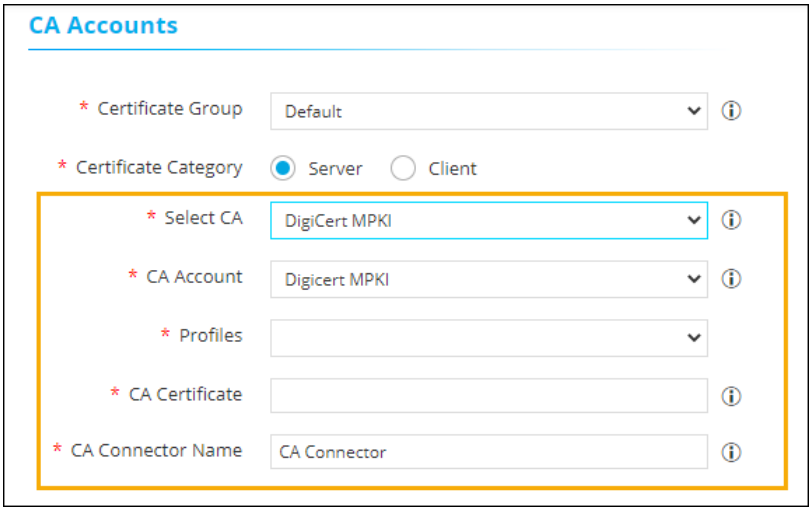
Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
**: Mandatory fields*	

When **DigiCert MPKI** is selected as CA.



The fields for DigiCert MPKI CA are as follows:

Details for DigiCert MPKI CA - Field Description Table

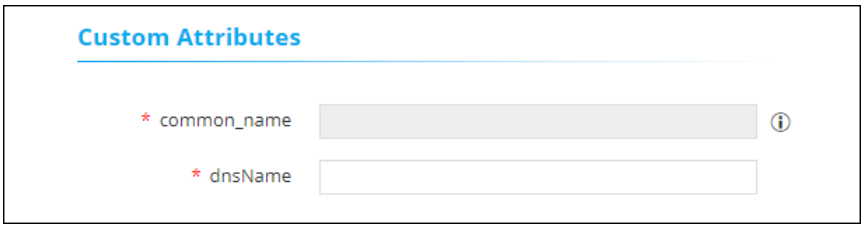
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Profiles**	Select a profile associated with the CA account.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

Note: Email address is a mandatory field on the enrollment form for DigiCert MPKI, but while passing it in the CSR, it is not added in certificate subject DN. Therefore, to successfully renew Digicert MPKI certificates using EST Fetch Certificate Parameters in EST Advanced Settings should be set to YES.

The **Custom Attributes** section is displayed on selecting the specific values from the **Profile** dropdown:



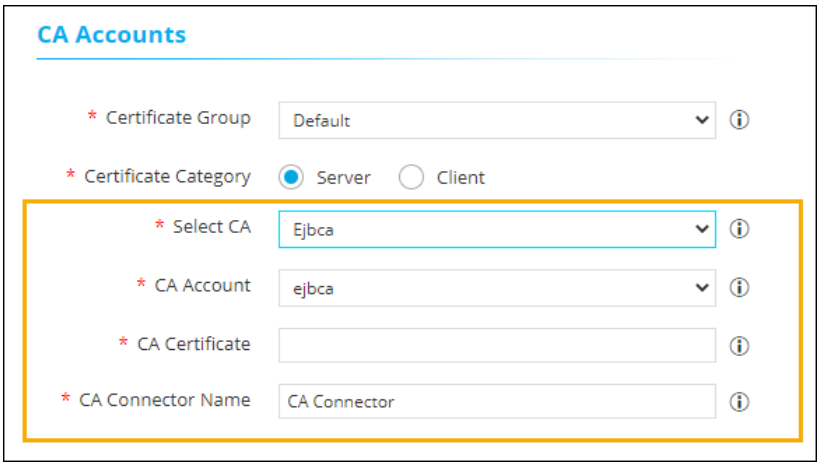
Custom Attributes for DigiCert MPKI CA - Field Description Table

Fields	Description
***common_name**	This field will be auto-populated from the CSR.
***dnsName**	Enter a valid DNS name.
*: Mandatory fields	

Note: Based on the DigiCert MPKI account configuration **Custom Attributes** section may also be displayed on the endpoint configuration page.

When **EJBCA** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

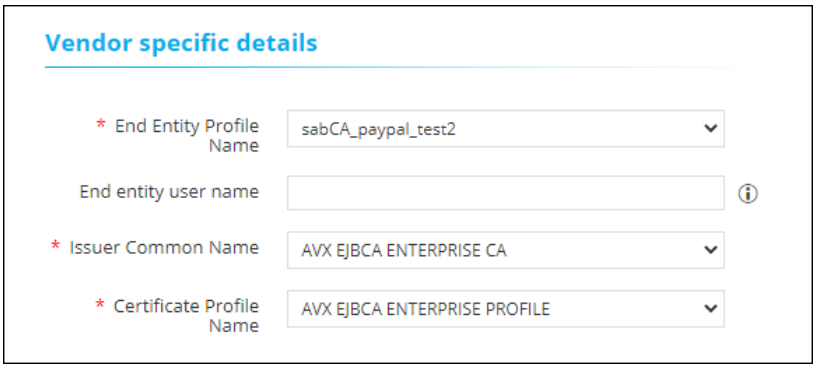


The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
**: Mandatory fields*	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section.



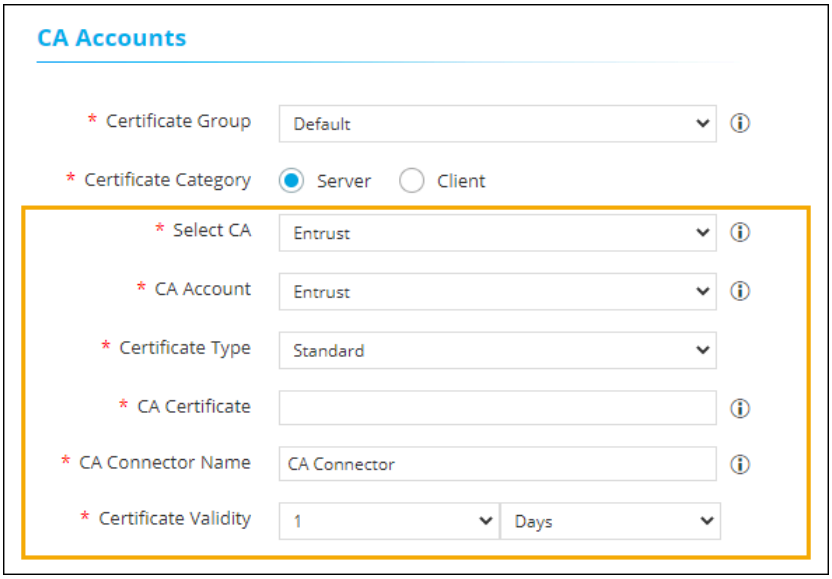
The fields for Vendor specific details are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
**: Mandatory fields*	

When **Entrust** is selected as CA.



The fields for Entrust CA are as follows:

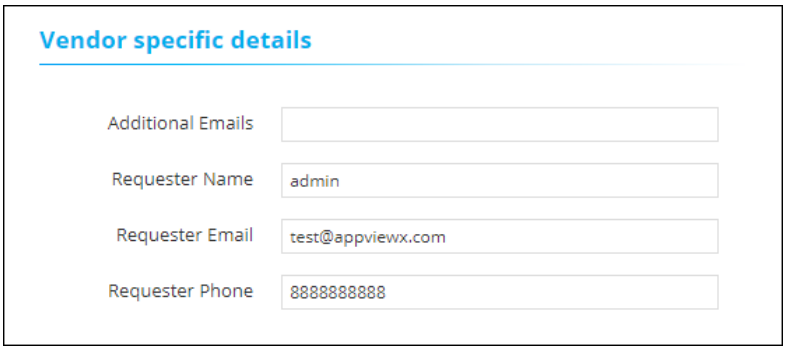
Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	Select a valid cert type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.



Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed as shown above.

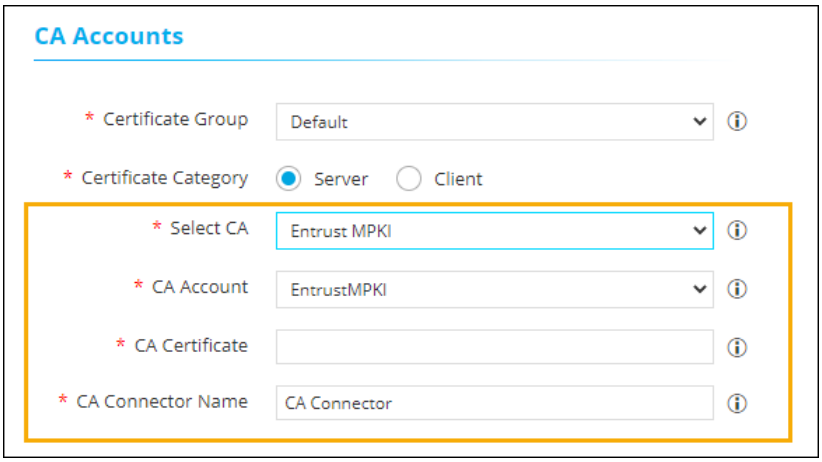
Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the demo details
Requester Email	Enter a valid email id

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Requester Phone	Enter the 10-digit phone number.
**: Mandatory fields*	

When **Entrust MPKI** is selected as CA.

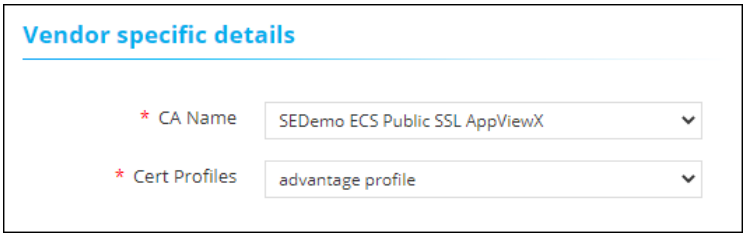


The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section.



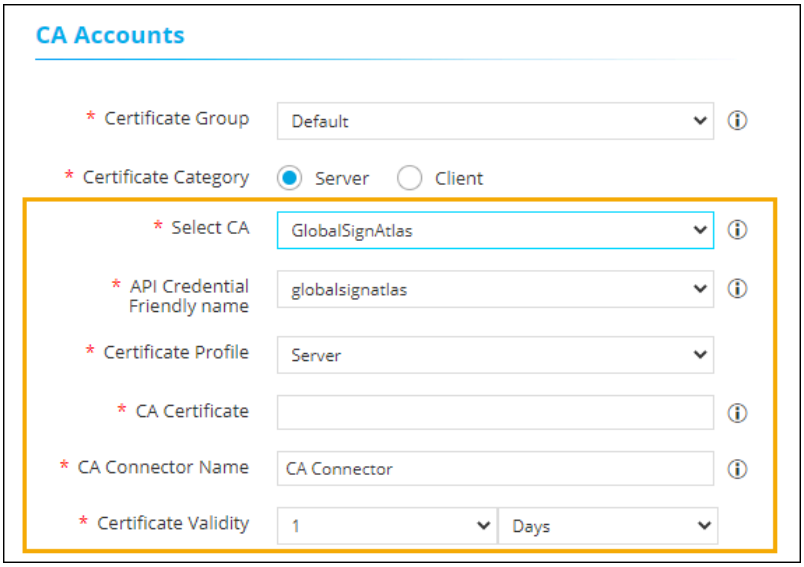
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
**: Mandatory fields*	

When **GlobalSign Atlas** is selected as CA



The fields for GlobalSign Atlas CA are as follows:

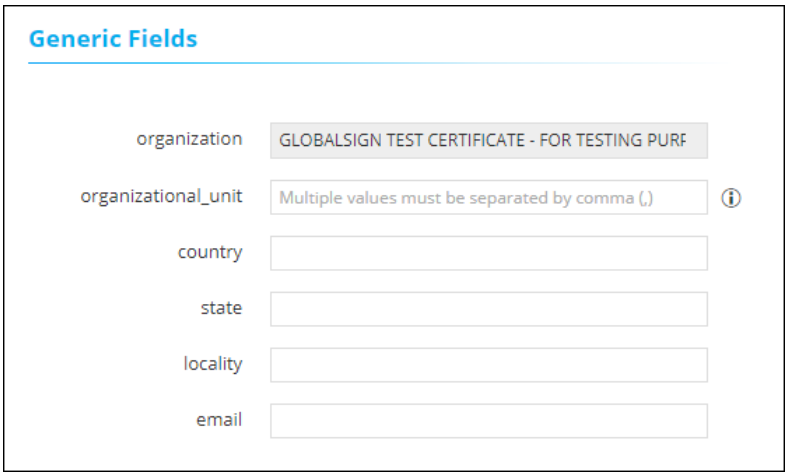
Details for GlobalSign Atlas CA - Field Description Table

Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.

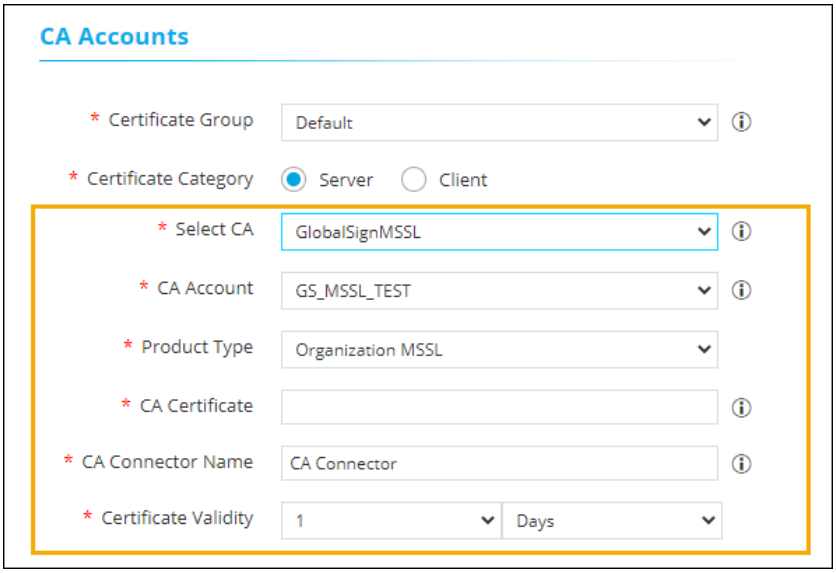
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.



When **GlobalSignMSSL** is selected as CA,



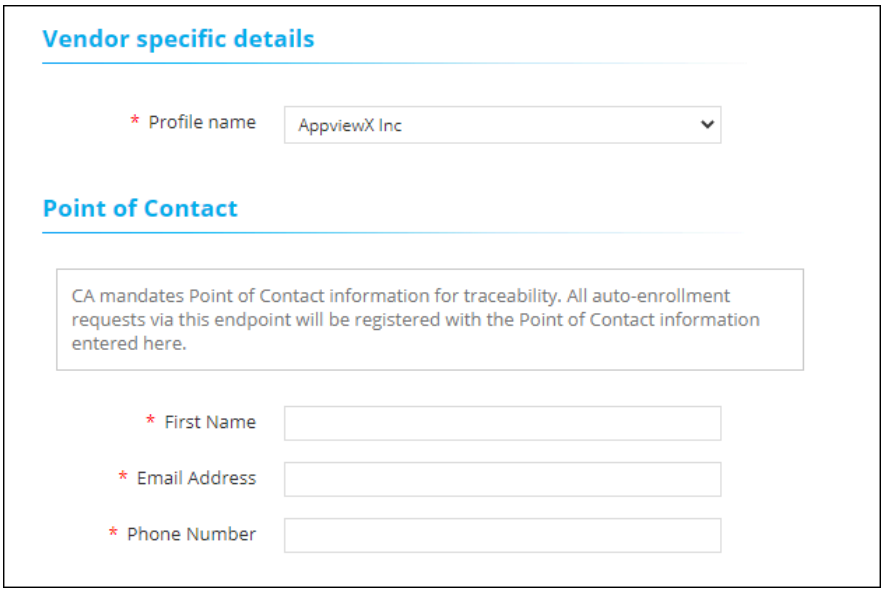
The fields for GlobalSign MSSL CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

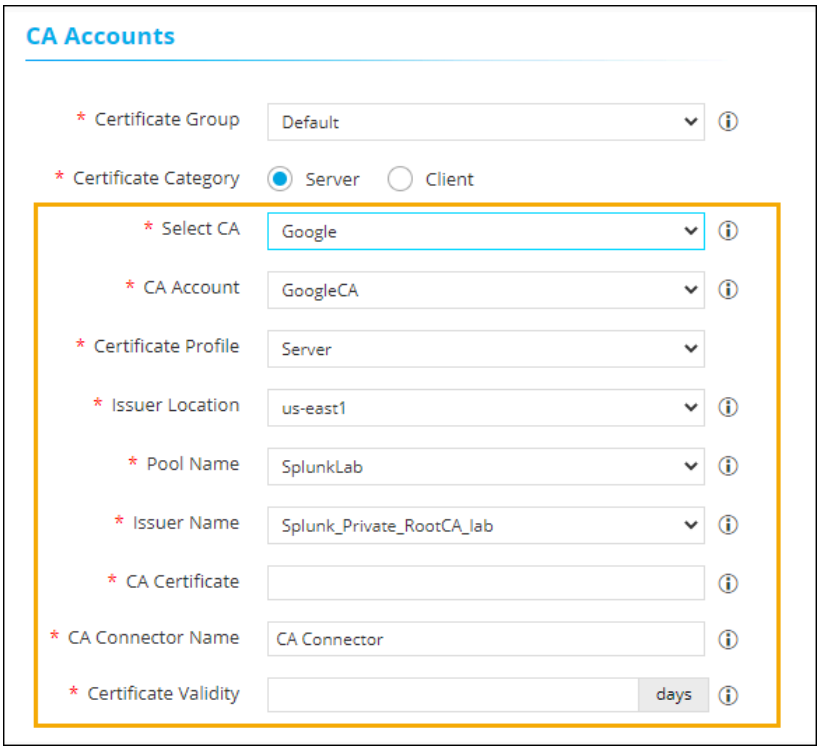
Fields	Description
*: Mandatory fields	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
*: Mandatory fields	

When **Google** is selected as CA.



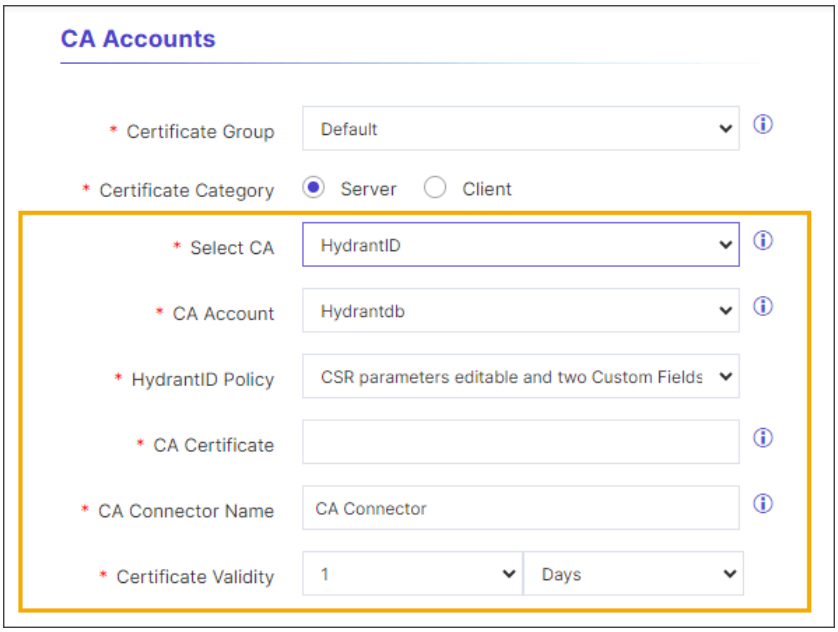
The fields for Google CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **HydrantID** is selected as CA.



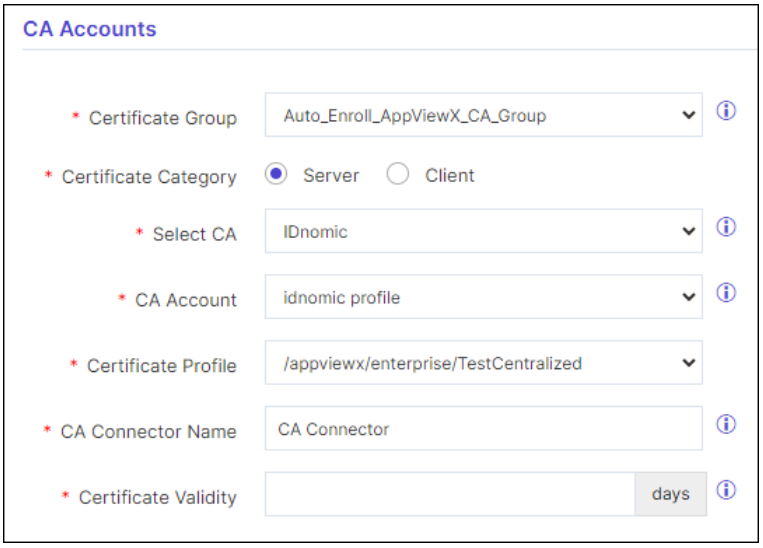
The fields for HydrantID CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for Lets HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **IDnomic** is selected as CA,



The fields for IDnomic CA are as follows:

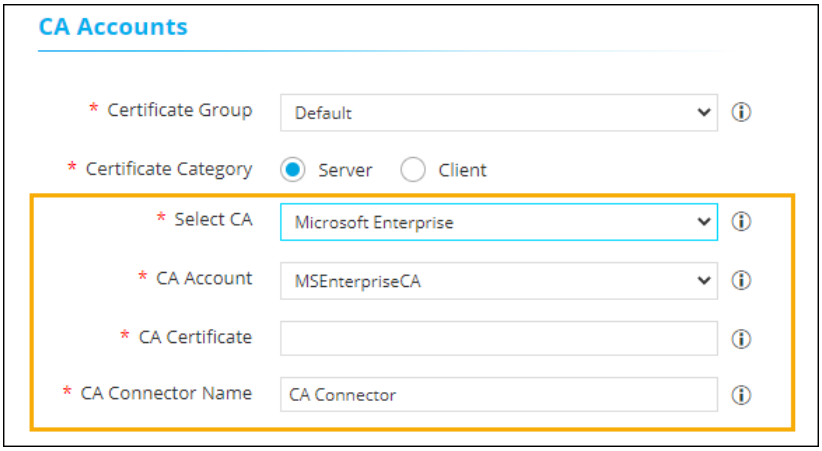
Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Microsoft Enterprise** is selected as CA.

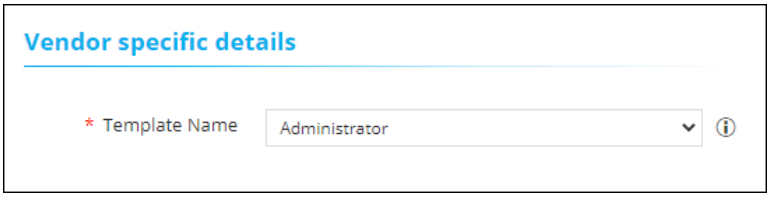


The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

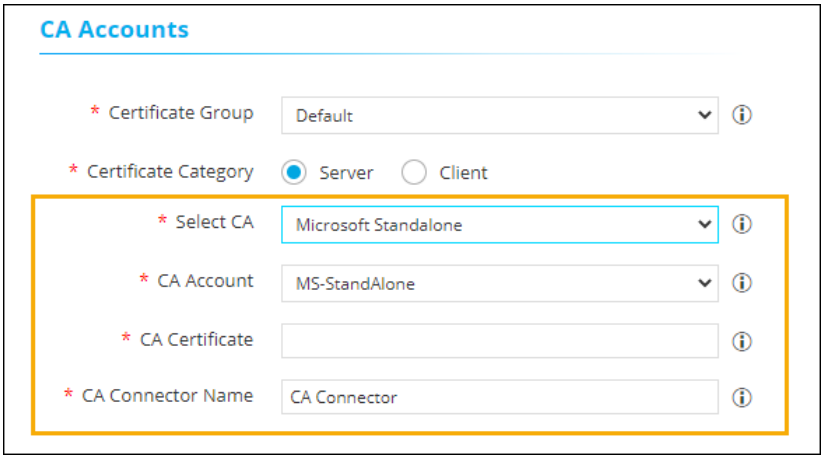
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed with a **Template Name** dropdown after the CA Accounts section.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

When **Microsoft Standalone** is selected as CA.



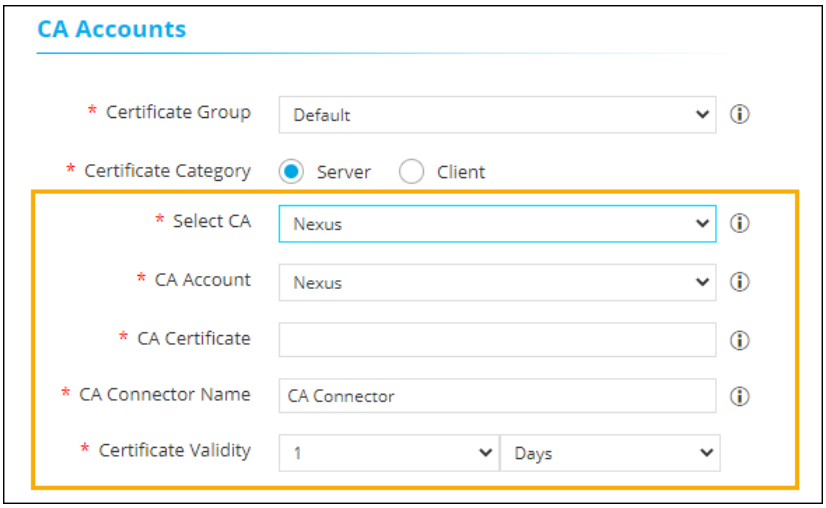
The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

When **Nexus** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

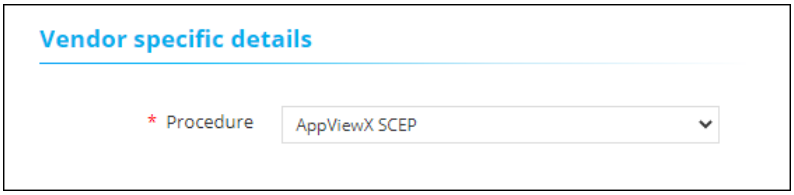


The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years).
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:



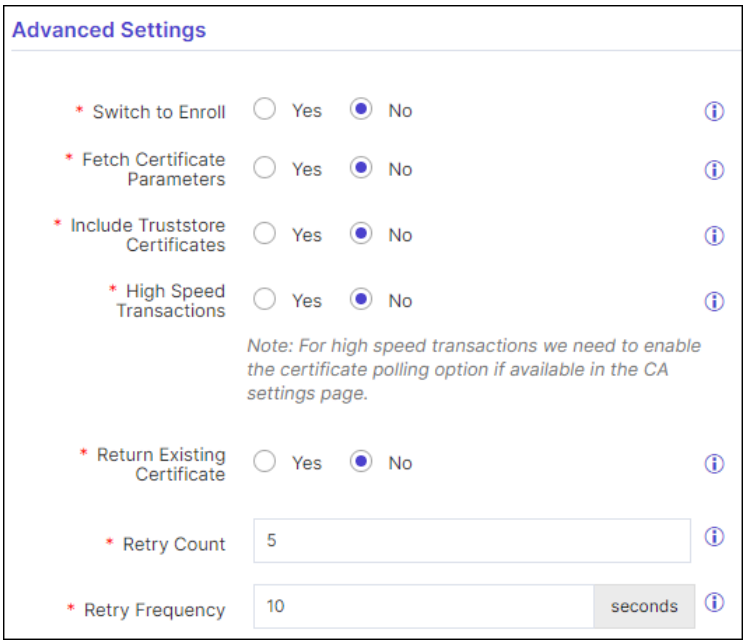
Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the Procedure based on the configurations made in the Certificate Authority Setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

6. Configure the **Advanced Settings**.

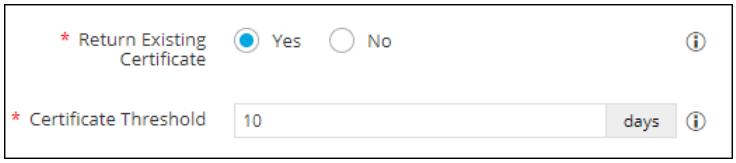


The fields in the Advanced Settings section are as follows:

Advanced Settings - Field Description Table

Fields	Description
***Switch to Enroll**	Select Yes or No Setting the radio button to Yes, will convert reenrollment requests to enrollment requests.
***Fetch Certificate Parameters**	Select Yes or No Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
***Include Truststore Certificates**	Select Yes or No Setting the radio button to Yes, will allow you to share the truststore certificates to client during authentication.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
High Speed Transactions	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol's Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed.  If the option is disabled (**No**) then the AppViewX will do the default behavior of enrolling a new certificate for each request.
Certificate Threshold	This field is enabled only if **Return Existing Certificate = Yes.** Enter the number of days in this field. This value is used to Initiate a new certificate request if the certificate is nearing the expiry date i.e., if existing certificate validity is less than the entered value.
***Retry Count**	Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received. Values accepted between 5 - 99.
***Retry Frequency**	The value specified in this field determines the duration taken between the trigger calls by the EST agent. Values accepted between 10 - 99.
**: Mandatory fields*	

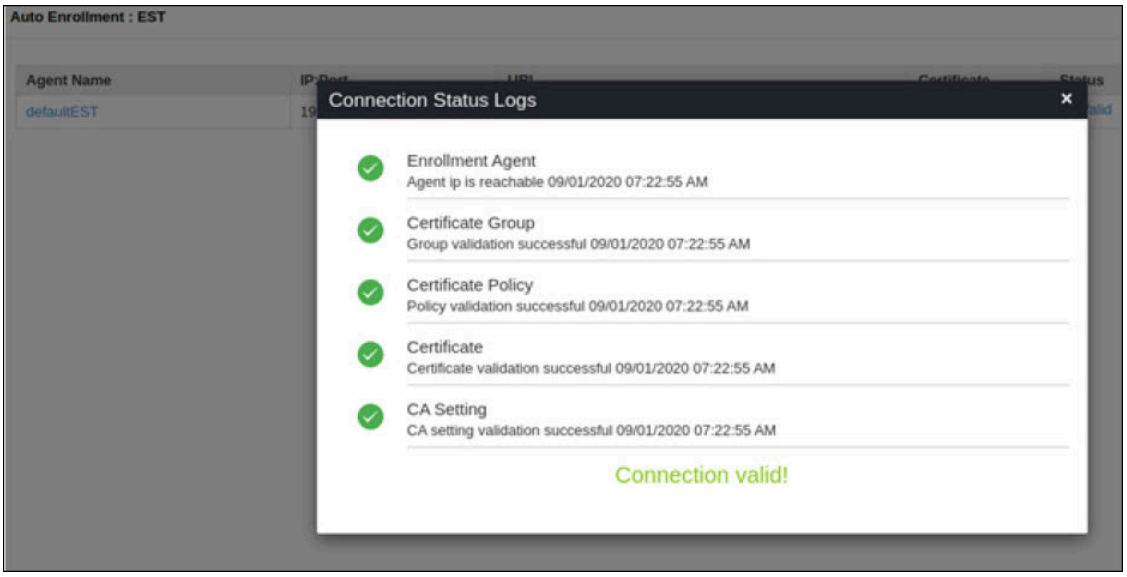
7. Click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Validating EST

Once the EST settings are added validation needs to be done to check whether the CA and Agent-related details are properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **EST**.
2. On the **EST** page, click **Check** from the Status column to validate the EST setting that has been created.
   The EST settings will be validated and the **Status** will be shown as either **Success** or **Failure.**



Microsoft Intune

Microsoft Intuneis a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). AppViewX has a SCEP based integration with MS Intune. This integration provides for provisioning of certificates to Microsoft Intune managed mobile devices.

- There should be an agent (avx_vendor_cert_intune_agent) up and running for MS Intune in AppViewX.
- This Intune plugin can either be in HTTPS or HTTP, but it needs a HTTP gateway running in order to communicate with the client.
- In order to make that HTTP gateway up and running go to /home/appviewx/appviewx/avxgw/avxgw-profile.json. Enable the HTTP profile and restart the gateway.
- It is highly recommended to keep the 'Approval Required' flag in OFF state from **Menu -> Inventory -> Certificate -> Policy** page.
- A valid agent settings should be available in **Menu -> Inventory -> Certificate -> Settings**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Configuring MS Intune
• Validating MS Intune

Configuring MS Intune

In order to conduct mobile device certificate enrollments for MS Intune managed devices using the MS Intune protocol (SCEP based) on AppViewX, the administrator or a privileged user must initially configure the MS Intune server agent using the AppViewX portal. Once the MS Intune server agent is successfully set up through the portal, a URL will be generated. Clients can then utilize this URL to submit enrollment requests to AppViewX via MS Intune.

To set up the MS Intune server,

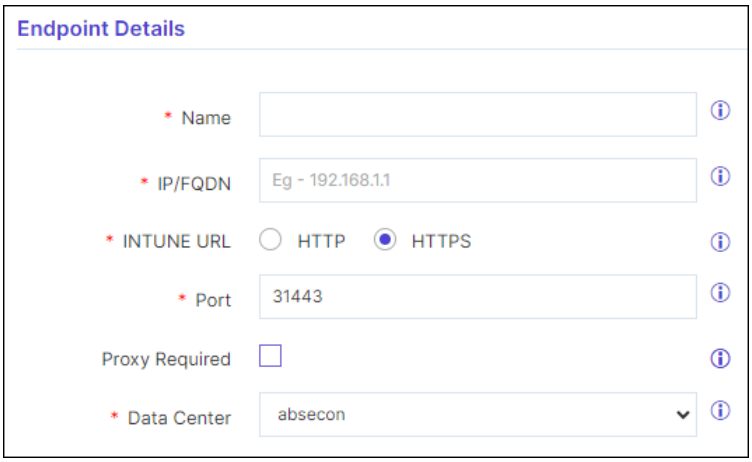
1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **MS INTUNE**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
3. Configure the **End Point Details** details as follows:

   Prerequisites for entering the IP/FQDN field:

   - For **SaaS**
     - The "Cloud Connector Name" (in the Add Cloud connector page) must be the same as the FQDN name entered.
     - If the customer is using LB on top of multiple CC then the FQDN of the LB should be used.
   - For On-Prem
     - The IP / FQDN of the machine where the external gateway is running.
     - If the customer is using LB on top of multiple CC then the FQDN of the LB should be used.
   - The given FQDN must be resolvable in the cloud connector machine and also in the company portal Application running machine
   - The CC should have the reachability to the Endpoint.

   The fields for Endpoint Details are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



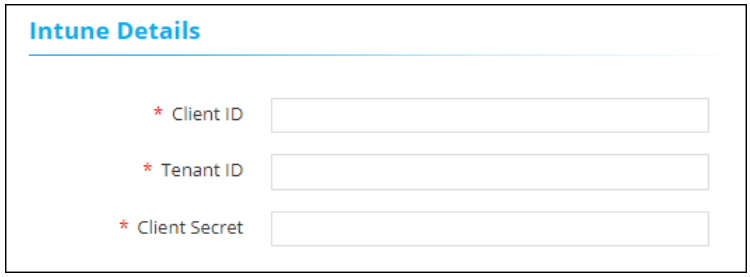
Endpoint Details - Field Description Table

Fields	Description
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable Characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	Enter the FQDN/IP address of the AppViewX SCEP gateway. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***Intune URL**	Select either HTTP or HTTPS. Based on the selection of this field, the Intune endpoints will be configured with HTTP or HTTPS URL. The port information will be dynamically updated based on this selection. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use HTTPS.
***Port**	The gateway port of the AppViewX node. In a standard AppViewX setup the HTTP MS Intune endpoints should be configured with port 30022 and for HTTPS the port used is 31443.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only port 443.
Proxy	Select the checkbox if required. If **enabled** the communication with the Azure portal to validate challenge password will go via the Proxy details provided in the general settings. It is used to perform the challenge verification in Intune, via the proxy server (in case there is no internet connectivity.)
***Datacenter**	The selected datacenter is where the intune pod present that accepts the enrollment call. The value is auto-populated based on the cloud connector. The communication with the Azure portal to validate challenge password will go via the CC in the datacenter. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, select "cloud-dc" (it is the only available value for this configuration.
**: Mandatory fields*	

4. Configure the **Intune Details** as below:



The fields for Intune Details section are as follows:

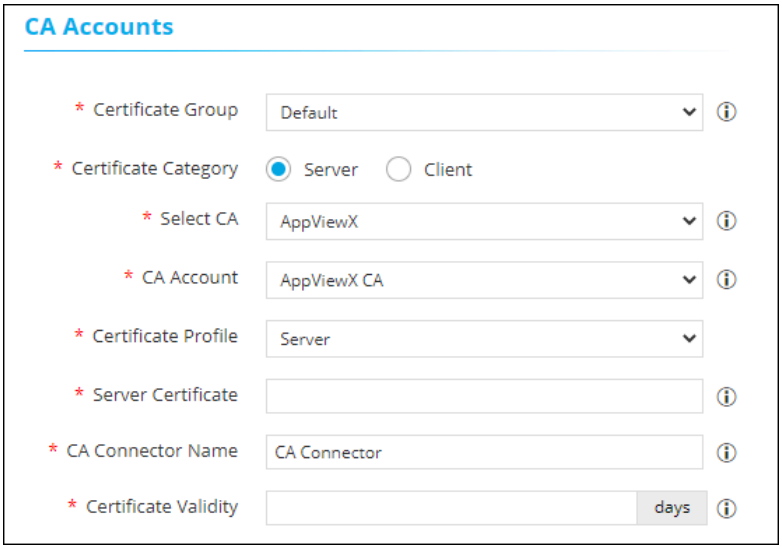
Intune Details - Field Description Table

Fields	Description
***Client ID**	Client ID of the Intune Account - this value should have been captured during Intune App Registration.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Tenant ID**	Tenant ID is the domain name in your account ID. For example, if your account id is **admin@test.onmicrosoft.com** then the tenant Id is **test.onmicrosoft.com**.
***Client Secret**	Client Secret for the Intune Account - this value should have been captured during Intune App Registration.
**: Mandatory fields*	

5. Configure the **CA Accounts** as follows:



The fields for CA Accounts section are as follows:

CA Accounts - Field Description Table

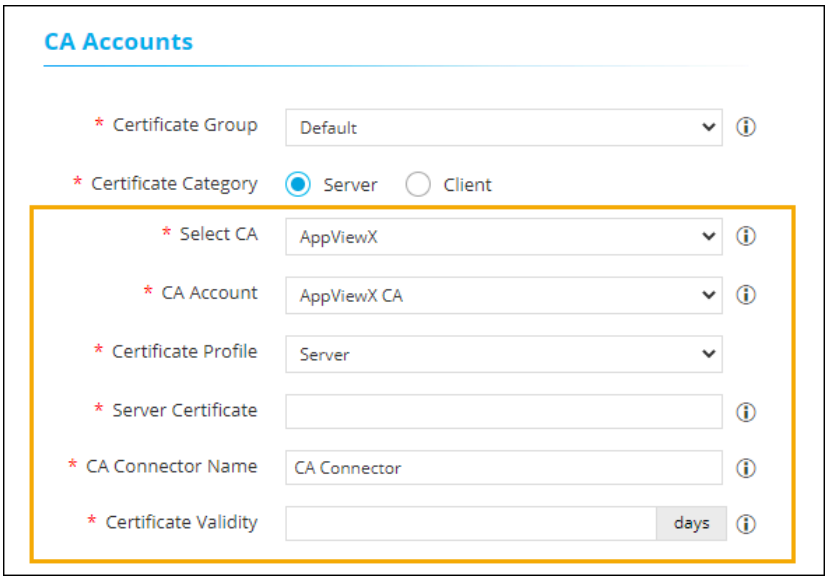
Fields	Description
Certificate Group	Select a specific group under which certificate needs to be enrolled.
Certificate Category	Select a specific certificate type (Server / Client) to be enrolled.
Select CA	Select the required CA from the available options. The certificate will be enrolled under the selected CA. The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• Amazon Private CA • DigiCert • DigiCert MPKI • Ejbca • Entrust MPKI • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus **Note:** The Vendor Specific Details section is displayed only after the following CA Account is selected: • DigiCert • Ejbca • Entrust • Entrust MPKI • GlobalSign MSSL • Microsoft Enterprise • Nexus
**: Mandatory fields*	

When **AppViewX** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



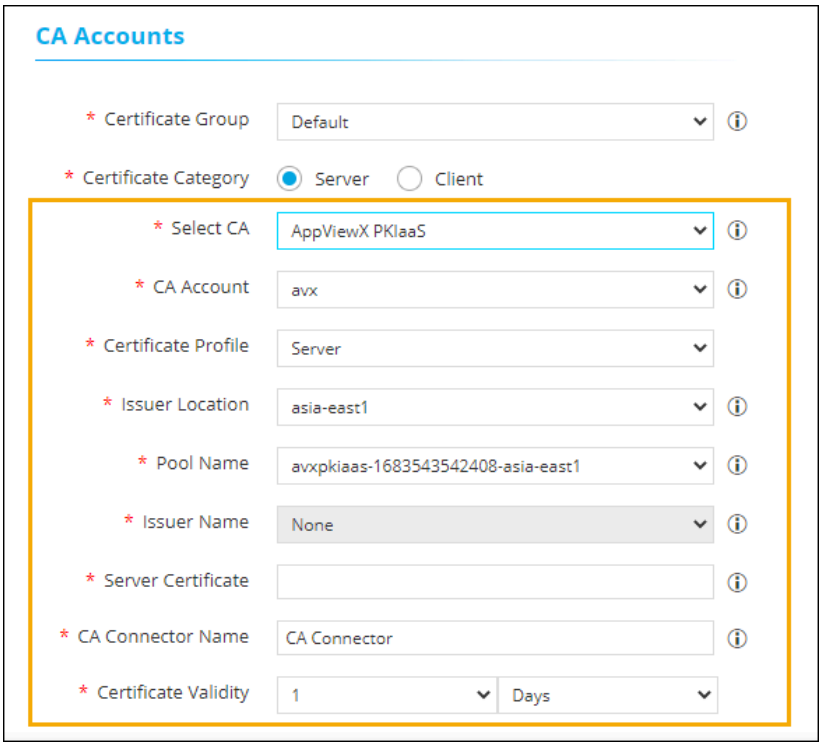
The fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **AppViewX PKIaaS** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for AppViewX PKIaaS CA are as follows:

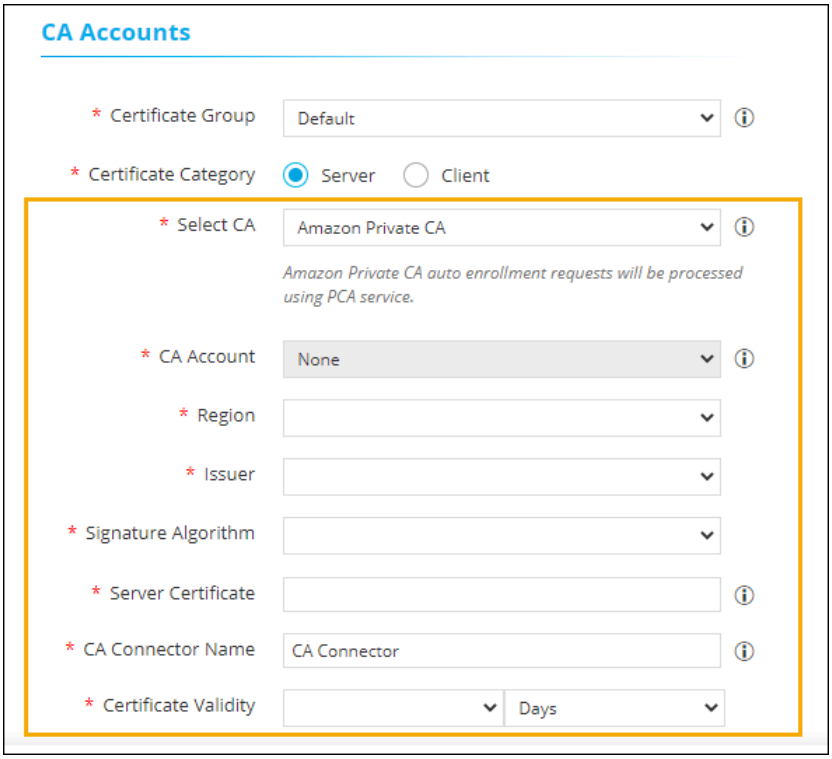
Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Certificate**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with MSIntune client machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Amazon Private CA** is selected as CA.



The fields for Amazon Private CA are as follows:

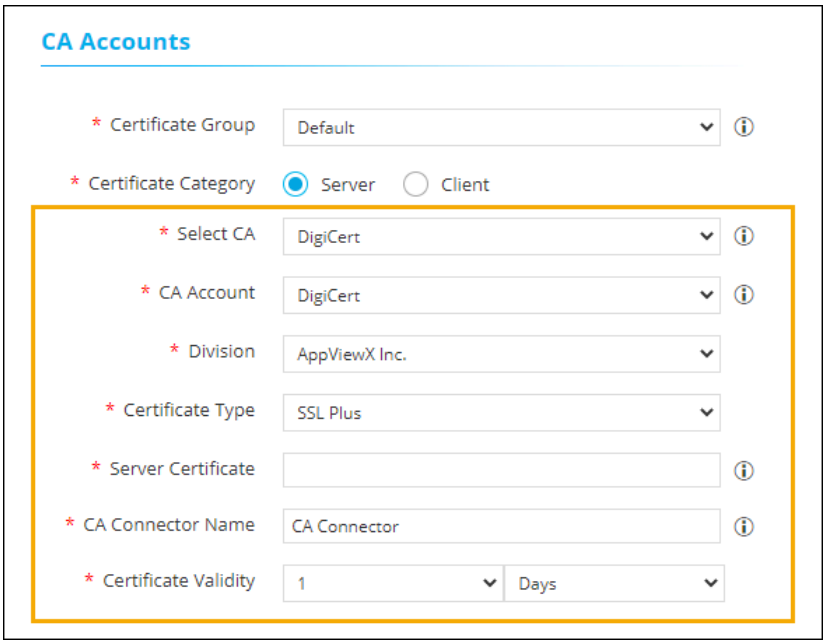
Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The dropdown list is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

When **DigiCert** is selected as CA.



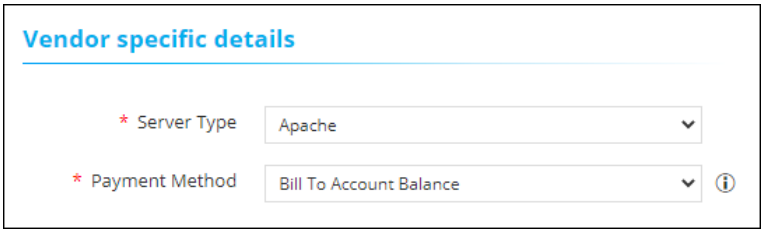
The fields for DigiCert CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid cert type associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.



The fields for Vendor specific details are as follows:

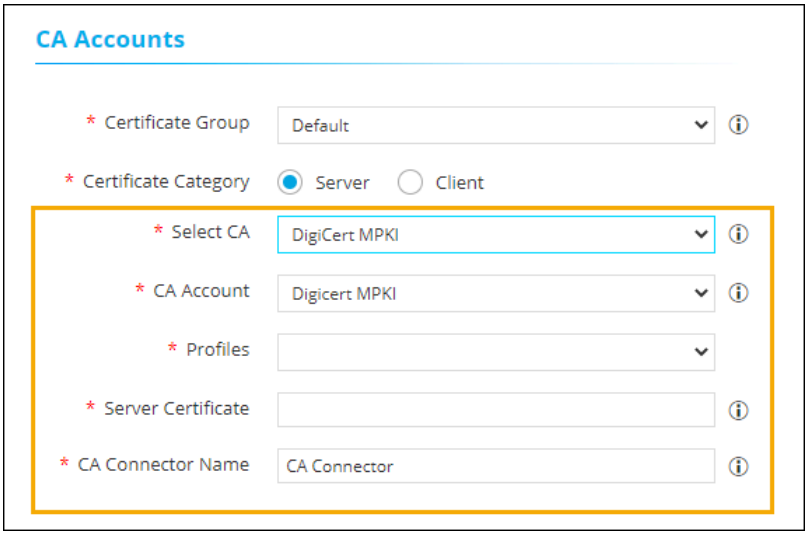
Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
**: Mandatory fields*	

When **DigiCertMPKI** is selected as CA.

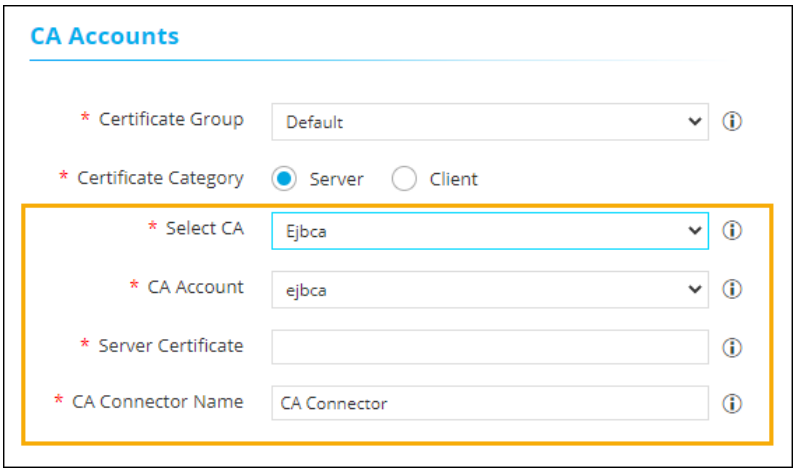


The fields for DigiCert MPKI CA are as follows:

Note: Based on the DigiCert MPKI account configuration **Custom Attributes** section may also be displayed on the endpoint configuration page.

When **EJBCA** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

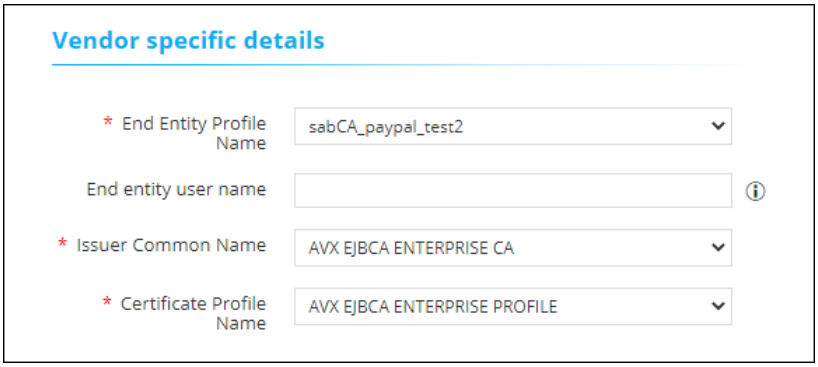


The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
**: Mandatory fields*	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.



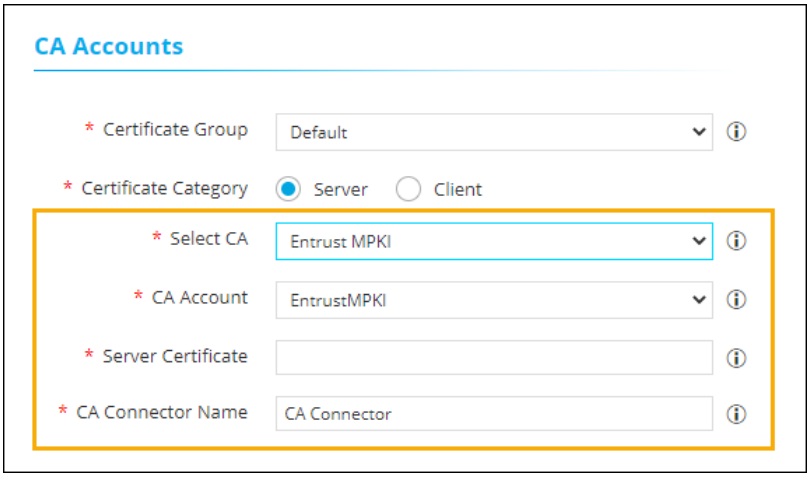
The fields for Vendor specific details are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
**: Mandatory fields*	

When **Entrust MPKI** is selected as CA.



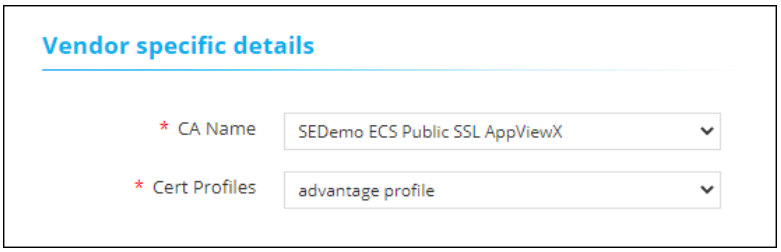
The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

If the selected CA is **Entrust MPKI**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

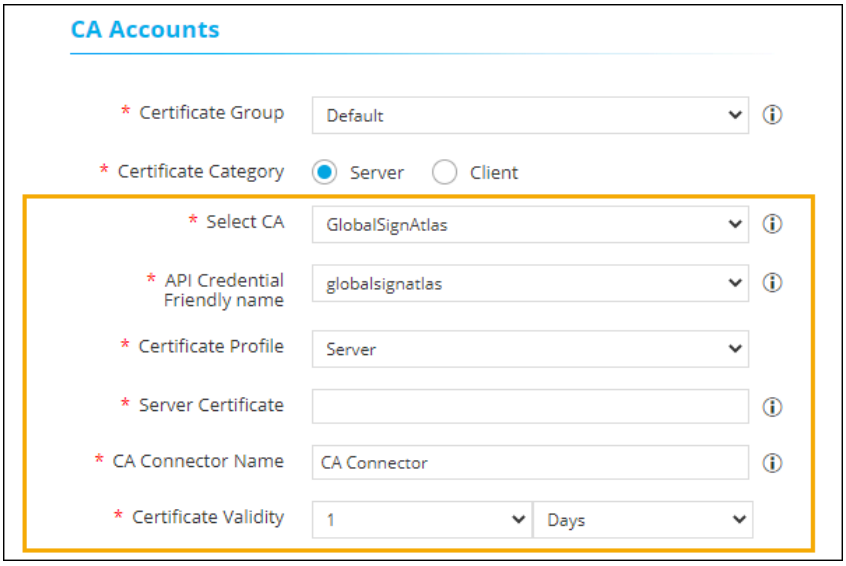


The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
**: Mandatory fields*	

When **GlobalSign Atlas** is selected as CA



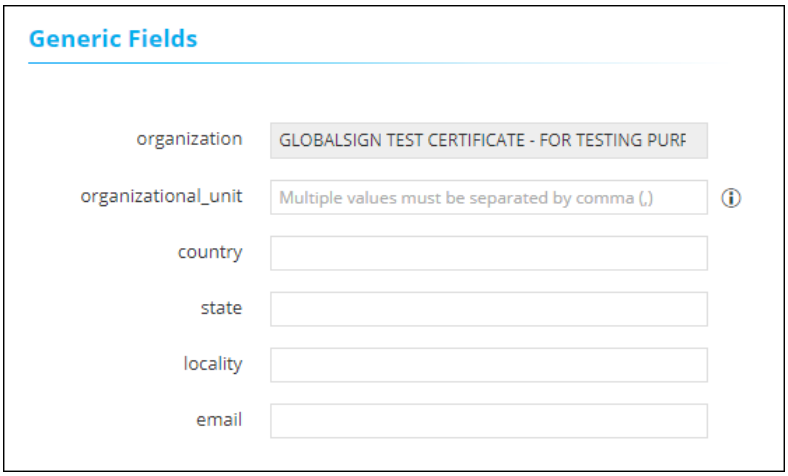
The fields for GlobalSign Atlas CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for GlobalSign Atlas CA - Field Description Table

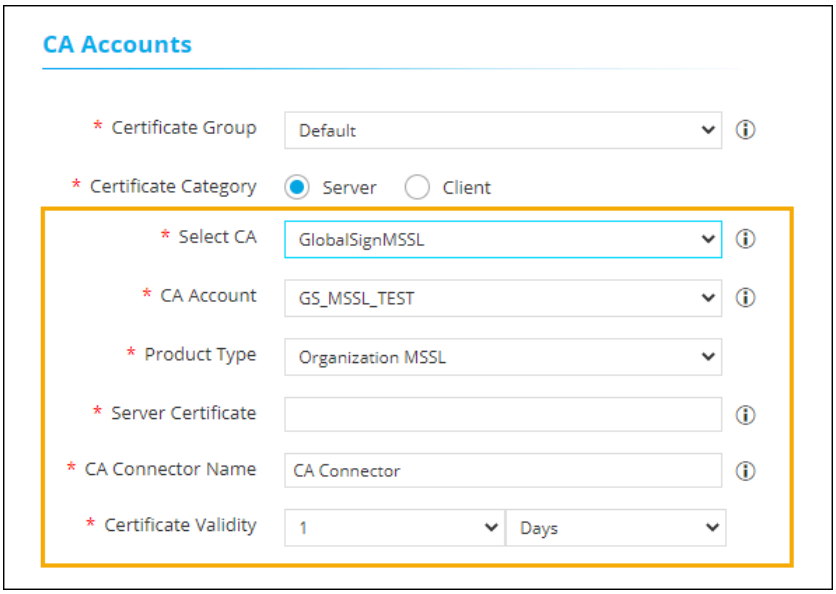
Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.



When **GlobalSignMSSL** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



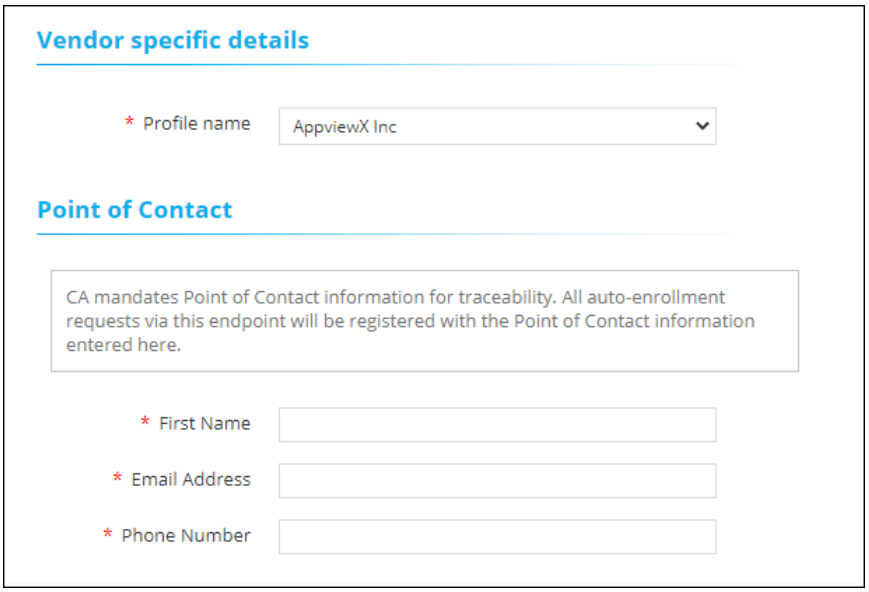
The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
**: Mandatory fields*	

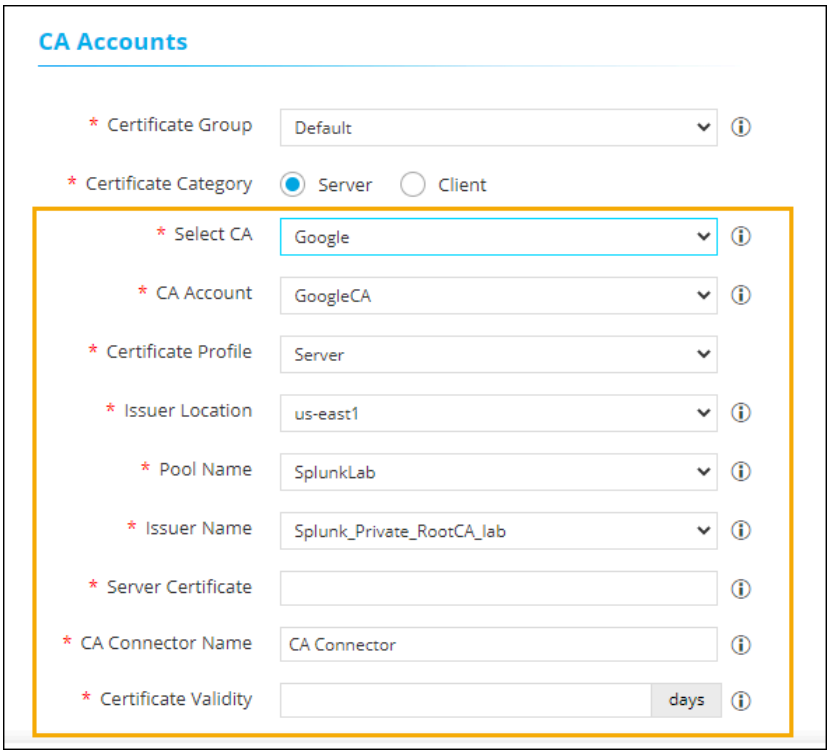
The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
**: Mandatory fields*	

When **Google** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for Google CA are as follows:

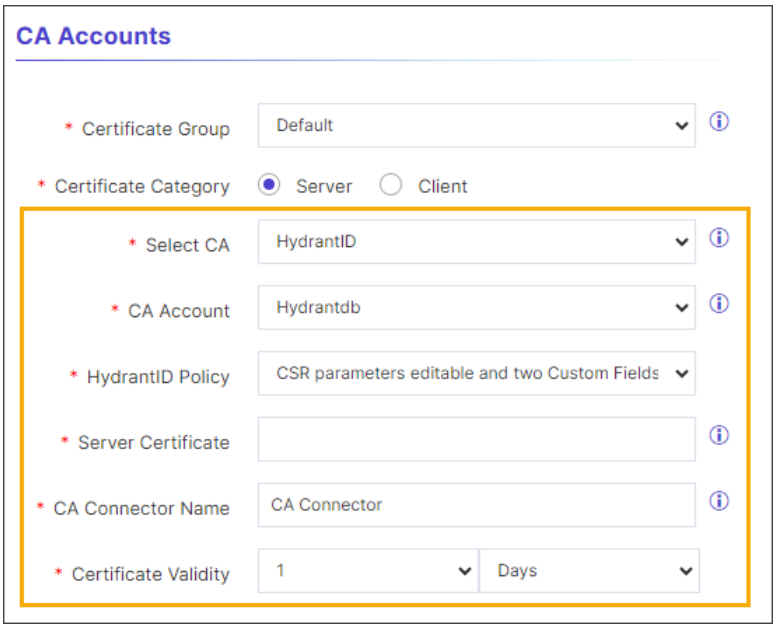
Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

When **HydrantID** is selected as CA,



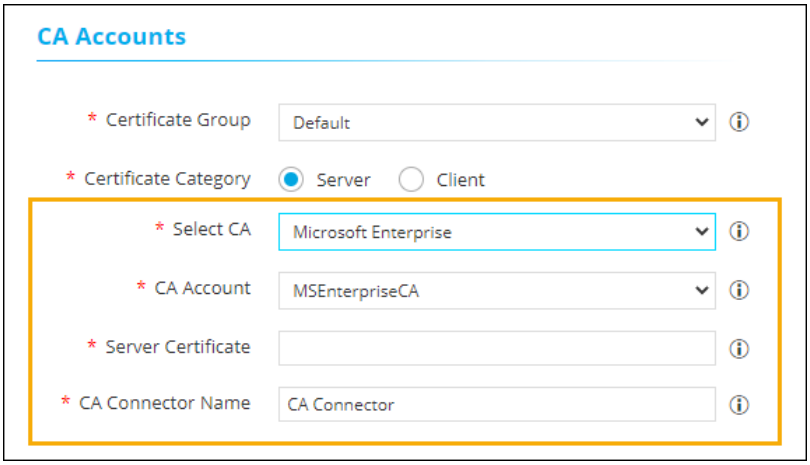
The fields for HydrantID CA are as follows:

Details for Lets HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
*** CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

When **Microsoft Enterprise** is selected as CA,

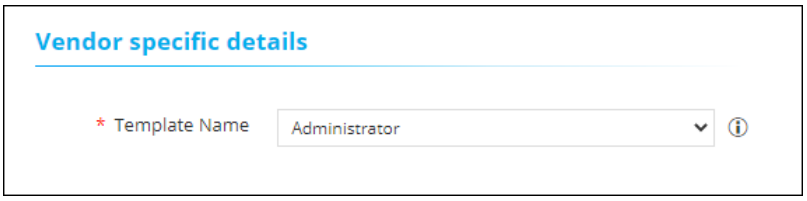


The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

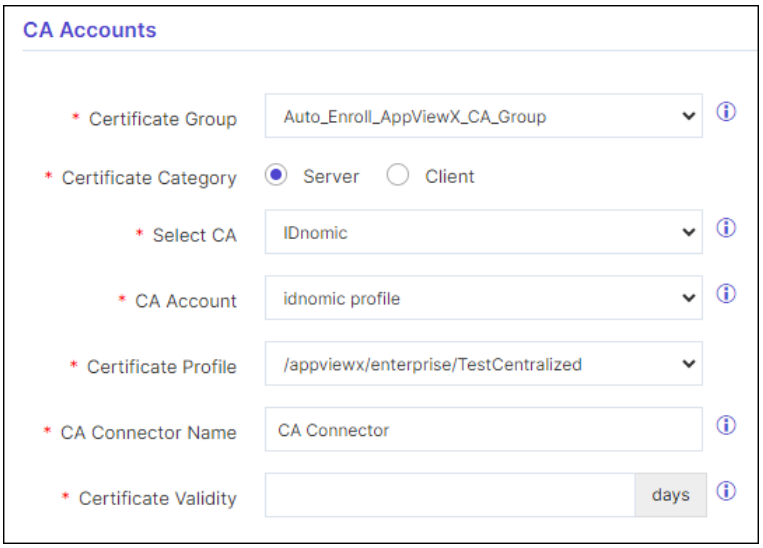
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed after the CA Accounts section with a dropown field - **Template Name** - Select a template from the dropdown list.



When **IDnomic** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

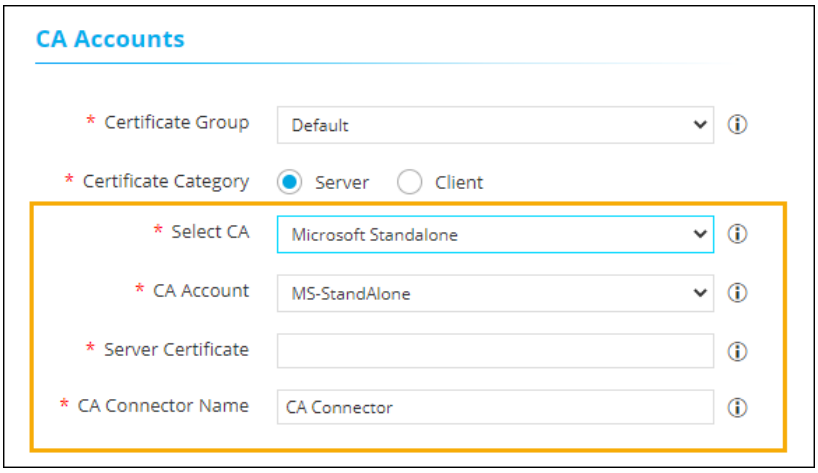


The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Microsoft Standalone** is selected as CA,



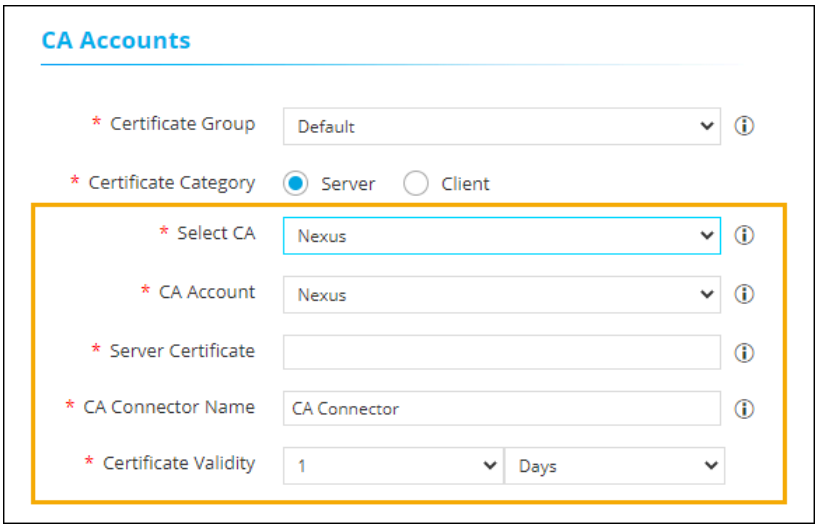
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

The following table provides the field description for **Nexus CA**:



The fields for Nexus CA are as follows:

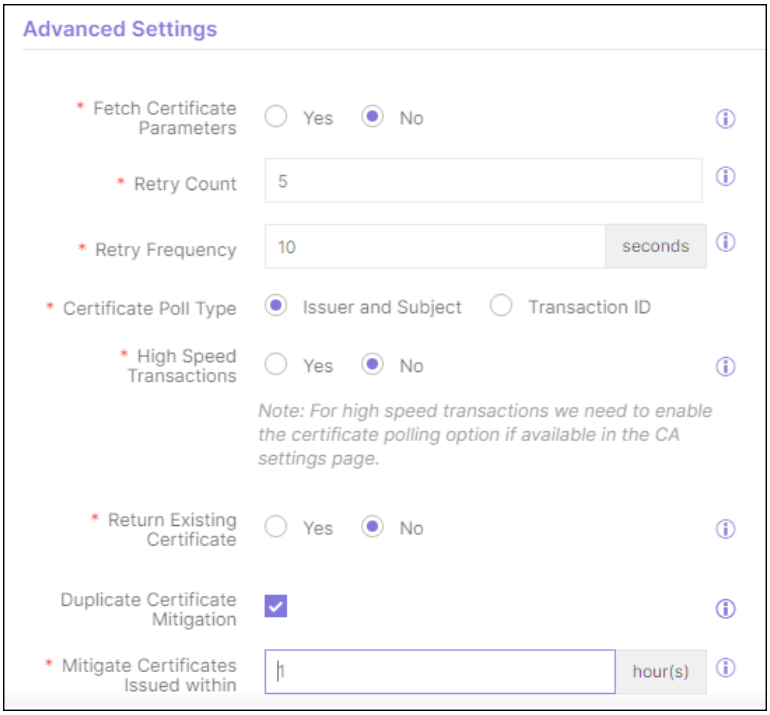
Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Server Certificate**	Select the chosen CA issued certificate, using which the trusted inventory is validated.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Type the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years).
**: Mandatory fields*	

6. Configure the **Advanced Settings**.

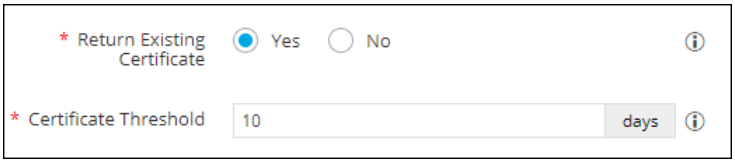


The fields in the Advanced Settings section are as follows:

Advanced Settings - Field Description Table

Fields	Description
***Fetch Certificate Parameters**	Select Yes or No Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Retry Count**	Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received. Values accepted between 5 - 99.
***Retry Frequency**	The value specified in this field determines the duration taken between the trigger calls by the EST agent. Values accepted between 10 - 99.
***Certificate Poll Type**	Select *Issuer and Subject* or *Transaction ID*. The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.
***High Speed Transactions**	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol's Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed.  If the option is disabled (**No**) then the AppViewX will do the default behavior of enrolling a new certificate for each request.
Duplicate Certificate Migration	Selecting this check-box will cause the previously issued certificates for the same CSR parameters to be revoked and deleted from AppViewX.
***Mitigate Certificates issued within**	This field is enabled only when the **Duplicate Certificate Migration** check-box is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

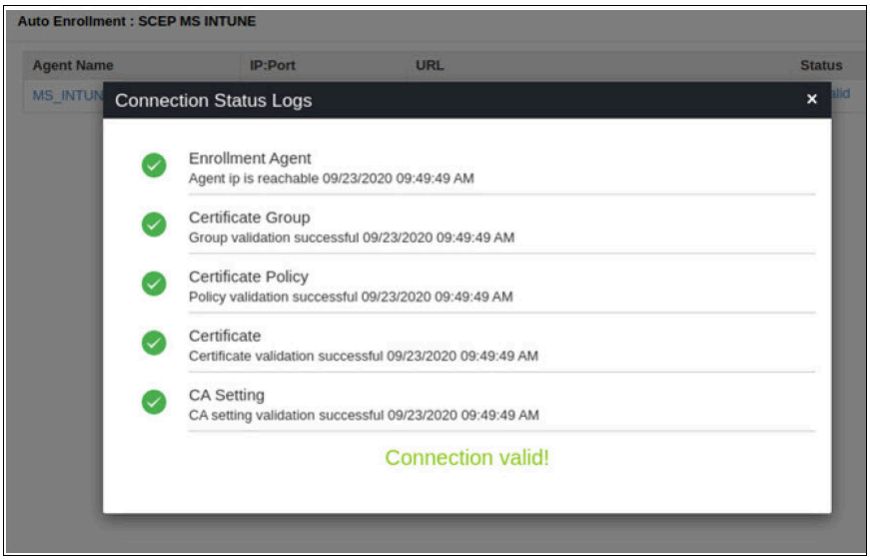
Fields	Description
*: Mandatory fields	

7. Click **Save**.

Validating MS Intune

Once the MS Intune settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **MS INTUNE**.
2. In the **MS Intune** page, click **Check** from the status column to validate the MS Intune setting that has been created.
   The Intune settings will be validated and the **Status** will be shown as either **Success** or **Failure**.



SCEP

SCEP stands for **Simple Certificate Enrollment Protocol**, it is a certificate management protocol targeting Public Key Infrastructure (PKI) clients which require digital certificates to prove their authenticity. SCEP also helps the clients in acquiring associated CA certificates. Some prerequisites and features are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- There should be an agent (avx_vendor_cert_scep_agent) up and running for SCEP in AppViewX.
- The SCEP plugin can either be in HTTPS or HTTP, but it needs an HTTP gateway running in order to communicate with the client.
- In order to make that HTTP gateway up and running go to /home/appviewx/appviewx/avxgw/avxgw-profile.json. Enable the HTTP profile and restart the gateway.
- It is highly recommended to keep the 'Approval Required' flag OFF in the **Menu -> Inventory -> Certificate -> Policy** page.
- The valid agent settings should be available in **Menu -> Inventory -> Certificate -> Settings**.

- Configuring SCEP
- Validating SCEP
- SCEP Enroll and Renew

Configuring SCEP

In order to carry out client certificate enrollments using the SCEP protocol, the administrator or a privileged user must initially configure the SCEP server agent using the AppViewX portal. Once the SCEP server agent is successfully set up through the portal, a URL will be generated. Clients can then utilize this URL to submit enrollment requests to AppViewX via SCEP.

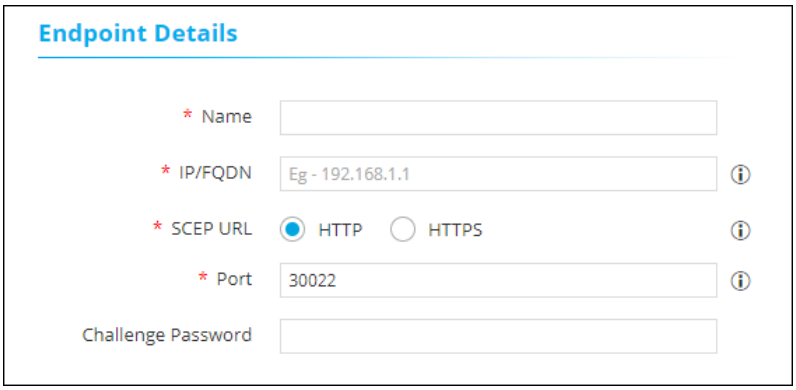
To set up the SCEP server agent,

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **SCEP**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
3. Configure the **End Point Details** details as follows:

   Prerequisites for entering the IP/FQDN field:

   - The "Cloud Connector Name" (in the Add Cloud connector page) must be the same as the FQDN name entered.
   - The CC should have the reachability to the Endpoint.
   - If entering the IP the ensure that single cloud connector is used.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for Agent Details section are as follows:

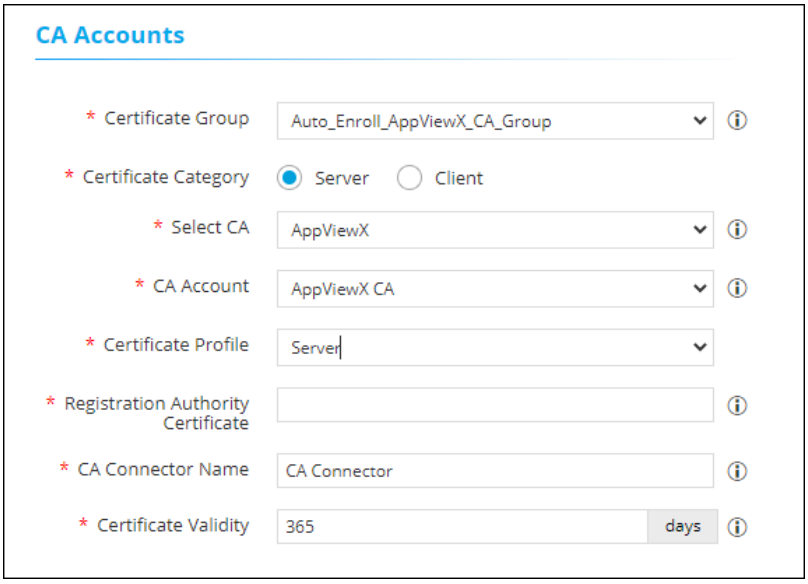
Endpoint Details - Field Description Table

Fields	Description
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable Characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	Enter the FQDN/IP address of the AppViewX SCEP gateway. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***SCEP URL**	Select either HTTP or HTTPS. Based on the selection of this field, the SCEP endpoints will be configured with HTTP or HTTPS URL. The port information will be dynamically updated based on this selection. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use HTTPS.
***Port**	The gateway port of the AppViewX node. In a standard AppViewX setup the HTTP SCEP endpoints should be configured with port 30022. (For HTTPS the port used in 31443).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only port 443.
Challenge Password	A challenge token to be used while enrolling certificates. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, it is recommended to provide a challenge password.
**: Mandatory fields*	

4. Configure the **CA Accounts** details as follows:



The fields for CA Accounts section are as follows:

CA Accounts - Field Description Table

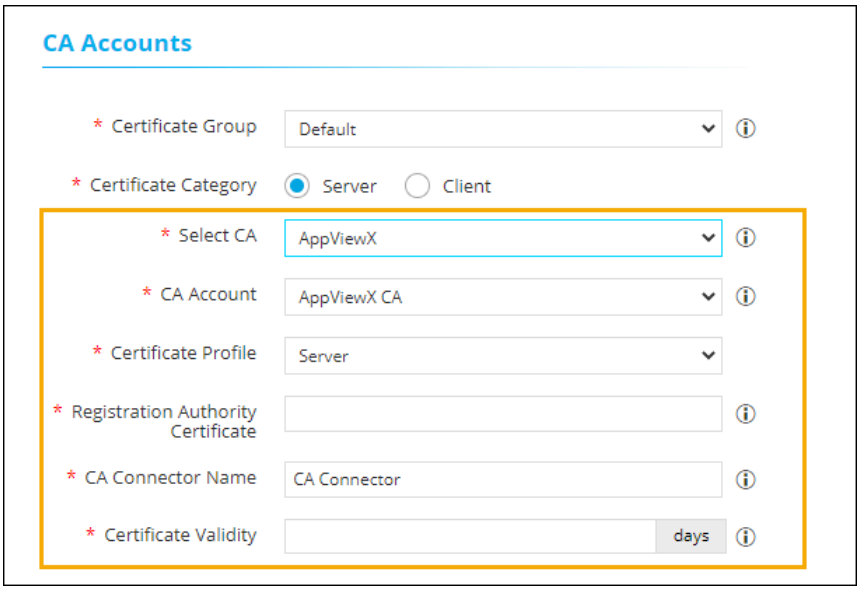
Fields	Description
Certificate Group	Select a specific group under which certificate needs to be enrolled.
Certificate Category	Select a specific certificate type (Server / Client) to be enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Select CA	Select the required CA from the available options. The certificate will be enrolled under the selected CA. The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • Amazon Private CA • DigiCert • DigiCert MPKI • Ejbca • Entrust • Entrust MPKI • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Nexus **Note:** The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs as follows: • Digicert • Ejbca • Entrust • Entrust MPKI • GlobalSign MSSL • MS Enterprise • Nexus
**: Mandatory fields*	

When **AppViewX** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



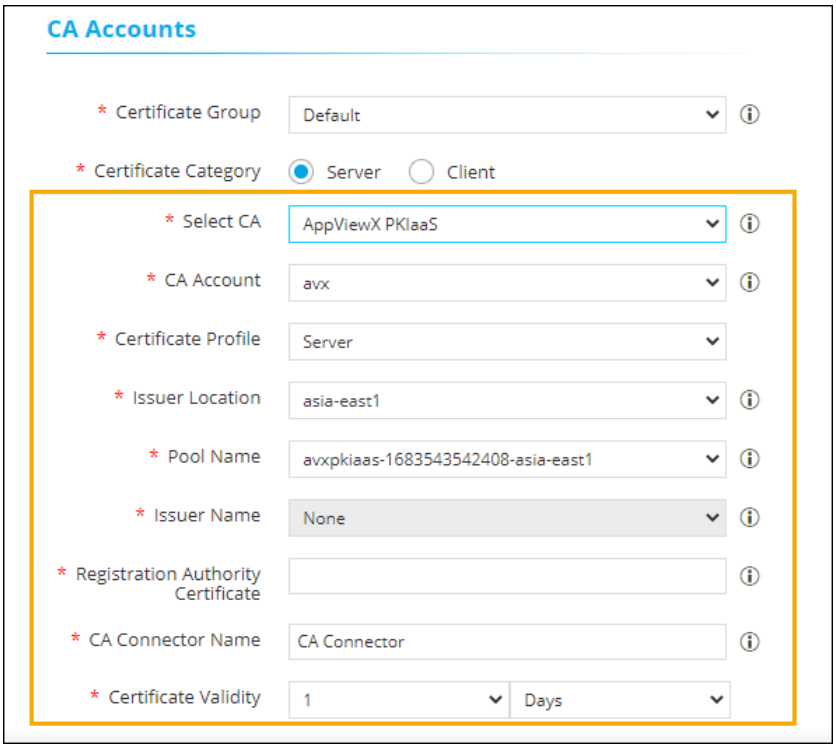
The fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **AppViewX PKIaaS** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for AppViewX PKIaaS CA are as follows:

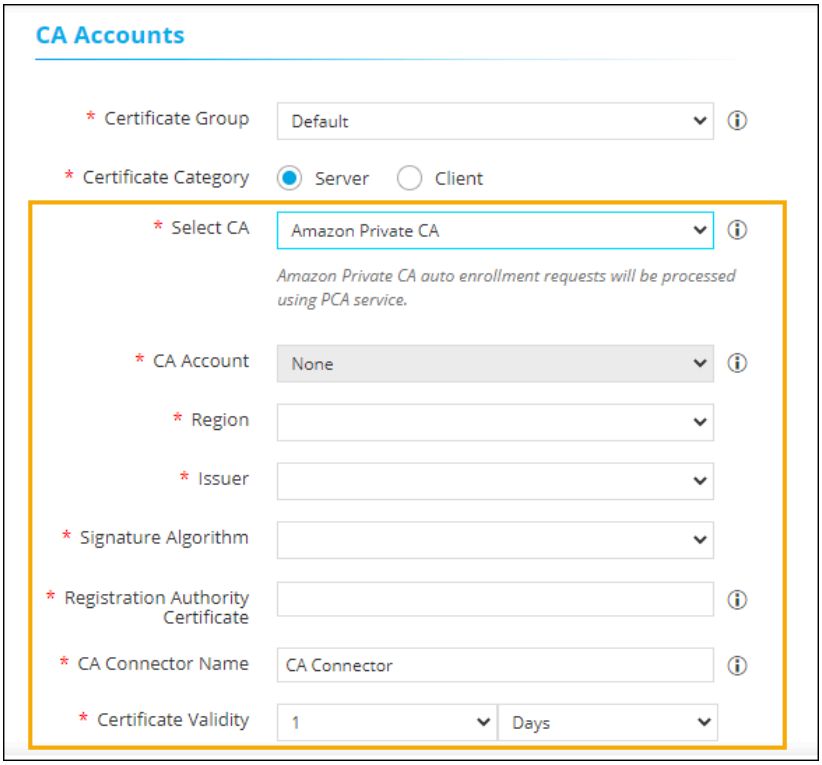
Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Amazon Private CA** is selected as CA.



The fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

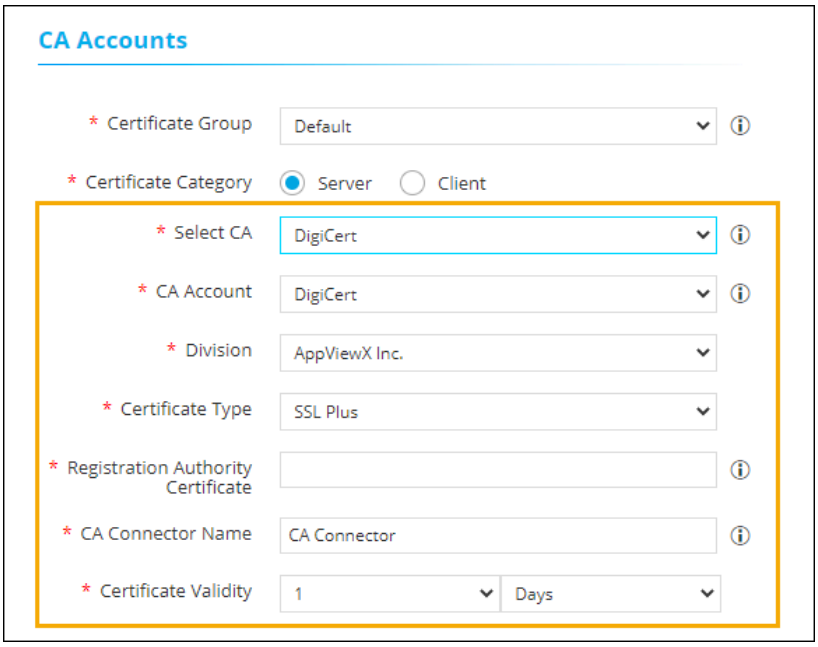
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The dropdown list is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

When **DigiCert CA** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for DigiCert CA are as follows:

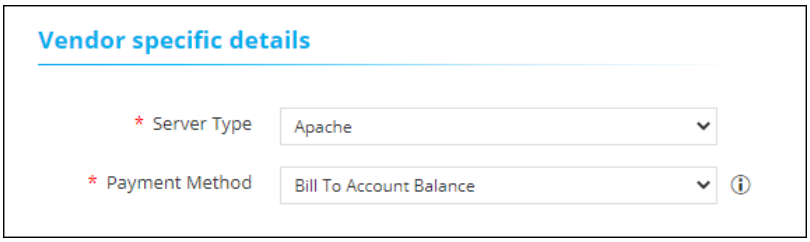
Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid cert type associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

If the **Select CA =DigiCert**, and the **Certificate type = Server**, a separate section **Vendor Specific Details** is displayed after the CA Accounts section with two fields.



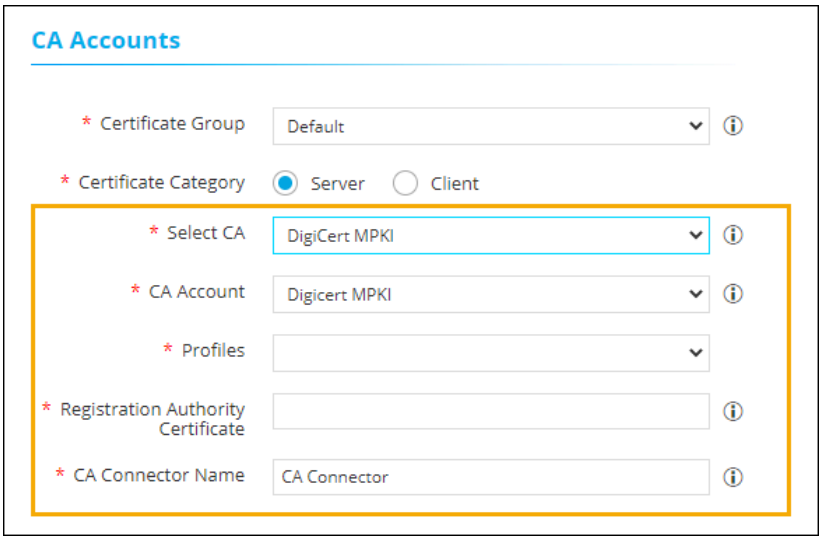
The fields for Vendor specific details are as follows:

Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
**: Mandatory fields*	

When **DigiCert MPKI** is selected as CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for DigiCert MPKI CA are as follows:

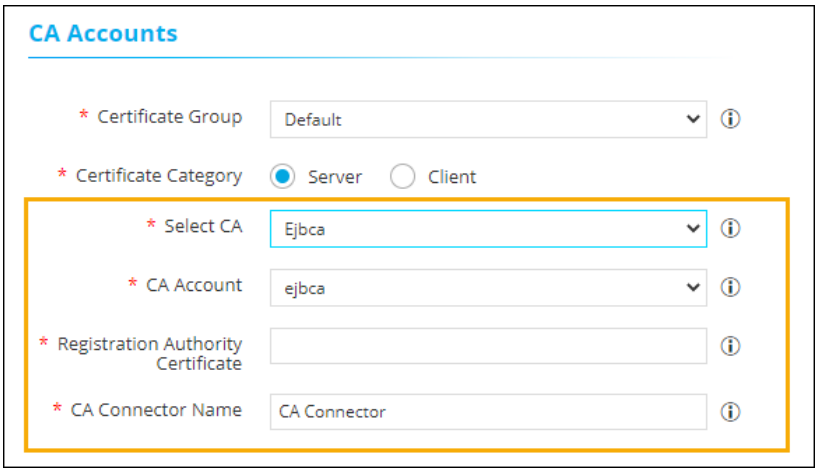
Details for DigiCert MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Profiles**	Select a profile associated with the CA account.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

Note: Based on the DigiCert MPKI account configuration **Custom Attributes** section may also be displayed on the endpoint configuration page.

When **EJBCA** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

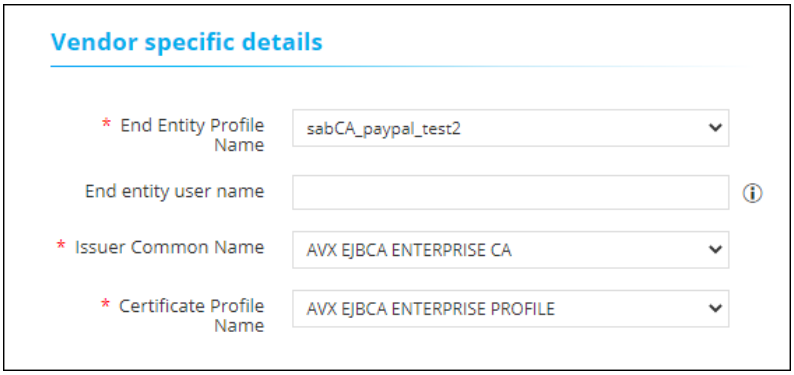


The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.
**: Mandatory fields*	

If the selected CA is Ejbca, a separate section **Vendor specific details** is displayed after the CA Accounts section.



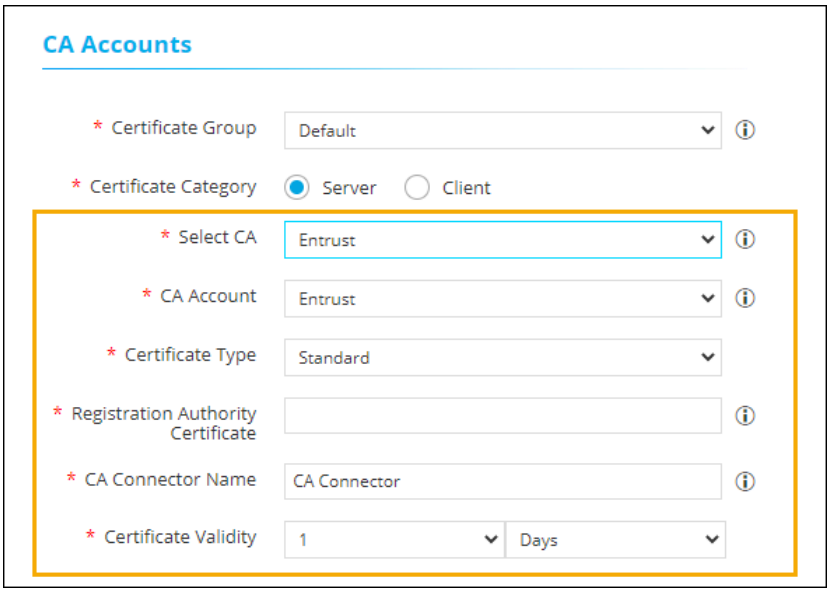
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The following table provides the field description for Vendor specific details:

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
**: Mandatory fields*	

When **Entrust** is selected as CA.



The fields for Entrust CA are as follows:

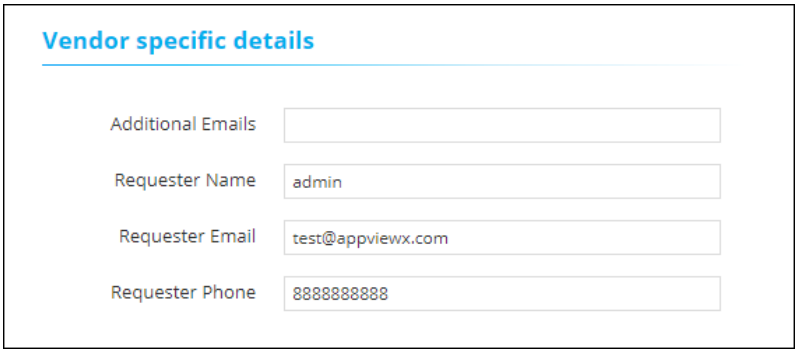
Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	Select a valid cert type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

If the selected CA is Entrust, a separate section displaying **Vendor specific details** is displayed after the **CA Accounts** section.



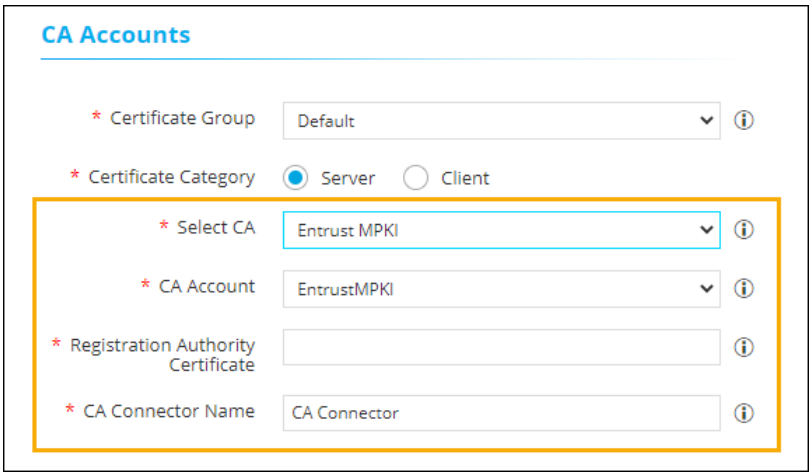
Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the demo details
Requester Email	Enter a valid email id

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Requester Phone	Enter the 10-digit phone number.
**: Mandatory fields*	

When **Entrust MPKI** is selected as CA,



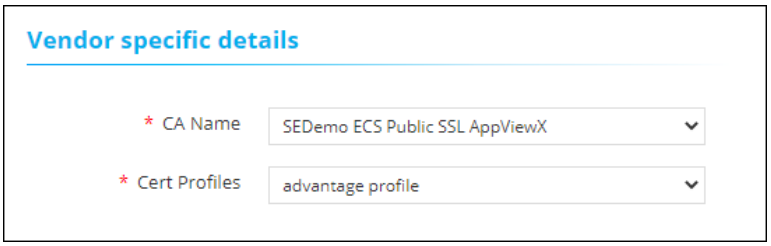
The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Entrust MPKI, a separate section **Vendor specific details** is displayed after the CA Accounts section.

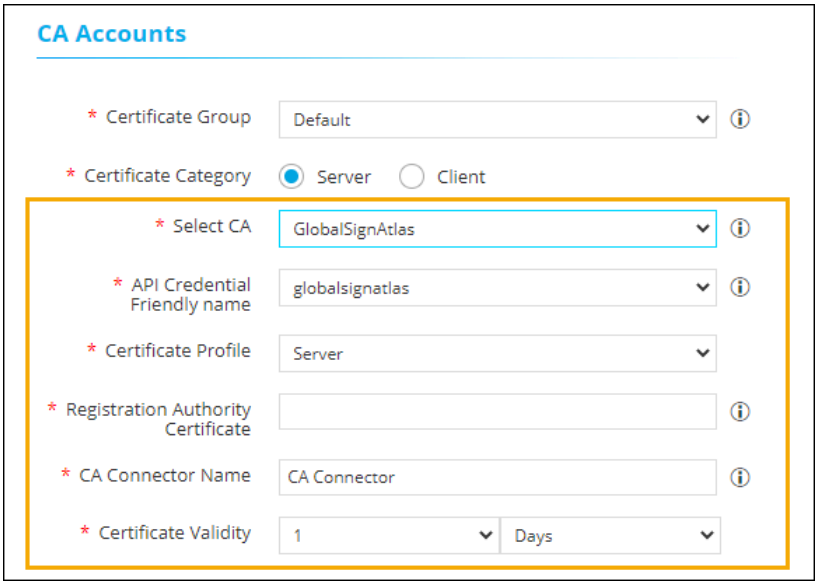
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
**: Mandatory fields*	

When **GlobalSign Atlas** is selected as CA



The fields for GlobalSign Atlas CA are as follows:

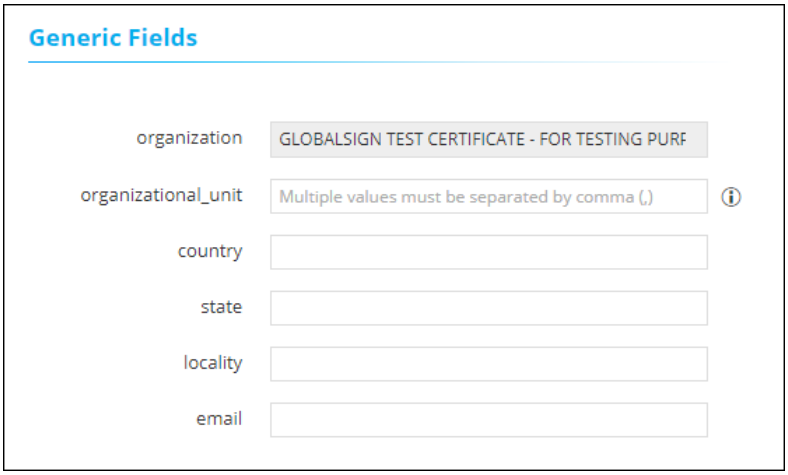
Details for GlobalSign Atlas CA - Field Description Table

Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

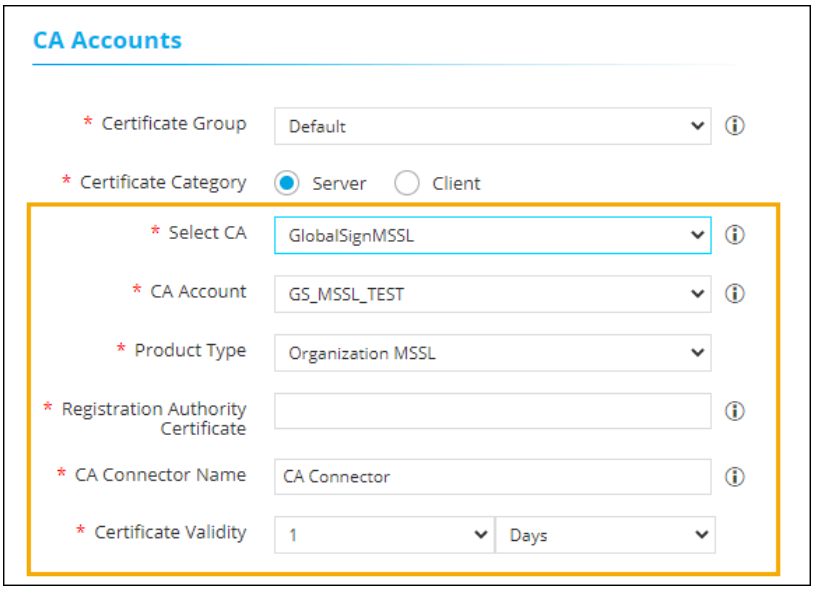
Fields	Description
Certificate Profile	Select the certificate Profile from the dropdown list.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.



When **GlobalSignMSSL** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



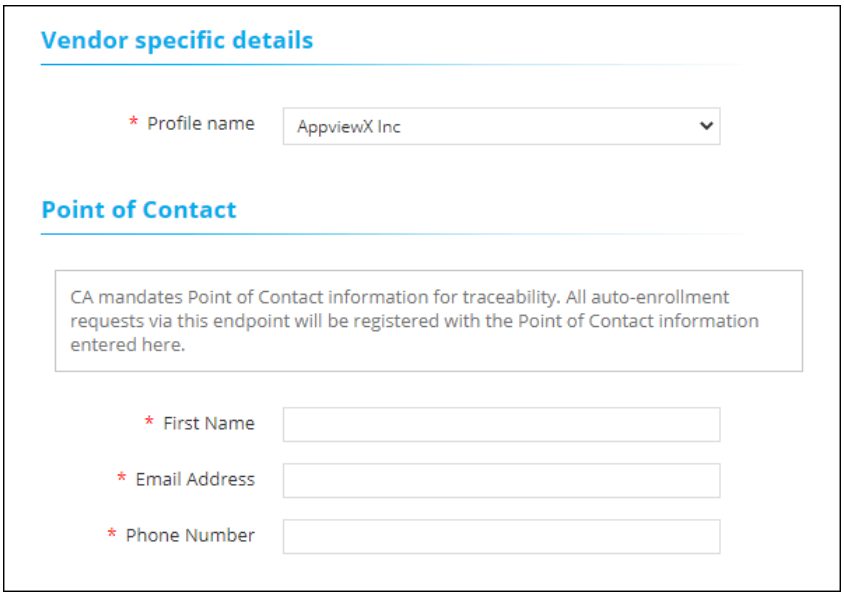
The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
**: Mandatory fields*	

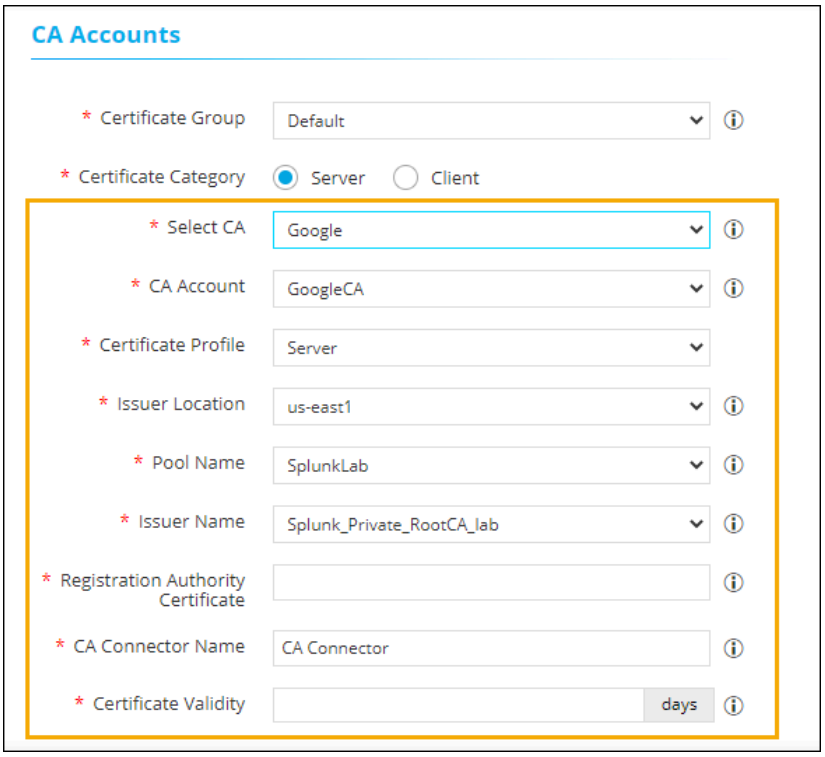
The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
**: Mandatory fields*	

When **Google** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for Google CA are as follows:

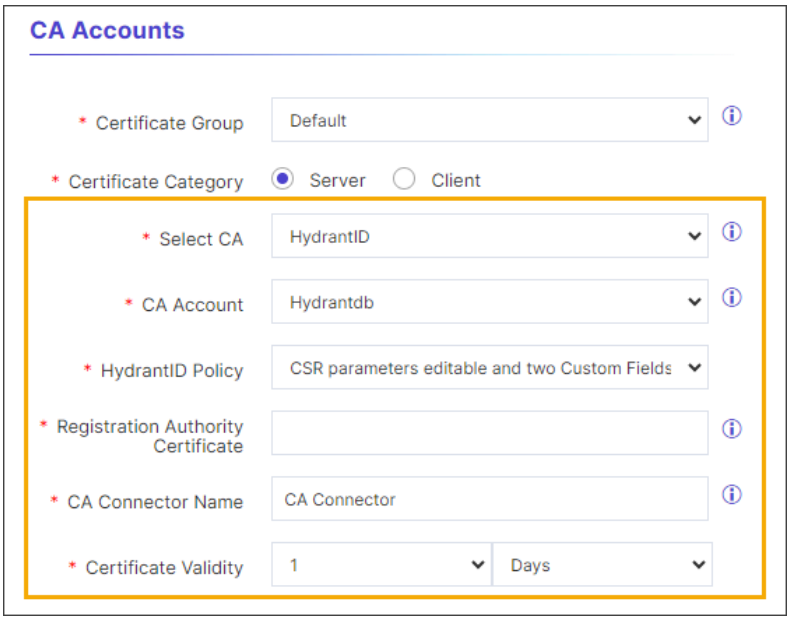
Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after certificate is being enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **HydrantID** is selected as CA,



The fields for HydrantID CA are as follows:

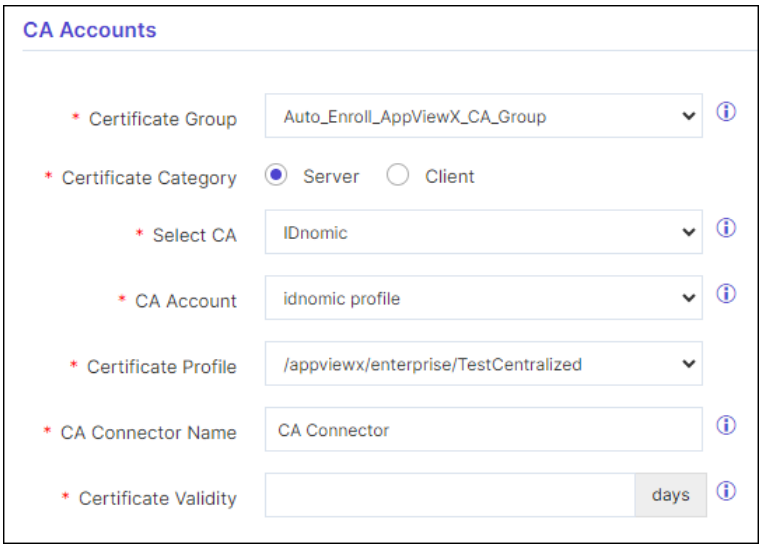
Details for Lets HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
*** CA Connector Name**	Name of the CA connector after certificate is being enrolled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **IDnomic** is selected as CA,



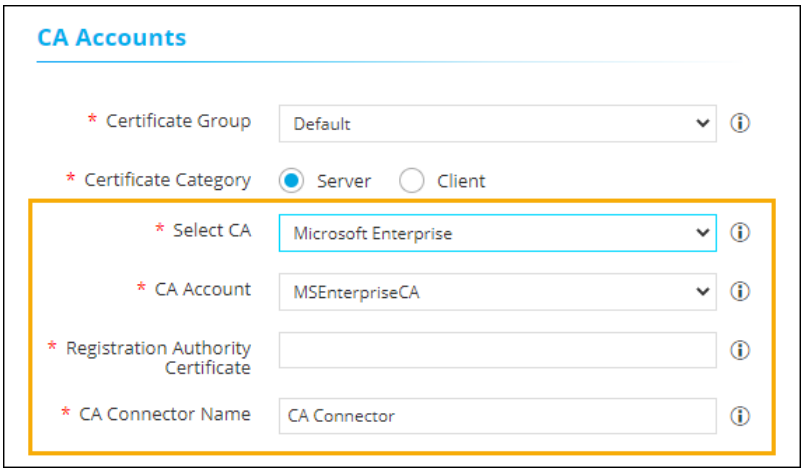
The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Microsoft Enterprise** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

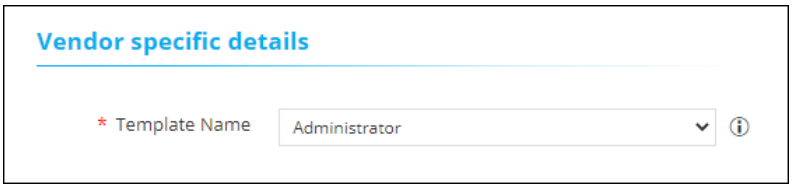


The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

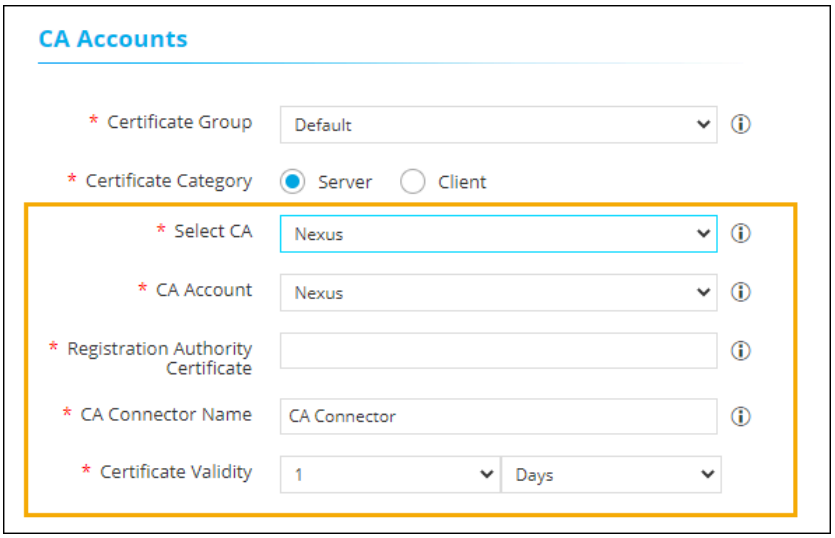
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed after the CA Accounts section. It consists of a single dropdown field **Template Name**. Select a template from the dropdown list.



The following table provides the field description for **Nexus CA**:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



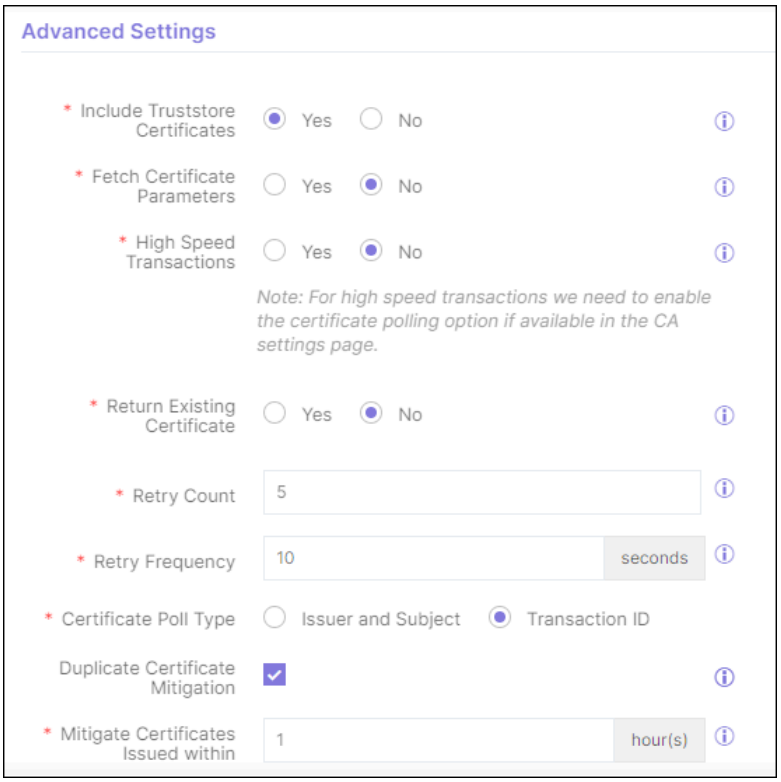
The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years).
**: Mandatory fields*	

5. Configure the **Advanced Settings** details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

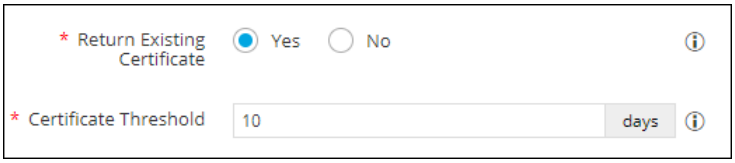


The fields in the Advanced Settings section are as follows:

Advanced Settings - Field Description Table

Fields	Description
***Include Truststore Certificates**	Select whether the issuer certificate needs to be sent to client machines after enrolment.
***Fetch Certificate Parameters**	Select Yes or No Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
High Speed Transactions	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol's Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed.  If the option is disabled (**No**) then the AppViewX will do the default behavior of enrolling a new certificate for each request.
***Retry Count**	Based on this value, the SCEP agent will trigger the number of calls to collect the certificate from AppViewX until it is received. Values accepted between 5 - 99.
***Retry Frequency**	The value specified in this field determines the duration taken between the trigger calls by the SCEP agent. Values accepted between 10 - 99.
***Certificate Poll Type**	Select *Issuer and Subject* or *Transaction ID*. The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.
Duplicate Certificate Migration	Selecting this check-box will cause the previously issued certificates for the same CSR parameters to be revoked and deleted from AppViewX.
***Mitigate Certificates issued within**	This field is enabled when the **Duplicate Certificate Migration** check-box is selected.
**: Mandatory fields*	

6. Click **Save**.

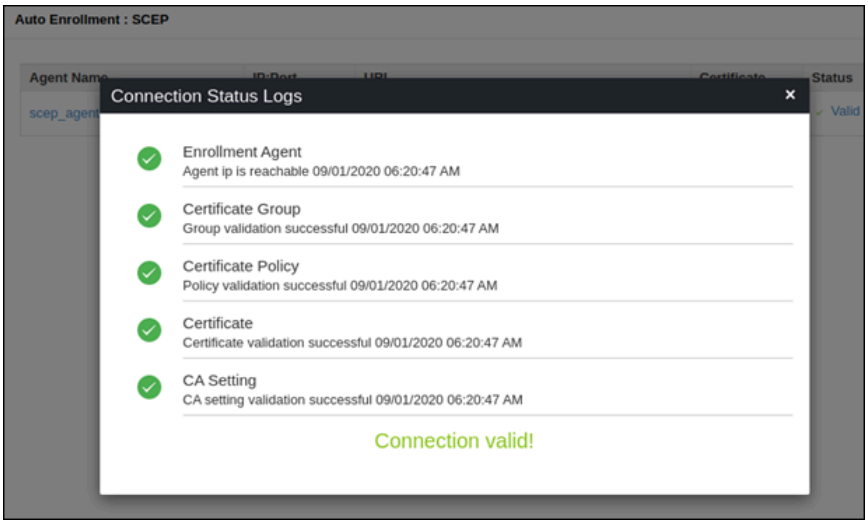
Validating SCEP

Once the SCEP settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

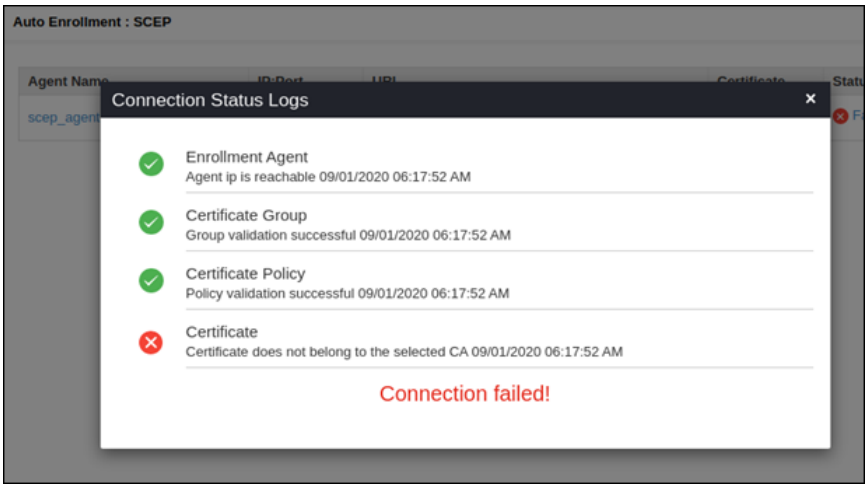
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **SCEP**.
2. On the **SCEP** page, click **Check** from the Status column to validate the SCEP setting that has been created.
   The SCEP settings will be validated and the **Status** will be shown as either **Success** or **Failure**.

Success Scenario



Failure Scenario



SCEP Enroll and Renew

The following conditions must be met, if the SCEP client sends a CSR to AppViewX SCEP Server for a certificate renewal:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. If the Signing certificate is self-signed, then validate if the subject name in the self signed certificate matches with the common name in the CSR subject.
   a. If it matches, then AppViewX will proceed with enrollment.
   b. If it doesn't match, then validate whether the challenge passphrase is configured for the endpoint and is validated by the application.

   Note: If the device enrollment uses a self-signed certificate, it is advised to configure challenge passphrase as part of the endpoint. This should be configured at the SCEP client side for any enrollment.

2. If the request is signed with an RA certificate (as configured in AppViewX SCEP endpoint) then AppViewX will proceed with the enrollment.
3. If the signer certificate is any other certificate in the inventory, then check if this certificate belongs to the same entity by doing the common name match. Check if the common name of the signer certificate and the common name in the CSR subject, if it matches, then it is considered as renewal and the certificate is issued.
4. If the signer certificate is any other certificate in the inventory and its common name doesn't match with the common name in the CSR subject, then the certificate request is rejected.

CMP

Certificate Management Protocol (CMP) is an internet protocol standardized by the Internet Engineering Task Force (IETF) used for obtaining X.509 digital certificates within a public key infrastructure (PKI). Some of the **general constraints** are as follows:

- Out-of-band distribution of authentication keys between RA and CA
  - RA / device should become a registered entity for AppViewX to accept requests from this entity
- Communication Protocol between RA and CA is SSL/TLS over TCP or HTTPS
  - Packet Exchanged are in the form of RFC 4210 and 4211 (Certificate Management Protocol and Certificate Request Message format)
  - All request and responses are digitally signed using certificate or MAC Key exchanged as challenge password
- User can be authenticated with two mechanisms:
  - SSL Certificate
  - Challenge Password
- HTTPS is the protocol used in CMP.
- Default port is 31443.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Management Protocol supports on-line interactions between PKI components. RA should be support for the following requests as per the standard:

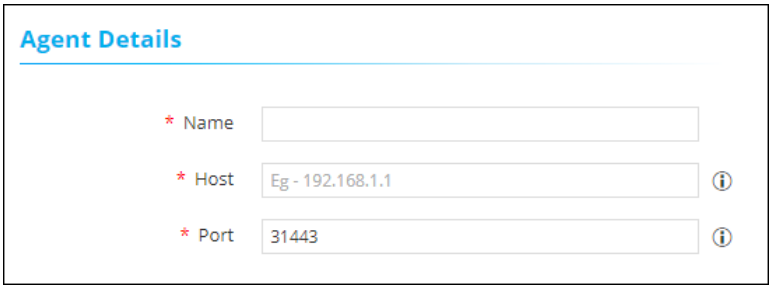
- Initialization Request and Response
- Certification Request and Response
- Renewal Request and Response
- Revocation Request and Response
- Polling Request and Response

- Configuring CMP
- Validating CMP

Configuring CMP

To set up the CMP server agent,

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **ACME**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
3. Configure the **Agent Details** as follows:



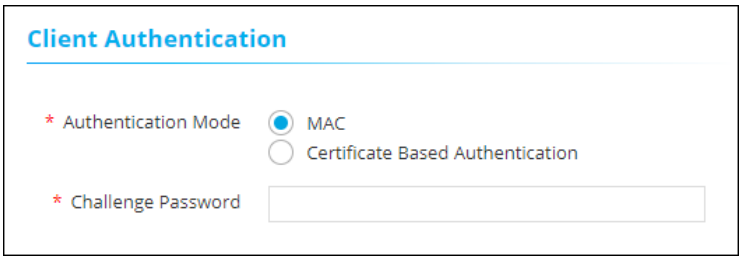
Agent Details - Field Description Table

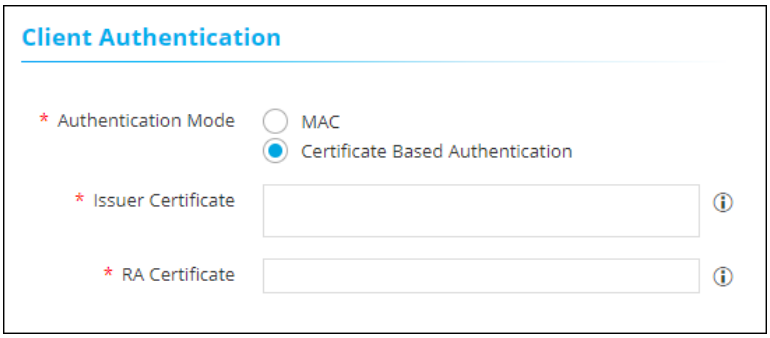
Fields	Description
***Name**	Unique name to identify the agent setting. No special characters other than '.', '-','_' are allowed. Name should not start with special characters.
***Host**	IP address of the AppViewX node gateway.
***Port**	HTTP gateway port of the AppViewX node. The default port being 31443.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Port will accept only numerical values between 0 to 65535.
**: Mandatory fields*	

4. Configure the **Client Authentication** details as follows:



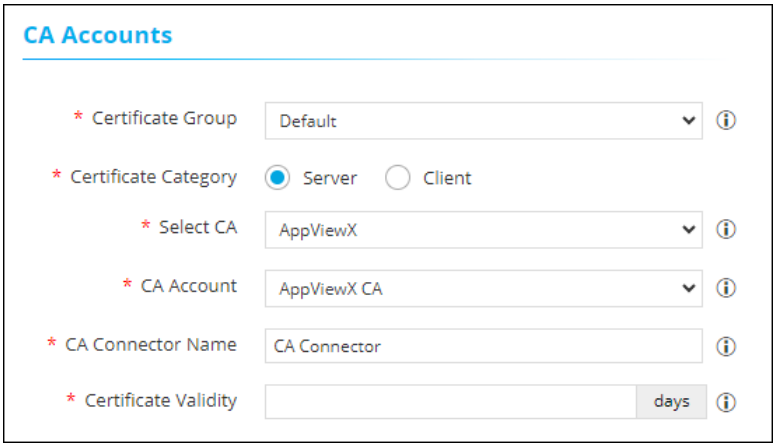


Client Authentication - Field Description Table

***Authentication Mode**	This field has two values • MAC • Certificate Based Authentication
***Challenge Password**	This field is enabled when **Authentication Mode = MAC** Enter the password which used to authenticate the CMP packet.
***Issuer Certificate**	This field is enabled when **Authentication Mode = Certificate Based Authentication** Enter the issuer certificate used to authenticate the client certificate,
***RA Certificate**	This field is enabled when **Authentication Mode = Certificate Based Authentication**Enter the common name/ serial number of the RA certificate,
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Configure the **CA Accounts** details as follows:



The fields for CA Accounts section are as follows:

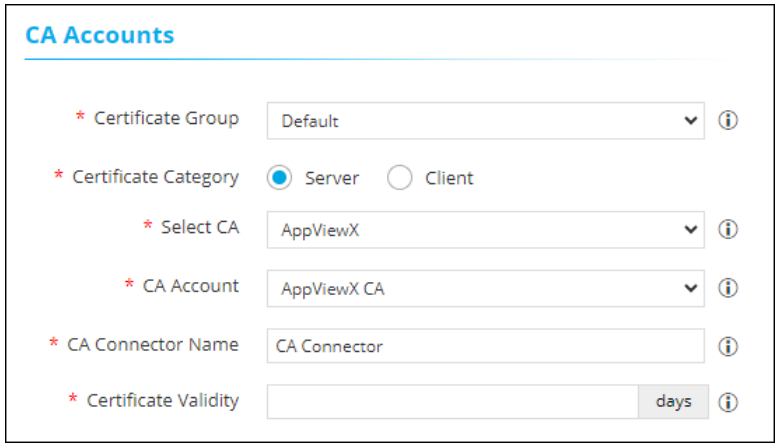
CA Accounts - Field Description Table

Fields	Description
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Certificate Category**	Select a specific certificate type (Server / Client) to be enrolled.
***Select CA**	Select the required CA from the available options: • AppViewX • AppViewX PKIaaS • Amazon Private CA • Comodo Certificate Manager • DigiCert • DigiCert MPKI • Ejbca • Entrust • Entrust MPKI • Globalsign • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• Nexus • OpenTrust The certificate will be enrolled under the selected CA.
**: Mandatory fields*	

When **AppViewX** is selected as CA,



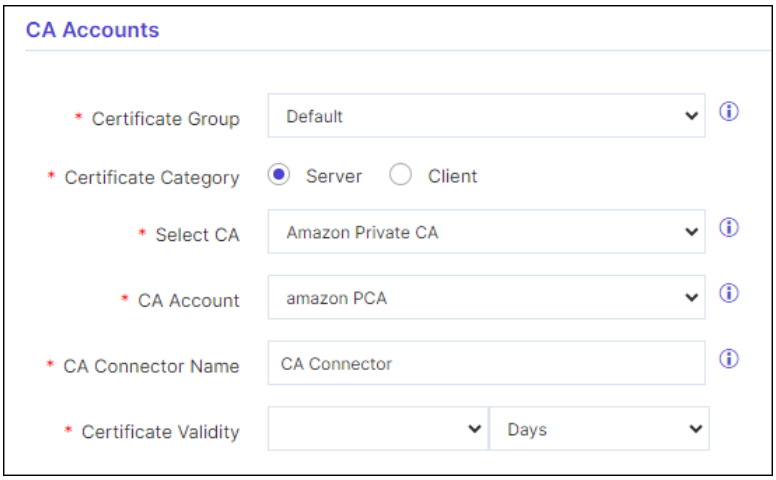
The fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Amazon Private CA** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

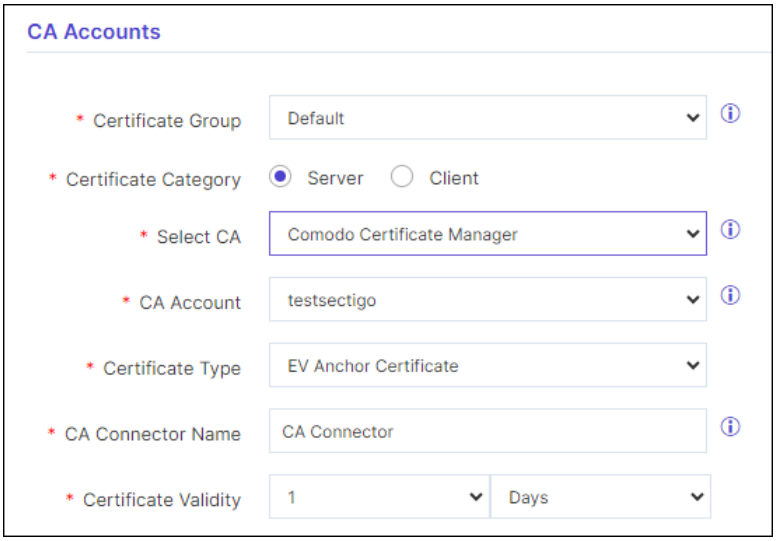


The fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **Comodo Certificate Manager** is selected as CA,



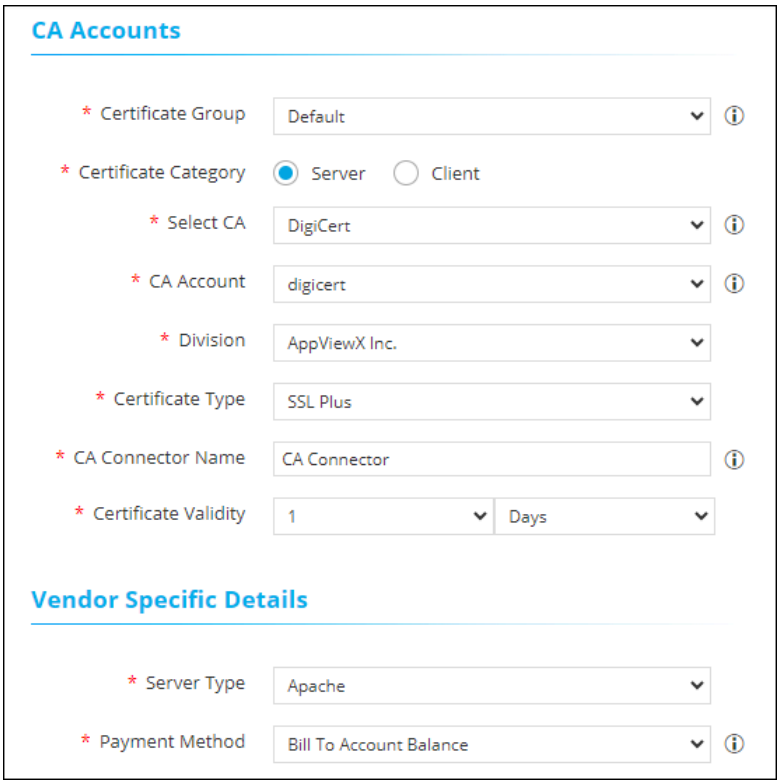
The fields for Comodo Certificate Manager CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for Comodo Certificate Manager CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Cert Type**	Select certificate type to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

When **DigiCert** is selected as CA,



The fields for DigiCert CA are as follows:

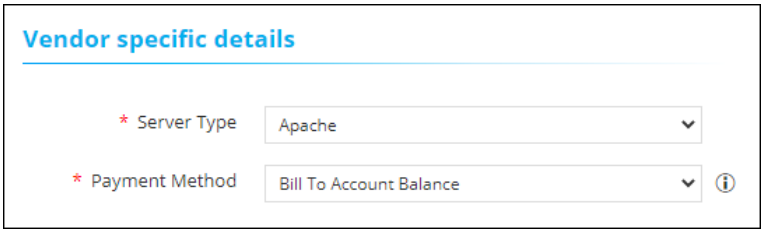
Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Division**	Select the division associated with the CA account.
***Cert Type**	Select certificate type to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
**: Mandatory fields*	

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.



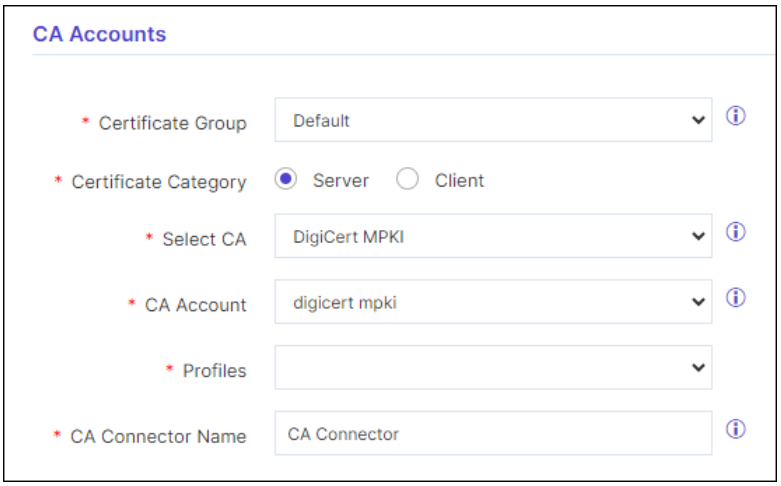
The fields for Vendor specific details are as follows:

Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
**: Mandatory fields*	

When **DigiCert MPKI** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for DigiCert MPKI CA are as follows:

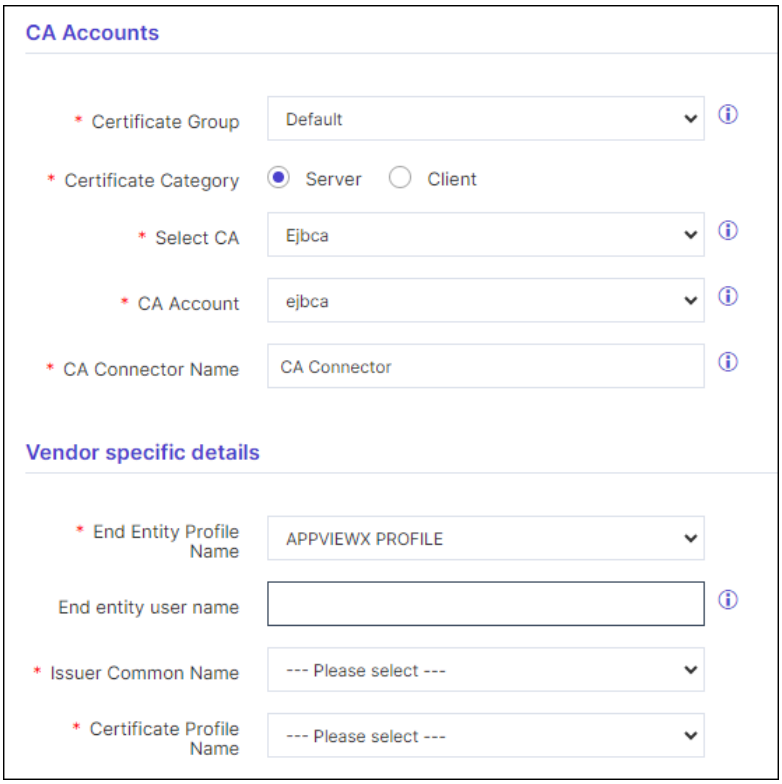
Details for DigiCert MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Profiles**	Select a profile associated with the CA account.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

Note: Based on the DigiCert MPKI account configuration Custom Attributes section may also be displayed on the endpoint configuration page.

When **EJBCA** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section.The fields for Vendor specific details are as follows:

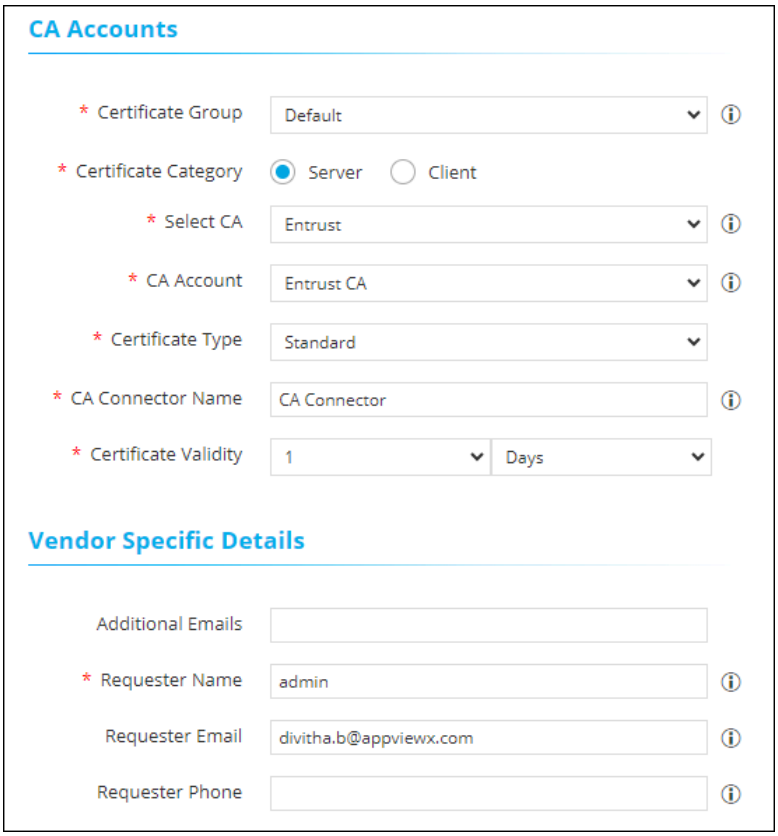
Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Profile Name**	Select a profile name of certificate.
**: Mandatory fields*	

When **Entrust** is selected as CA,



The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select a valid cert type associated with the CA account. If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

If the selected CA is Entrust, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section.

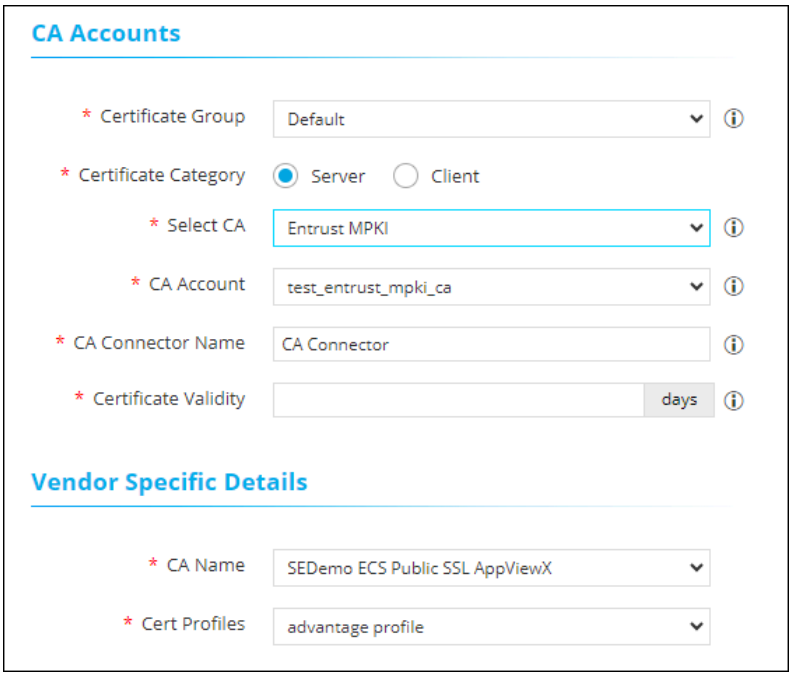
Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the demo details
Requester Email	Enter a valid eamil id
Requester Phone	Enter the 10-digit phone number.
**: Mandatory fields*	

When **Entrust MPKI** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

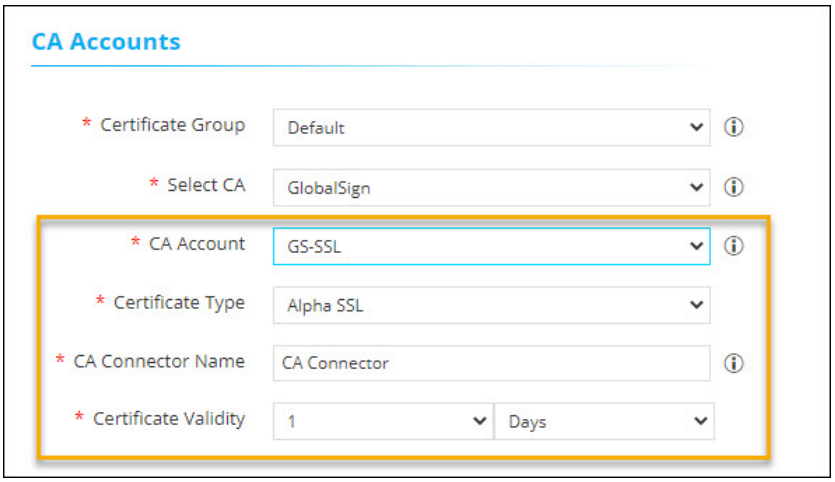
If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The following table provides the field description for Vendor specific details:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
**: Mandatory fields*	

When **GlobalSign** is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

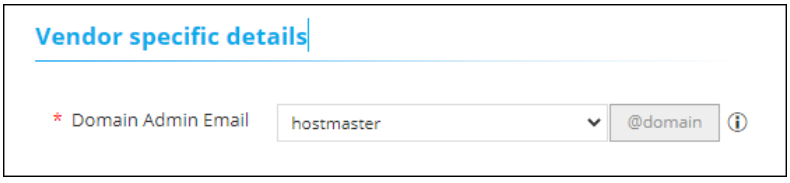


The fields for GlobalSign CA are as follows:

Details for GlobalSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Alpha SSL or Domain SSL**



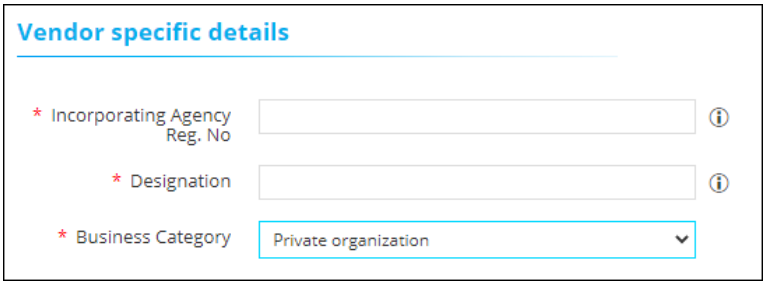
Vendor Specific Details for GlobalSign CA - Field Description Table

Fields	Description
***Domain Admin Email**	Select the email id to receive the approval requests from GlobalSign CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

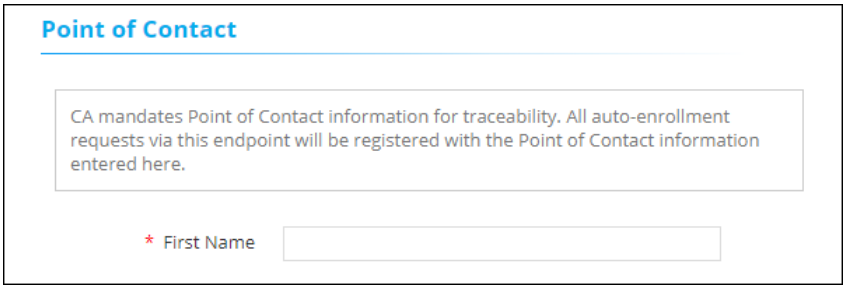
The following fields are displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Extended SSL**



Vendor Specific Details for GlobalSign CA - Field Description Table

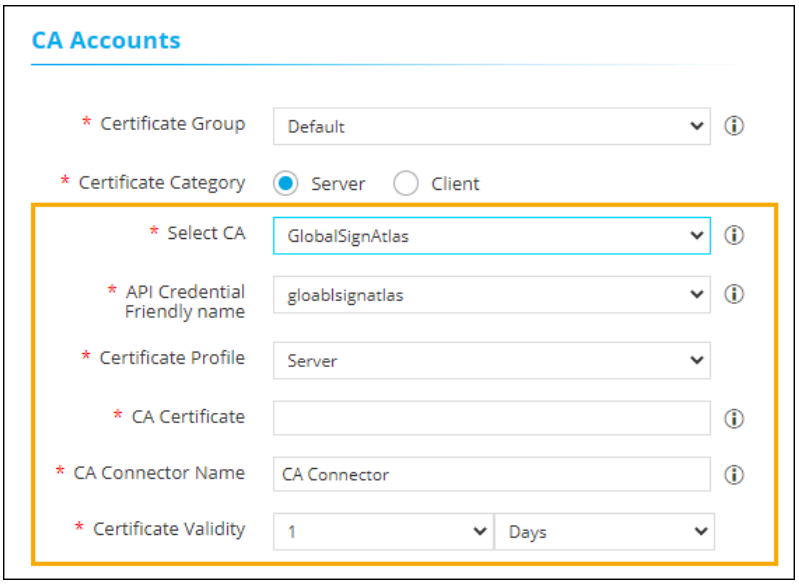
Fields	Description
***Incorporating Agency Reg. No**	Enter the Registration number of the incorporating agency.
***Designation**	Enter the designation of the requester.
***Business Category**	Select the type of business (private org., government entity, or business entity
**: Mandatory fields*	

:The following field is displayed in the **Point of Contact** section as per the selected CA if the **Select CA =GlobalSign**, and the **Certificate type = Organization SSL** . The CA mandates the point of contact information (**First Name**) for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.



When **GlobalSign Atlas** is selected as CA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



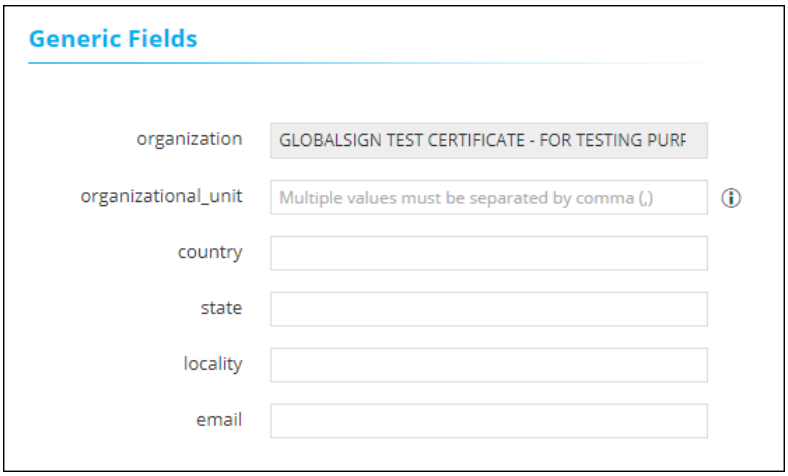
The fields for GlobalSign Atlas CA are as follows:

Details for GlobalSign Atlas CA - Field Description Table

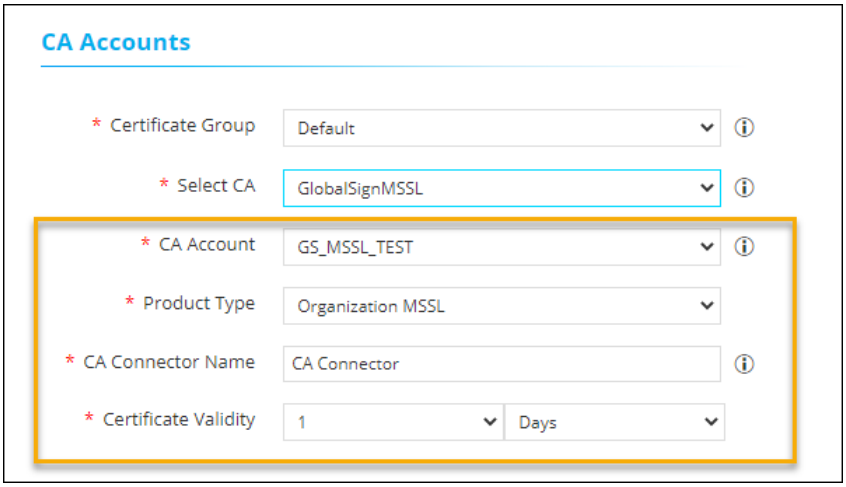
Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)
**: Mandatory fields*	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



When **GlobalSign MSSL** is selected as CA.



The fields for GlobalSign MSSL CA are as follows:

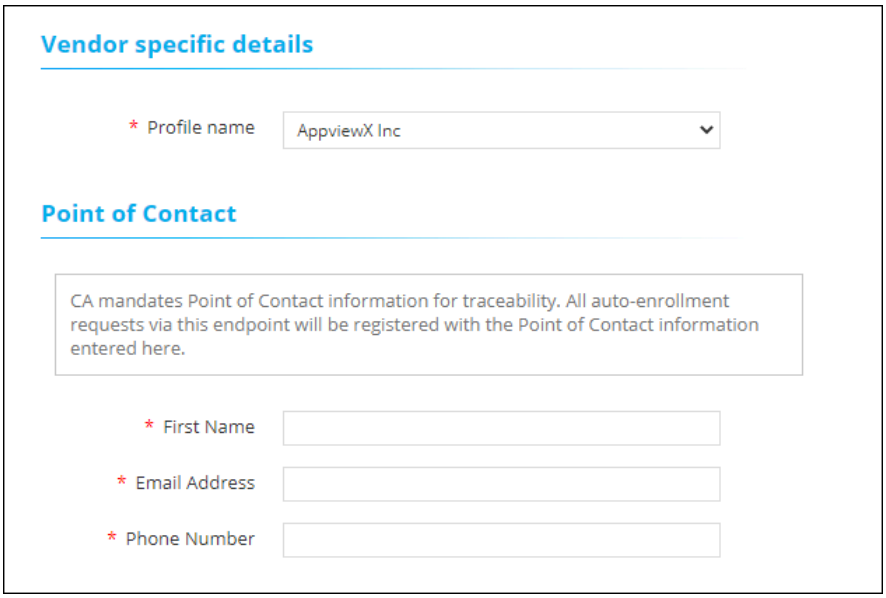
Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

The following field is displayed in the **Vendor Specific Details** and **Point of Contact** section as per the selected CA:



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
**: Mandatory fields*	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.

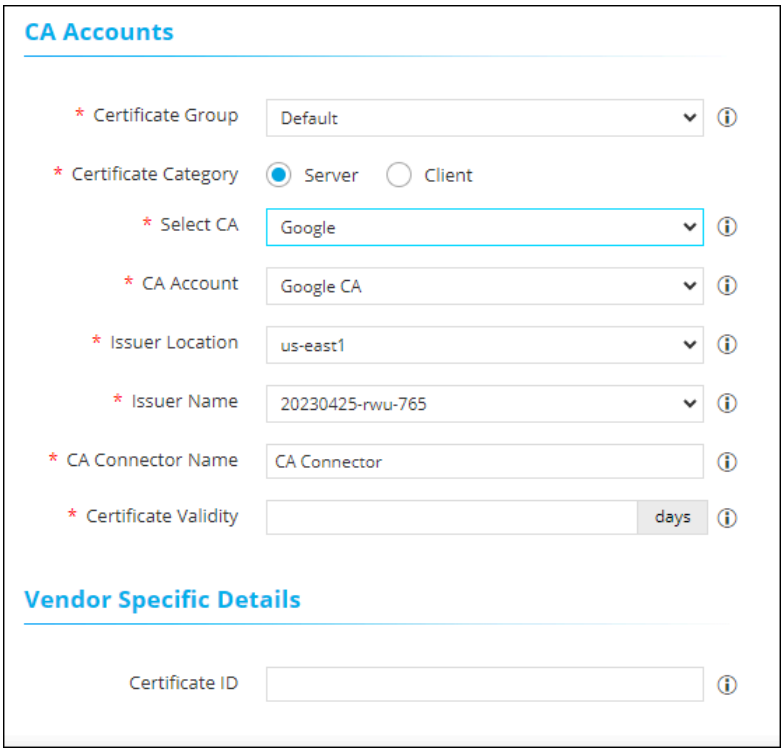
Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Phone Number**	Enter the valid phone number.
**: Mandatory fields*	

When **Google** is selected as CA,



The fields for Google CA are as follows:

Details for Google CA - Field Description Table

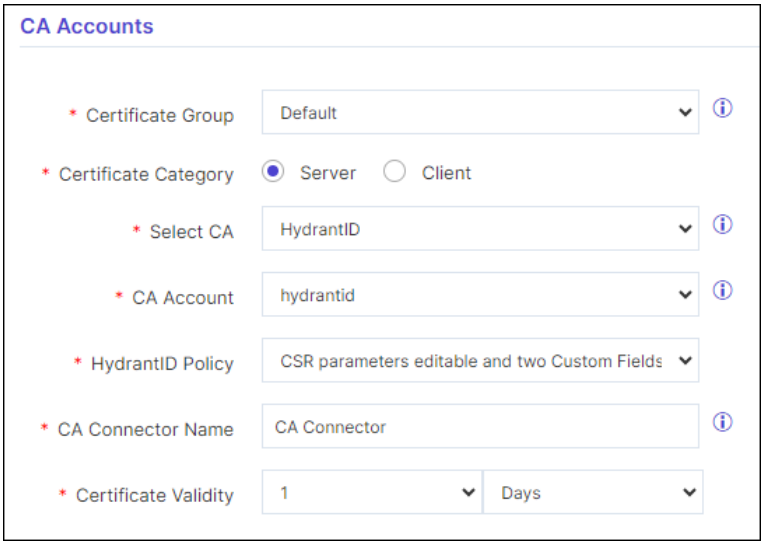
Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Issuer Location**	Select the issuer location associated with the CA account.
***Issuer Name**	Select a issuer name to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for Vendor Specific details are as follows:

Field Name	Description
Certificate ID	Enter the valid certificate id.

When **HydrantID** is selected as CA,



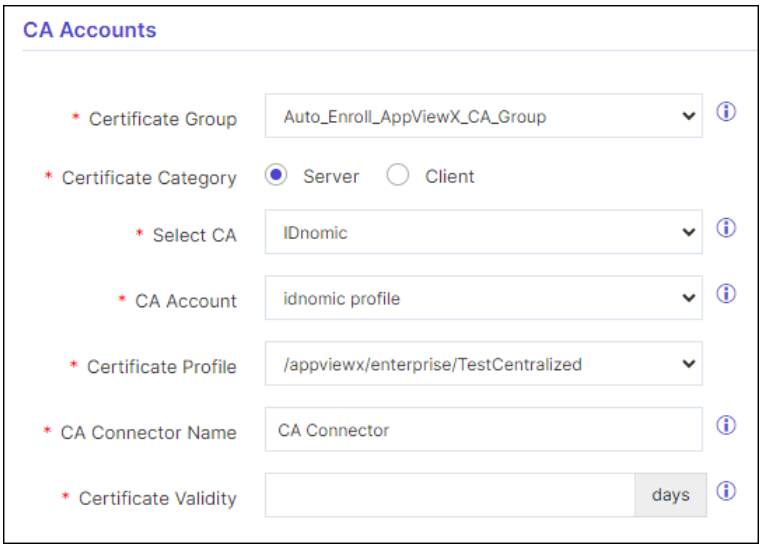
The fields for HydrantID CA are as follows:

Details for Lets HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **IDnomic** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



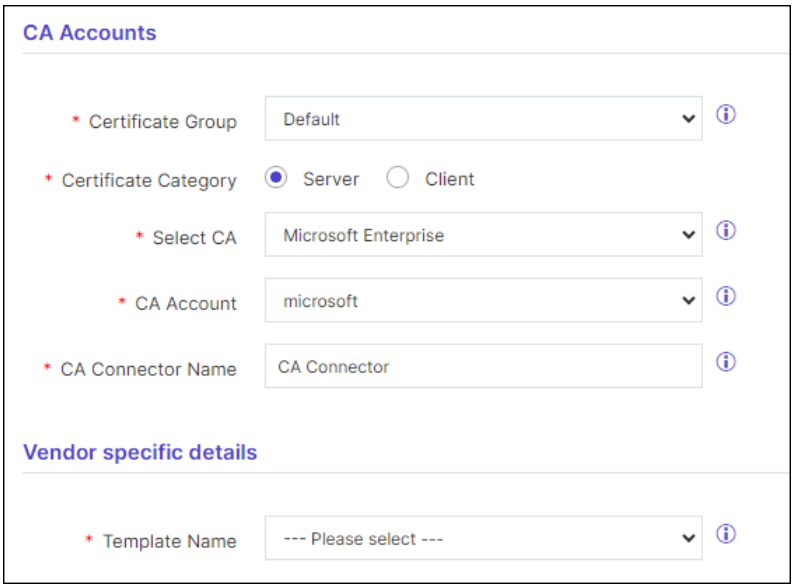
The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

When **Microsoft Enterprise** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

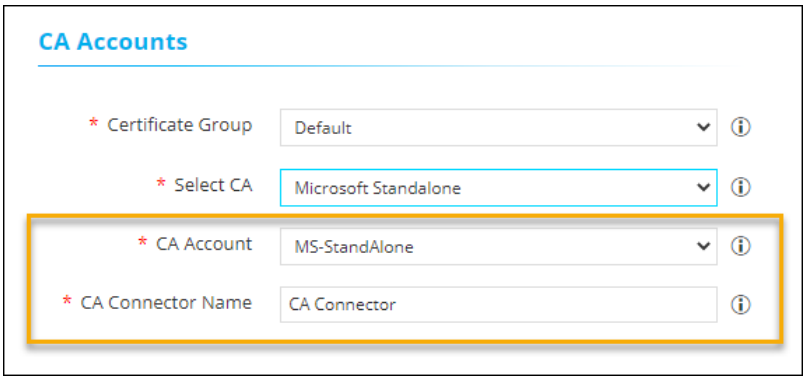
If the selected CA is Microsoft Enterprise, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section.

Vendor Specific Details - Field Description Table

Fields	Description
***Template Name**	Select the desired template name. This value is based on the policy setting and its group association.
**: Mandatory fields*	

When **Microsoft Standalone** is selected as CA,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

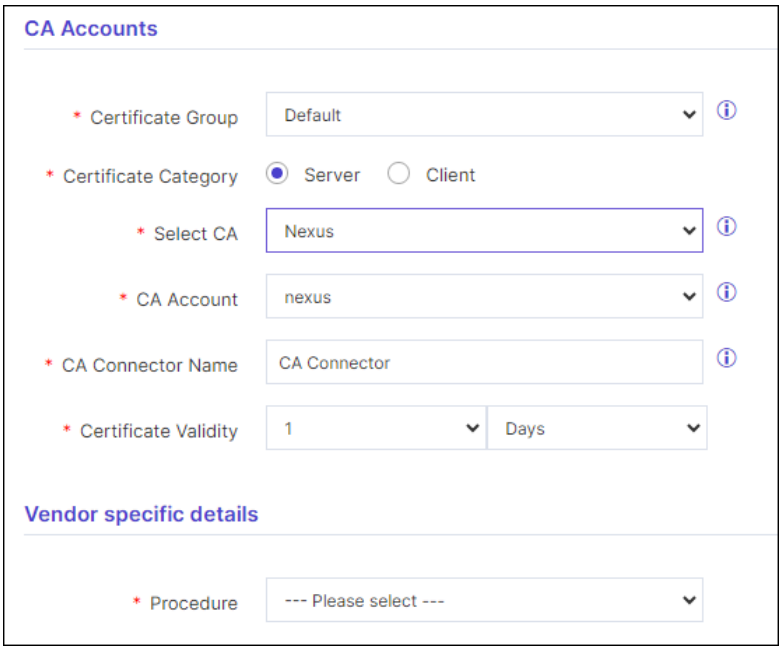


The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

When **Nexus** is selected as CA.



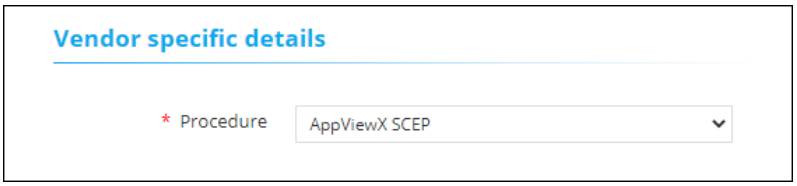
The fields for Nexus CA are as follows:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
**: Mandatory fields*	

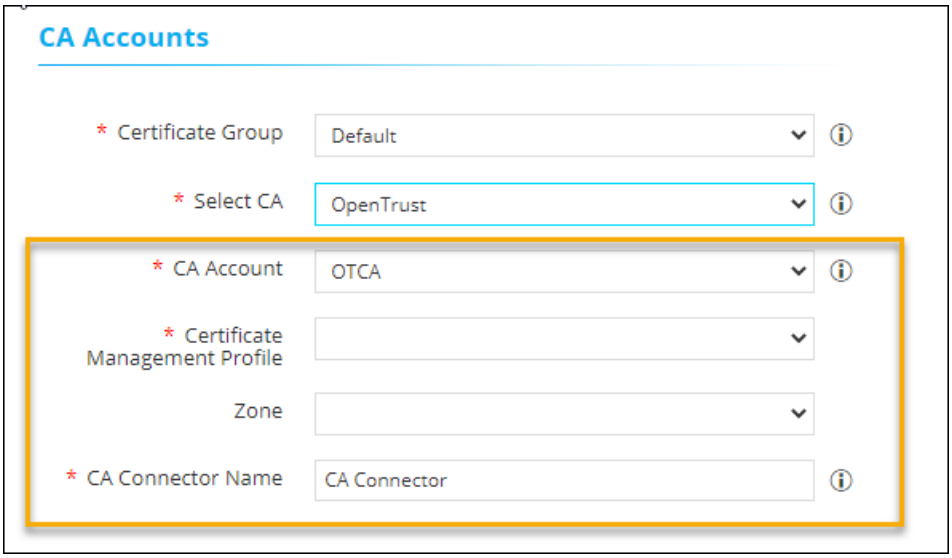
The following field is displayed in the **Vendor Specific Details** section as per the selected CA:



Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the Procedure based on the configurations made in the Certificate Authority Setting.
**: Mandatory fields*	

When **OpenTrust** is selected as CA.



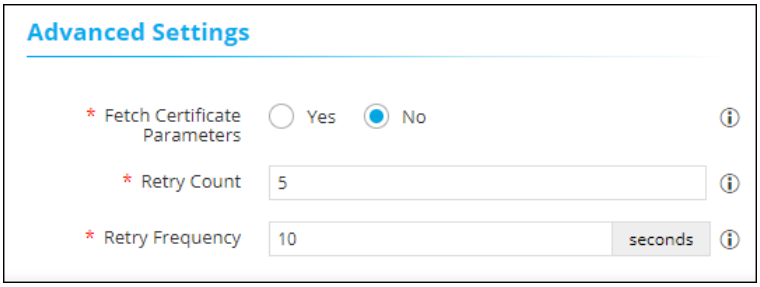
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The fields for OpenTrust CA are as follows:

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Management Profile**	Select one issuer certificate from the dropdown list. This issuer certificate will be used for signing the CSR by the certificate authority. **Note:** Only the issuer certificates available in the root or intermediate certificates inventory will be shown for selection.
Zone	Select the zone pertaining to the Certificate Management Profile
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
**: Mandatory fields*	

6. Configure the **Advanced Settings** section as follows:



The following table provides the field description for the Advanced Settings section:

Advanced Settings - Field Description Table

Fields	Description
***Fetch Certificate Parameters**	Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

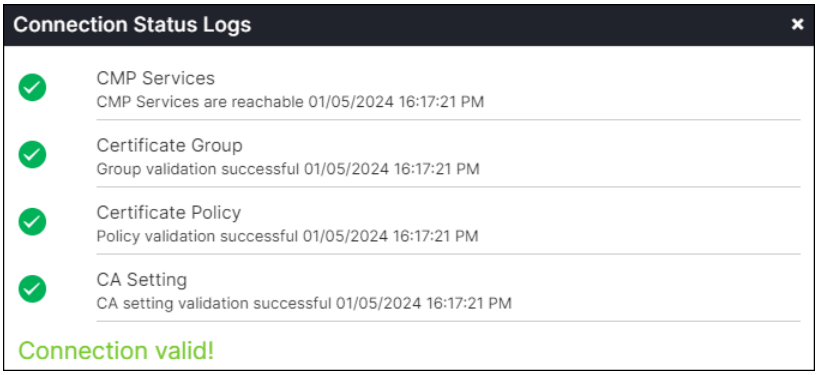
Fields	Description
***Retry Count**	Specify a retry count up to which the agent will retry for the certificate to be fetched.
***Retry Frequency**	Specify a retry frequency up to which the agent will wait for each retry count.
**: Mandatory fields*	

Validating CMP

Once the CMP settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Auto Enrollment** > **SCEP**.
2. On the **CMP** page, click **Check** from the Status column to validate the CMP setting that has been created.
   The CMP settings will be validated and the **Status** will be shown as either **Success** or **Failure**.

   Success Scenario



EST Client Authentication in Cloud Connectors

This section describes the steps to replace the Default TLS Certificate with Signed Certificate and to add a CA issuer certificates for EST client authentication in CC (Cloud Connector).

By default, AppViewX provides a default certificate in the gateway. For ACME you must bind a valid certificate (Certificate with CC hostname) with the gateway.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To bind a TLS certificate to gateway :

- • The certificate's common name must be the hostname of the CC.
  • Download the certificate with .crt format and key file.

By default, AppViewX cloud connector will only allow the AppViewX CA issued certificates for client authentication. The cloud connector gateway will not allow the other CA certificates for client authentication.

To add other CA issuer certificates for EST client authentication:

- Download the required issuer certificates in .crt format

To update the certificate:

1. Copy the certificate and key file to <cc_installation_folder>/deps/properties/ directory.
2. Navigate to the **cc_installation_folder** and execute the below command

   ```
   /avxctl upgrade gateway-cert
   ```

3. you will be prompted with the question `Do you want to bind a SSL certificate to gateway? (y/n):`

   a. To bind a certificate to gateway enter **y**.

   b. You will then be asked for the *certificate path* and the *key path*. Provide the relative path of the files as indicated below
   If the certificate and key file is copied into <cc_installation_folder>/deps/properties/ folder then the path should be
   - *Please enter the certificate file path:* `/properties/test.crt`
   - *Please enter the key file path:* `/properties/test.key`

   c. If this step is not required please enter **n**.

4. You will now be prompted with `Do you want to add trusted CA certificates for mTLS authentication for EST? (y/n):`

   a. To give the the issuer certificate list of the client certificate used in EST enter **y**.

   b. You will then be asked for the *certificate path*. You may give more than one certificate path using comma (,).
   If the issuer certificate are copied into <cc_installation_folder>/deps/properties/ folder then the path should be

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- *Please provide comma separated values of the certificate file path:* /properties/test.crt

c. If this step is not required please enter **n**.

5. Wait for the script to complete and the gateway will be upgraded.

```
[appviewx@pe-pltf-node46 cert-upgrade-test]$ ./avxctl upgrade gateway-cert
Do you want to bind a SSL certificate to gateway? (y/n) : y
Please enter the certificate file path
/properties/test.crt
Please enter the key file path
/properties/test.key
Do you want to add trusted ca certificates for mTLS authentication for EST? (y/n) : y
Please provide comma separated values of the certificate file path
/properties/Splunk_Private_IssuingCA.crt,/properties/Splunk_Private_RootCA.crt,/properties/AppViewX-AWS-RootCA.crt,/properties/AppViewX-AWS
A.crt

Upgrading Gateway ...
**************************************************

Check if previous version of gateway exists
uninstalling previous version...
release "avx-mid-server-gateway" uninstalled
Updating gateway profile
Loading required certificates for gateway...
Running helm upgrade for gateway...
Release "avx-mid-server-gateway" does not exist. Installing it now.
NAME: avx-mid-server-gateway
LAST DEPLOYED: Mon Sep 11 13:34:52 2023
NAMESPACE: cc
STATUS: deployed
REVISION: 1
TEST SUITE: None
HELM INSTALL SUCCESS
Gateway Upgrade Successful

**************************************************
```

Note: When there a LB (Load Balancer) on top of the cloud connectors follow the basic prerequisites below:

- A valid certificate should be bound to the LB (Certificate with LB's hostname)
- LB should not block the client authentication certificate in the request

Direct Requests

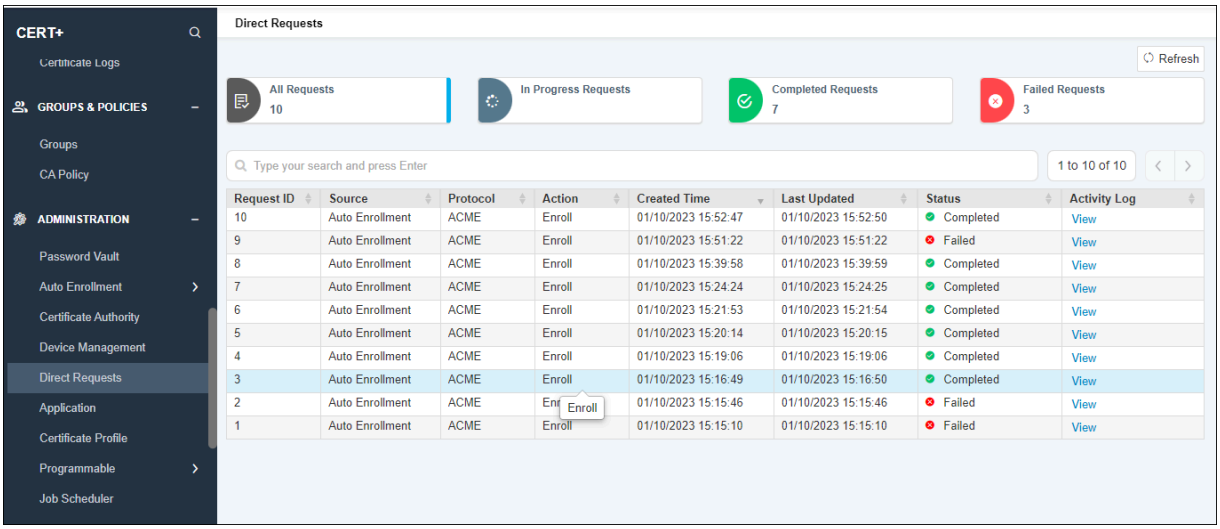
The Direct Request page lists the auto-enrollment certificate requests for which the visual workflow will not be displayed for generating the certificates, resulting in a greatly improved performance. This page only displays the status and other details of certificate requests. No actions can be performed on this page.

Note: While creating an auto-enrollment request (for EST, ACME, SCEP, MS INTUNE), in the **Advanced Setting** section , select the radio button in **High Speed Transaction** field to "Yes" to display the requests in the Direct Requests page.

Accessing the Direct Request Page

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

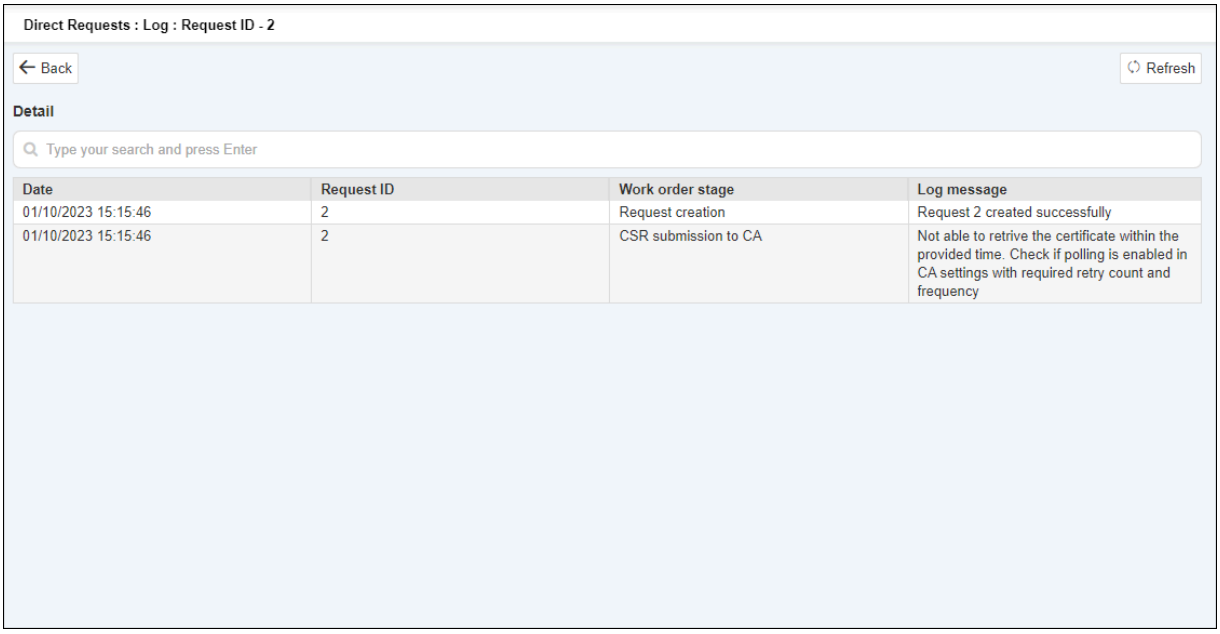
1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Direct Requests** .



2. The Direct requests page displays the following:
   - **Echelons** - All requests, In Progress Requests, Completed Requests, and Failed Requests. all echelons have the count of requests and are clickable. Clicking each echelon will display only those specific status requests.
   - **Refresh** button
   - **Search** field - users can enter values w.r.t. Request ID, Time Created, Request Status, CLM Action to search/filter for specific requests.
   - Grid with the following columns -
     - *Request ID* - displays ID of the current request
     - *Source* - displays the source type, usually Auto Enrollment
     - *Protocol* - displays the type of protocol (EST, ACME, SCEP, MS INTUNE)
     - *Action* - displays the latest CLM action on the request
     - *Created Time* - displays the time the request was created
     - *Last Updated* - displays the time the request was last updated
     - *Status* - displays the status of the certificate request
     - Activity *Log* - displays the “View” link, when clicked displays the detailed logs at each status for the certificate request cycle.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

An example of a failed request log is displayed below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 3: CERT+ API Guide

This guide informs you about the APIs to be used for different CLM actions.

- Login to AppViewX
- Create a Certificate in Async mode
- Create a Certificate in Sync mode
- Renew a Certificate in Async mode
- Renew a Certificate in Sync mode
- Revoke a Certificate in Async mode
- Revoke a Certificate in Sync mode
- Reissue a Certificate in Async mode
- Reissue a Certificate in Sync mode
- Regenerate a Certificate in Async mode
- Regenerate a Certificate in Sync mode
- Suspend a Certificate
- Reinstate a Certificate
- Search/ Get Certificate Inventory
- Add Certificate Attributes
- Update Certificate Attributes
- Get Certificate Attributes
- Delete Certificate Attributes
- Download a Certificate
- Download a Certificate by Format
- Common Response Objects
- Push and Bind Certificate to a Firewall Profile
- Rollback certificate to firewall profile
- Get Available Server Profiles
- Push and Bind Certificate to a server profile
- Rollback Certificate to server profile
- After you are done
- Download Private Key of a Certificate
- Delete Certificate using UUID

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- CERT+ ADC API
- Discover Certificates from Firewall
- Discover Certificates from Server
- HP iLO Vendor Integration via REST Interface

Login to AppViewX

Authenticate into the AppViewX application with the username and password.

Request Structure

URL: */login*

Type: `POST`

Parameters

Param Type	Name	Description	Field Type	Constraints
Header	`username`	AppViewX login username	`String`	NA
Header	`password`	AppViewX login password	`String`	NA
Header	`Content-Type`	Specifies the nature of the data in the payload.	`String`	Value of the param should be '**application/json**'
Query	`gwkey`	Tenant Key. Needed only in case of multi-tenant installations	NA	NA
Query	`gwsource`	Source from which the request is triggered (for example: web, external)	`String`	NA

Response Structure

200 OK, returns a string of type application/JSON with the following body params:

Body Parameters

Name	Description	Field Type
`response`	Contains the response for the session activation with the authentication/ session ID.	`Key Value Pair`

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Body Parameters (continued)

Name	Description	Field Type
message	Success message along with the objectIds or failure description in case of error.	String
appStatusCode	Application-specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	Key value pair

Status Codes

Status Codes and Description

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK	-	Login successful	NA
400 Bad request		Username or password cannot be null or empty	Check and ensure if a non-null/non-empty value is given in the header field for username or password
401 Unauthorized		Login failed. Invalid credentials.	Check and ensure if the username and password provided are valid and correct.

Sample Request/Response

Use Case

Login to the application with the username appviewxuser and password appviewxpassword. The session id received as response in the example below is ce7f1a14-2bf9-4e4a-89a8-bc780a255813

Sample Response


```
{
"response":
{
 "status":"SUCCESS",
 "appStatusCode":null,
 "statusDescription":null,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"sessionId":"ce7f1a14-2bf9-4e4a-89a8-bc780a255813",
"availableLoginAttemptCount":null
},
"message":null,
"appStatusCode":null,
"tags":null,
"headers":null
}
```


Related reference
Create a Certificate in Async mode
Create a Certificate in Sync mode

Create a Certificate in Async mode

The API initiates the creation of a new certificate in async mode. This mode requests certificate generation and provides a request ID in the response. The request payload varies depending on the Certificate Authority (CA) used for enrollment. After successfully triggering the create certificate API, the response includes the resourceId, which can be used to activate the search API and retrieve the created certificate. Please refer to the After you are done section for instructions on approving and implementing the request.

Before you begin

Ensure the following before attempting to enroll a certificate from a particular CA through AppViewX:

- The CA must configured in AppViewX from the CA settings page.
- Connectivity to the CA via the chosen setting should be working fine.
- A certificate group is created and associated with the policy. If not, the certificate will be created under the Default group.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/create
Type:	POST

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample URL:
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
csrGenerationSource	(Optional) Specifies where the CSR is to be generated. **Type**: **Possible values:**: AppViewX, Endpoint, HSM, uploadCSR. The default value is **AppViewX**
caConnectorInfo	(Mandatory) Details related to the certificate authority (CA) and the CSR parameters. **Type**: Any of the following data: • Amazon caConnectorInfo • AppViewX caConnectorInfo • DigiCert caConnectorInfo • EJBCA caConnectorInfo • Entrust caConnectorInfo • EntrustMPKI caConnectorInfo • GlobalSign caConnectorInfo • GoDaddy caConnectorInfo • Google caConnectorInfo • InCommon caConnectorInfo • LetsEncrypt caConnectorInfo • Microsoft Enterprise caConnectorInfo • Microsoft Standalone caConnectorInfo • OpenTrust caConnectorInfo • Sectigo caConnectorInfo • Symantec caConnectorInfo • Trustwave caConnectorInfo
certificateGroup	Specifies the group (category) to which the newly created certificate should be assigned. **Type**: certificateGroup **Constraint**: Default certificate Group is "**Default**".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
deviceDetails	(Optional) Information about the device or endpoint where the Certificate Signing Request (CSR) will be generated. **Type**: deviceDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **Endpoint**.
certificateHSMDetails	(Optional) Information about the Hardware Security Module (HSM) device. **Type**: certificateHSMDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **HSM**.
uploadCsrDetails	(Optional) Information about the CSR. **Type**: uploadCsrDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **uploadCSR**.
certificateFormat	(Optional) Certificate download format details. **Type**: certificateFormat

certificateGroup

Name	Mandatory
name	(Optional) Specifies the group under which the created certificate needs to be tagged. **Type**: String **Constraint**: The certificate group must be present in AppViewX.

deviceDetails

Name	Mandatory
category	(Mandatory) Specifies the device category **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

deviceDetails (continued)

Name	Mandatory
	Possible values: ADC, Server, and Firewall.
vendor	(Mandatory) Name of the vendor for the chosen device. For example, **Apache** is a vendor for **Server** category. **Type**: String
deviceName	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
csrFileName	(Mandatory) Name of the CSR file that is generated in the device. **Type**: String
keyFileName	(Mandatory) Name of the key file that is generated in the device. **Type**: String
attributes	(Optional) Additional attributes for the chosen device as mentioned the sub-attributes - csrLocation, tenant, and partition. **Type**:
csrLocation attributes	(Optional) The location within the device where the CSR is generated. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Server** and the **deviceDetails.vendor** is **Tomcat**.
tenant attributes	(Optional) Name of the partition within the AVI device. **Type**: String
partition attributes	(Optional) Name of the partition within the device. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Friewall** and the **deviceDetails.vendor** is **Fortinet**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateHSMDetails

Name	Mandatory
type	(Mandatory) Type of the HSM device. **Type**: String **Possible values**: ADC and HSM.
keyReference	(Mandatory) Reference name for the key that is mapped by the HSM device. **Type**: String
hsmSettings	(Mandatory) Configuration details for the HSM device. Contains the sub-parameters vendorType and vendorSpecificSettings **Type**: List <String>
vendorType hsmSettings	(Mandatory) Category of the vendor. **Type**: String **Possible values**: Safenet, Thales, and Fortanix.
vendorSpecificSettings hsmSettings	(Mandatory) Settings related to HSM vendor. Contains the sub-parameter moduleId **Type**: String
moduleId hsmSettings. vendorSpecificSettings	(Optional) The module id. **Type**: String **Constraints**: Applicable if **hsmSettings.vendorType** is **Thales**.
vendor	(Mandatory) The name of the vendor for the chosen device e.g., F5. **Type**: String
deviceName	(Mandatory) The name of the device as per AppViewX Device Inventory. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

uploadCsrDetails

Name	Mandatory
category	(Mandatory) Certificate category **Type**: String **Possible values**: Server, Client, and Code Signing
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

certificateFormat

Name	Mandatory
format	(Mandatory) Certificate download format. Refer to the Possible values for Certificate Download Format table. **Type**: String
password	(Optional) The field is mandatory for some parameters (refer to the table below). **Type**: String

Possible Values for Download Format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Possible Values for Download Format (continued)

Certificate Extension	Value in the Payload	Password Required
.pk12	PK12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
resourceId response	Identifier of the certificate record that has been created (the resourceId in the above request can be found using the search API using commonName, serial No. or other search parameters). **Type**: String
requestId response	Open work order request ID. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate submission triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_CSR_GEN_SOURCE	Invalid csr generation source specified. **Remediation**: Ensure that a valid value is provided for the csrGenerationSource field in the request.
417 Expectation failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure that the field csrGenerationSource field has read write permission.
404 Expectation failed	GROUP_NOT_FOUND	Invalid group name specified. **Remediation**: Ensure that a valid value is provided for the certificateGroup section in the request.
404 Not Found	CERT-CA-0001	CA settings are not available. **Remediation**: Ensure that a valid value is provided for the caSettingName section in the request.

Related Information

Add Certificate Attributes

Download a Certificate

Download a Certificate by Format

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• CA Specific Information
• Common Payload Objects

CA Specific Information

Payload structure, sample request/response and the possible response codes for all the supported CAs are as follows:

• Sectigo
• DigiCert
• InCommon
• AppViewX
• EJBCA
• GlobalSign
• Trustwave
• Entrust
• Symantec
• Let’s Encrypt
• GoDaddy
• Google
• Amazon
• Microsoft Enterprise
• Microsoft Standalone
• OpenTrust
• Sample Request/Response
• Entrust MPKI

Sectigo

Sectigo Request Objects

Sectigo caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo caConnectorInfo (continued)

Name	Description
	Type: String **Constraint**: The value should be **Comodo Certificate Manager**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo caConnectorInfo (continued)

Name	Description
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Sectigo CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Sectigo genericFields
vendorSpecificDetails	(Optional) Data specific to the Sectigo vendor. **Type**: Sectigo vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo caConnectorInfo (continued)

Name	Description
name	(Optional) Name for the CA connector. **Type**: String

Sectigo CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo CSR Parameters (continued)

Name	Description
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Sectigo genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sectigo vendorSpecificDetails

Name	Description
serverType	(Mandatory) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
"caConnectorInfo":
{
"certificateAuthority": "Comodo Certificate Manager",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
 "caSettingName": "Sectigo_Test",
"certificateType": "EliteSSL Certificate",
 "description": "",
"csrParameters":
{
"commonName": "testcert2n.ams1907.com",
"hashFunction": "SHA256",
"keyType": "RSA",
 "bitLength": "2048",
 "certificateCategories":
 [
"Server",
"Client"
],
 "ellipticCurve": "",
 "enhancedSANTypes":
 {
"dNSNames": []
 }
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 },
 "genericFields":
{
"device_name_Comodo Certificate Manager": "TestDevice",
"vs_ip_Comodo Certificate Manager": "192.168.192.168"
},
 "vendorSpecificDetails":
{
"serverType": "Apache-SSL (Ben-SSL, not Stronghold)"
},
 "validityUnitValue": "365",
"validityInDays": "365",
"validityUnit": "days"
},
 "certificateGroup":
{
 "name": "Default"
},
"certificateFormat":
{
 "format": "PEM",
"password": ""
 }
 }
```


Response


```
 {
"response":
{
 "resourceId": "5e98047171eee023092ba006",
"requestId": "242"
 },
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

DigiCert

DigiCert Request Objects

DigiCert caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Digicert**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

DigiCert caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
divisionId	(Mandatory) Digicert division id. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Digicert CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Digicert genericFields
vendorSpecificDetails	(Optional) Data specific to the Digicert vendor. **Type**: Digicert vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

DigiCert caConnectorInfo (continued)

Name	Description
	Type: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Digicert CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Digicert CSR Parameters (continued)

Name	Description
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Digicert CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Digicert genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Digicert vendorSpecificDetails

Name	Description
caCertId	(Optional) Certificate id for the chosen certificate authority. **Type**: String **Constraint**: It is **mandatory** for DigiCert private product types e.g. "Private SSL Plus."
serverType	(Optional) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload

```
{
 "csrGenerationSource": "ENDPOINT",
"deviceDetails":
{
"vendor": "Apache",
"category": "Server",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 "deviceName": "Apache server",
"csrFileName": "test",
 "keyFileName": "test",
"attributes":
{
 "csrLocation": ""
 }
 },
"caConnectorInfo":
{
 "certificateAuthority": "DigiCert",
"isAutoRenewal": false,
 "autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "DigiCert",
"divisionId": "80312",
"certificateType": "Private SSL Plus",
 "description": "", "csrParameters":
{
 "commonName": "testcert8g.appviewx.plus",
"organization": "AppViewX Inc.",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
 "certificateCategories": ["Server", "Client"],
"ellipticCurve": "", "enhancedSANTypes":
{
"dNSNames": []
 }
},
 "genericFields":
{
 "device_name_DigiCert": "test_device",
 "vs_ip_DigiCert": "xxx.xxx.xxx.xxx"
 },
"vendorSpecificDetails":
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"caCertId": "741B2D2F05C7F6543EFB",
"serverType": "Apache" },
"validityUnitValue": "1",
"validityInDays": 365,
"validityUnit": "years"
},
"certificateGroup":
{
"name": "Default"

}
}
```


Response


```
{
"response":
{
"resourceId": "5f4faf3e70040d33314f1142",
"requestId": "173"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


InCommon

InCommon Request Objects

InCommon caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

InCommon caConnectorInfo (continued)

Name	Description
	Constraint: The value should be **InCommon**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

InCommon caConnectorInfo (continued)

Name	Description
	Type: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: InCommon CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: InCommon genericFields
vendorSpecificDetails	(Optional) Data specific to the InCommon vendor. **Type**: InCommon vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer

InCommon CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

InCommon CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

InCommon genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

InCommon vendorSpecificDetails

Name	Description
serverType	(Mandatory) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "InCommon",
 "isAutoRenewal": "false",
"autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "Incommon_test_ca",
"certificateType": "EliteSSL Certificate",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes":
"dNSNames": []
}
},
"genericFields": {
"device_name_InCommon": "test_device",
"vs_ip_InCommon": "192.168.142.162"
},
"vendorSpecificDetails": {
"serverType": "AOL"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response":
{
"resourceId": "5f47b29938c8c041c2c7096b",
"requestId": "112
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX

AppViewX Request Objects

AppViewX caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **AppViewX**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateProfileName	(Optional) Determines the category of certificate that is being requested. **Type**: String **Constraint**: Possible values - Server, Client, and Code Signing. The default value is Server.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: AppViewX CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: AppViewX genericFields
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX caConnectorInfo (continued)

Name	Description
	Constraint: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

AppViewX CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX CSR Parameters (continued)

Name	Description
	Constraint: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

AppViewX genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "AppViewX",
"isAutoRenewal": false,
"autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "AppViewX CA",
"certificateProfileName":"Server",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"locality": "Plano",
"state": "Texas",
"country": "US",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": ["*.testcert4d.appviewx.com, testcert4b1.avx.com"],
"iPAddresses": ["xxx.xxx.xxx.xxx"]
}
},
"genericFields": {
"device_name_AppViewX": "test_device",
"vs_ip_AppViewX": "192.168.142.162"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
}
}
```

Response

```
{
"response": {
"resourceId": "5f4842fd70040d33314f0748",
"requestId": "135"
},
 "message": "Certificate submission triggered successfully.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
}
```

EJBCA

EJBCA Request Objects

EJBCA caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Ejbca**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EJBCA caConnectorInfo (continued)

Name	Description
	Constraint: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String **Constraint**: *Prerequisite* - End entity profiles should have been fetched and updated in the specified CA setting.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Ejbca CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Ejbca genericFields
vendorSpecificDetails	(Optional) Data specific to the Ejbca vendor. **Type**: Ejbca vendorSpecificDetails
customAttributes	(Optional) Custom fields configured for EJBCA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EJBCA caConnectorInfo (continued)

Name	Description
postalCode customAttributes	(Optional) This field is given as an example, there could be any number of fields as specified in the policy. **Type**: String
name	(Optional) Name for the CA connector. **Type**: String

EJBCA CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EJBCA CSR Parameters (continued)

Name	Description
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EJBCA CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, rfc822Names, iPAddresses and uniformResourceIdentifiers.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
rfc822Names `enhancedSANTypes`	(Optional) Email addresses to be considered as Subject Alternative Names. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) URIs to be considered as Subject Alternative Names. **Type**: Array of String

EJBCA genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EJBCA genericFields (continued)

Name	Description
	Type: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

EJBCA vendorSpecificDetails

Name	Description
userName	(Optional) The username configured at the CA's end. **Type**: String
endEntityProfileName	(Mandatory) The name of the end-entity profile configured at the CA's end. **Type**: String
issuerCommonName	(Mandatory) The common name of the issuer configured at the CA's end. **Type**: String
certificateProfileName	(Mandatory) The name of the certificate profile selected from the available options for the chosen "endEntityProfile." **Type**: String

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Ejbca",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"isAutoRenewal": false,
"autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "ejbca",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"locality": "Plano",
"state": "Texas",
"country": "US",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": ["testcert5.avx.com"],
"rfc822Names": ["test@testcert5.avx.com"],
"iPAddresses": ["xxx.xxx.xxx.xxx"],
"uniformResourceIdentifiers": ["http://testcert5.avx.com"]
}
},
"genericFields": {
"device_name_Ejbca": "test_device",
"vs_ip_Ejbca": "192.168.142.162"
},
"vendorSpecificDetails": {
"userName": "",
"endEntityProfileName": "APPVIEWX PROFILE",
"issuerCommonName": "Ejbca New Intermediate CA",
"certificateProfileName": "SERVER PROFILE"
},
"customAttributes": {}
},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "147"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


GlobalSign

GlobalSign Request Objects

GlobalSign caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **GlobalSign**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign caConnectorInfo (continued)

Name	Description
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String **Constraint**: Possible values - Alpha SSL, Domain SSL, Organization SSL, and Extended SSL.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign caConnectorInfo (continued)

Name	Description
	Type: GlobalSign CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the GlobalSign vendor. **Type**: GlobalSign vendorSpecificDetails **Constraint**: Mandatory for the following "cerificateTypes" - Alpha SSL, Domain SSL, and Extended SSL.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

GlobalSign CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign CSR Parameters (continued)

Name	Description
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GlobalSign vendorSpecificDetails

Name	Description
domainAdminMailId	(Mandatory) The local-part of the email address for the administrator or group responsible for issuing and approving certificate requests. For instance, in hostmaster@test.com, "hostmaster" is the local-part. **Type**: String
incorporatingAgencyRegistrationNumber	(Optional) The registration number of the company. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.
designation	(Optional) The designation of the authorized signer. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.
businessCategory	(Optional) The category code for the business type. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
 "caConnectorInfo": {
"certificateAuthority": "GlobalSign",
"autoRegenerateEnabled": false,
"caSettingName": "Globalsign",
"certificateType": "Alpha SSL",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"streetAddress": "Park Street",
"locality": "Plano",
"state": "Texas",
"country": "US",
"postalCode": "73301",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"vendorSpecificDetails": {
"domainAdminMailId": "hostmaster",
"incorporatingAgencyRegistrationNumber": "",
"designation": "",
"businessCategory": "PO",
"orderId": ""
},
"validityInDays": 183
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e876e70040d33314f0f0b",
"requestId": "149"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Trustwave

Trustwave Request Objects

Trustwave caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Trustwave**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Trustwave caConnectorInfo (continued)

Name	Description
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Trustwave CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Trustwave genericFields
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Trustwave CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters (continued)

Name	Description
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Trustwave genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Trustwave",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "trustwave",
"certificateType": "SecureTrust Organization Validation",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"streetAddress": "Park Street",
"locality": "Plano",
"state": "Texas",
"country": "US",
"postalCode": "75093",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"genericFields": {
"device_name_Trustwave": "test_device",
"vs_ip_Trustwave": "xxx.xxx.xxx.xxx"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"response": {
"resourceId": "5f4e934570040d33314f0f1d",
"requestId": "151"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Entrust

Entrust Request Objects

Entrust caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Entrust**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust caConnectorInfo (continued)

Name	Description
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
divisionId	(Mandatory) Entrust division id. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Entrust CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Entrust genericFields
vendorSpecificDetails	(Optional) Data specific to the Entrust vendor.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust caConnectorInfo (continued)

Name	Description
	Type: Entrust vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
customAttributes	(Optional) Custom fields configured for Entrust, such as email1.
email1 customAttributes	(Optional) The field "email1" is given as an example. Multiple custom attributes could be configured. **Type**: String
name	(Optional) Name for the CA connector. **Type**: String

Entrust CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, and uniformResourceIdentifiers.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URIs to be considered as subject alternative names. **Type**: Array of String

Entrust genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Entrust vendorSpecificDetails

Name	Description
additionalEmails	(Optional) Additional emailID to be associated with the request. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust vendorSpecificDetails (continued)

Name	Description
	Constraint: It should be a valid email address.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Entrust",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "Entrust",
"certificateType": "Standard",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
"iPAddresses": [],
"uniformResourceIdentifiers": []
}
},
"genericFields": {
"device_name_Entrust": "test_device",
"vs_ip_Entrust": "xxx.xxx.xxx.xxx"
},
"vendorSpecificDetails": {
"additionalEmails": "test1@test.com"
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
},
"customAttributes": {
"email1": "test@test.com",
"text2": "ID12345",
"dropdown1": "Server Cert",
"number1": "1",
"date1": 1598985000000
},
"validityInDays": 90
},
"certificateGroup": {
"name": "Default"
}
```


Response


```
{
"response": {
"resourceId": "5f4fcb1770040d33314f11f0",
"requestId": "184"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Symantec

Symantec Request Objects

Symantec caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Symantec**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Symantec caConnectorInfo (continued)

Name	Description
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Symantec caConnectorInfo (continued)

Name	Description
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Symantec CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Symantec genericFields
vendorSpecificDetails	(Optional) Data specific to the Symantec vendor. **Type**: Symantec vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Symantec CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String **Type**: String
encryptedChallengePassword	(Mandatory) Base64 encoded challenge password.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
dNSNames	(Optional) List of subject alternative names for the certificate.
enhancedSANTypes	**Type**: Array of String

Symantec genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Symantec vendorSpecificDetails

Name	Description
serverType	(Optional) The server category to which the certificate is requested, such as Redhat. **Type**: String

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Symantec",
"isAutoRenewal": "true",
"renewBefore": "30",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"autoRegenerateEnabled": false,
"caSettingName": "Symantec",
"certificateType": "Standard",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"locality": "Plano",
"state": "Texas",
"country": "US",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QXBwVmlld1hAMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"genericFields": {
"device_name_Symantec": "test_device",
"vs_ip_Symantec": "xxx.xxx.xxx.xxx"
},
"vendorSpecificDetails": {
"serverType": "Red Hat"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"response": {
"resourceId": "5f4fe53c70040d33314f122d",
"requestId": "190"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Let’s Encrypt

Lets Encrypt Request Objects

Lets Encrypt caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Lets Encrypt**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Lets Encrypt caConnectorInfo (continued)

Name	Description
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: LetsEncrypt CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: LetsEncrypt genericFields
vendorSpecificDetails	(Optional) Data specific to the LetsEncrypt vendor. **Type**: LetsEncrypt vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Lets Encrypt caConnectorInfo (continued)

Name	Description
	Type: String

Lets Encrypt CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Lets Encrypt CSR Parameters (continued)

Name	Description
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Lets Encrypt CSR Parameters (continued)

Name	Description
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Lets Encrypt genericFields

Name	Description
device_name_LetsEncrypt	(Optional) Server device name for which certificate is requested. **Type**: String
vs_ip_LetsEncrypt	(Optional) Server IP address for which certificate is requested. **Type**: String
f5_device	(Optional) F5 device name/IP address. **Type**: String
data_group_name	(Optional) Data group name. **Type**: String
infoblox_device	(Optional) Infoblox device name/IP address. **Type**: String
validation_ip	(Optional) Validation IP address.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Lets Encrypt genericFields (continued)

Name	Description
	Type: String

Lets Encrypt vendorSpecificDetails

Name	Description
challengeType	(Mandatory) The challenge validation type. **Type**: String **Possible values**: DNS or HTTP.

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
 "caConnectorInfo": {
 "certificateAuthority": "LetsEncrypt",
 "isAutoRenewal": "false",
 "autoRegenerateEnabled": true,
 "regenerateBeforeInDays": "30",
 "caSettingName": "LetsEncrypt",
 "description": "",
 "csrParameters": {
 "commonName": "testcert.testdomain.net",
 "hashFunction": "SHA256",
 "keyType": "RSA",
 "bitLength": "4096",
 "certificateCategories": ["Server"],
 "ellipticCurve": "",
 "enhancedSANTypes": {
 "dNSNames": ["test.lab.appviewx.net"]
 }
 },
 "genericFields": {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"device_name_LetsEncrypt": "",
"vs_ip_LetsEncrypt": "",
"f5_device": "",
"data_group_name": "",
"infoblox_device": "",
"validation_ip": ""
},
"vendorSpecificDetails": {
"challengeType": "DNS"
},
"validityInDays": 90
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f510caa70040d33314f13d7",
"requestId": "204"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


GoDaddy

GoDaddy Request Objects

GoDaddy caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GoDaddy caConnectorInfo (continued)

Name	Description
	Type: String **Constraint**: The value should be **GoDaddy**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GoDaddy caConnectorInfo (continued)

Name	Description
	Type: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: GoDaddy CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the GoDaddy vendor. **Type**: GoDaddy vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String

GoDaddy CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GoDaddy CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GoDaddy CSR Parameters (continued)

Name	Description
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

GoDaddy vendorSpecificDetails

Name	Description
firstName	(Optional) User’s first name as configured in GoDaddy. **Type**: String
lastName	(Optional) User’s last name as configured in GoDaddy. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

GoDaddy vendorSpecificDetails (continued)

Name	Description
emailAddress	(Optional) Email address of the user to be configured at the CA. **Type**: String **Constraint**: It should be a valid email address.
phone	(Optional) Phone number of the user. **Type**: String
apiKey	(Mandatory) API key to be used for GoDaddy CA communication. **Type**: String
apiSecret	(Mandatory) API secret to be used for GoDaddy CA communication. **Type**: String
customerNumber	(Mandatory) Customer number obtained from the user's GoDaddy portal. **Type**: String
url	(Mandatory) Base URL to be used for GoDaddy CA communication. **Type**: String

Sample Request/Response

Request Payload


```
{
"certificateGroup": {
"name": "Default"
},
"caConnectorInfo": {
"name": "GoDaddy Deluxe UCC SSL SAN UCC OV SSL connector",
"description": "",
"certificateUuid": "",
"certificateAuthority": "GoDaddy",
"certificateType": "Deluxe UCC SSL - SAN (UCC_OV_SSL)",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"csrParameters": {
"commonName": "testgodaddy",
"organization": "",
"locality": "",
"country": "",
"enhancedSANTypes": {
"dnsnames": [
"testgodaddy"
],
"dNSNames": [
"testgodaddy"
]
},
"organizationUnit": "",
"state": "",
"mailAddress": "",
"keyType": "RSA",
"bitLength": "1024",
"hashFunction": "SHA160",
"ellipticCurve": "",
"encryptedChallengePassword": "",
"certificateCategories": [
"Server",
"Client"
]
},
"renewBefore": 0,
"autoRegenerateEnabled": false,
"regenerateBeforeInDays": 0,
"inheritedFromGroup": false,
"caSettingName": "Godaddy",
"validityInDays": 365,
"vendorSpecificDetails": {
"slotSize": "10",
"orderId": ""
},
"whiteLabelledCA": false,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"existingUuid": "",
"validityUnit": "years",
"validityUnitValue": 1,
"certificateCategory": "Server and Client",
"isAutoRenewal": false
},
"csrGenerationSource": "appviewx",
"fileIds": []
}
```


Response


```
{
 "response": {
 "resourceId": "60630a762be80b7ea8f03c06",
 "requestId": "155"
 },
 "message": "Certificate submission triggered successfully.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
}
```


Google

Google Request Objects

Google caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Google**.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays."

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google caConnectorInfo (continued)

Name	Description
	Type: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
issuerName	(Mandatory) Location of the Issuer configured at the CA end. **Type**: String
issuerLocation	(Mandatory) Parameters that are necessary for generating the CSR. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Google CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Google genericFields
vendorSpecificDetails	(Optional) Data specific to the Digicert vendor. **Type**: Google vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google caConnectorInfo (continued)

Name	Description
	the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Google CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Google genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Google genericFields (continued)

Name	Description
	Constraint: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Google vendorSpecificDetails

Name	Description
certificateId	(Optional) Unique name of the certificate maintained in Google CA. **Type**: String **Constraint**: If there's no value entered, it will be filled with common name and the current timestamp.

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Google",
"autoRegenerateEnabled": false,
"caSettingName": "Google",
"issuerLocation": "us-east1",
"issuerName": "AppViewX-Demo",
"description": "",
"csrParameters": {
"commonName": "testgooglecertificate",
"subjectAlternativeNames": [
"dNSNames"
],
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"postalCode": "",
"certificateCategories": [
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testgooglecertificate"
]
}
},
"genericFields": {
"device_name_Google": "",
"vs_ip_Google": ""
},
"vendorSpecificDetails": {
"certificateId": ""
},
"validityUnitValue": "1",
"validityInDays": 365,
"validityUnit": "years"
},
"certificateGroup": {
"name": "Default"
}
}
```


Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"response": {
 "resourceId": "5f4e5c2e70040d33314f0e9d",
 "requestId": "148"
 },
 "message": "Certificate submission triggered successfully.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Amazon

Amazon Request Objects

Amazon caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Amazon**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Amazon caConnectorInfo (continued)

Name	Description
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Amazon CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Amazon genericFields
name	(Optional) Name for the CA connector. **Type**: String

Amazon CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Amazon CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as 'Strict.'
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Amazon CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames	(Optional) List of subject alternative names for the certificate. enhancedSANTypes **Type**: Array of String

Amazon genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
 "caConnectorInfo": {
 "certificateAuthority": "Amazon",
 "isAutoRenewal": false,
 "autoRegenerateEnabled": false,
 "caSettingName": "Amazon",
 "certificateType": "",
 "description": "",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testamazon.appviewx.com"
]
}
},
"genericFields": {
"device_name_Amazon": "",
"vs_ip_Amazon": ""
},
"vendorSpecificDetails": {
"orderId": ""
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "149"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Microsoft Enterprise

Microsoft Enterprise Request Objects

Microsoft Enterprise caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Microsoft Enterprise**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise caConnectorInfo (continued)

Name	Description
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Microsoft Enterprise CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Microsoft Enterprise genericFields
vendorSpecificDetails	(Optional) Data specific to the Microsoft Enterprise vendor. **Type**: Microsoft Enterprise vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String

Microsoft Enterprise CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, directoryNames, rfc822Names, registeredIDs, uniformResourceIdentifiers, and otherNames.
dNSNames	(Optional) List of subject alternative names for the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
`enhancedSANTypes`	**Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
directoryNames `enhancedSANTypes`	(Optional) List of Directory names as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid directory name.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid mail address.
registeredIDs `enhancedSANTypes`	(Optional) List of registered ids as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid registered id.
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
otherNames `enhancedSANTypes`	(Optional) List of other names as as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Microsoft Enterprise vendorSpecificDetails

Name	Description
templateName	(Mandatory) Template name to issue the certificate with. **Type**: String

MS Enterprise enhancedSANTypes

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	List of Subject Alternative names for the Certificate.	Array of String	Should be a valid domain name.
iPAddresses	No	IP addresses to be considered as Subject Alternative Names.	Array of String	Must be valid ip addresses.
directoryNames	No	List of Directory names as Subject Alternative names for the Certificate.	Array of String	Should be a valid directory name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

MS Enterprise enhancedSANTypes (continued)

Name	Mandatory	Description	Field Type	Constraints
rfc822Names	No	List of mail addresses as Subject Alternative names for the Certificate.	Array of String	Should be a valid mail address.
registeredIDs	No	List of registered ids as Subject Alternative names for the Certificate.	Array of String	Should be a valid registered id.
uniformResourceIdentifiers	No	List of URI as Subject Alternative names for the Certificate.	Array of String	Should be a valid URI.
otherNames	No	List of other names as Subject Alternative names for the Certificate.	Array of String	Should be a valid other name.

Sample Request/Response

Sample Request


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Microsoft Enterprise",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "MS_ENT",
"certificateType": "",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"hashFunction": "SHA256",
"encryptedChallengePassword": "QWRtaW5AMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testmscert.appviewx.com"
]
}
},
"genericFields": {
"device_name_Microsoft Enterprise": "",
"vs_ip_Microsoft Enterprise": ""
},
"vendorSpecificDetails": {
"templateName": "ServerCertificate"
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Sample Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "150"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Microsoft Standalone

Microsoft Standalone Request Objects

Microsoft Standalone caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Comodo Certificate Manager**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone caConnectorInfo (continued)

Name	Description
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Microsoft Standalone CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Microsoft Standalone genericFields
name	(Optional) Name for the CA connector. **Type**: String

Microsoft Standalone CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, directoryNames, rfc822Names, registeredIDs, uniformResourceIdentifiers, and otherNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses	(Optional) List of IP address to be considered as subject alternative names.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
`enhancedSANTypes`	**Type**: Array of String
directoryNames `enhancedSANTypes`	(Optional) List of Directory names as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid directory name.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid mail address .
registeredIDs `enhancedSANTypes`	(Optional) List of registered ids as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid registered id.
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
otherNames `enhancedSANTypes`	(Optional) List of other names as as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid name.

Microsoft Standalone genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone genericFields (continued)

Name	Description
	Type: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Microsoft Standalone",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "MS_STD",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QWRtaW5AMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testmscert.appviewx.com"
]
}
},
"genericFields": {
"device_name_Microsoft Standalone": "",
"vs_ip_Microsoft Standalone": ""
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "151"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


- Microsoft Standalone Request Objects
- Sample Request/Response

Microsoft Standalone Request Objects

Microsoft Standalone caConnectorInfo

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
certificateAuthority	Yes	Name of the certificateAuthority that will issue the certificate.	String	Value should be **Microsoft Standalone**.
isAutoRenewal	No	If enabled, renewal will be triggered before expiry based on renewBefore days.	Boolean	Should be disabled if autoRegenerateEnabled is **true**.
renewBefore	No	Specifies the no of days prior to expiry for triggering the renewal request.	Integer	Value must be provided if isAutoRenewal is **true**.
autoRegenerateEnabled	No	If enabled, renewal will be triggered before expiry based on renewBefore days.	Boolean	Should be disabled if isAutoRenewal is **true**.
regenerateBeforeInDays	No	Specifies the no of days prior to expiry for triggering the regenerate request.	Integer	Value must be provided if autoRegenerateEnabled is **true**.
caSettingName	Yes	Name of the CASetting that has been created in AppViewX for the chosen Certificate Authority.	String	NA
description	No	Note about the certificate.	String	NA
csrParameters	Yes	Parameters that are necessary for generating the CSR.	MS EnterprisecsrParameters	NA
genericFields	No	Custom fields configured for the CA/Customer.	genericFields	NA
name	No	Specifies the name for the CA connector	String	NA

MS Enterprise csrParameters

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
commonName	Yes	Fully qualified domain name (FQDN) of the server for which certificate is requested.	String	Must be compliant with the common name specified in the policy, if the policy is set as '**Strict**'.
organization	No	Legal name of the organization.	String	Default value - Value configured in the policy.
organizationUnit	No	Division or department of the organization handling the certificate.	String	Default value - Value configured in the policy.
locality	No	City where the organization is located. This shouldn't be abbreviated.	String	Default value - Value configured in the policy.
state	No	State or region where the organization is located.This shouldn't be abbreviated.	String	Default value - Value configured in the policy.
country	No	The two-letter code for the country where your organization is located.	String	Default value - Value configured in the policy.
EmailAddress	No	Email address of the organization.	String	Default value - Value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
hashFunction	No	Hash function to be used in the Certificate. For example, SHA160. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
keyType	No	Algorithm to be used for Key generation. For example, RSA, DSA, EC. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
bitLength	No	Bit length for the key is dependent on the key type chosen. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
encryptedChallengePassword	Yes	Base64 encoded challenge password.	String	NA
certificateCategories	Yes	Purpose for which the generated certificate will be used.	Array	Possible values - Server, Client, Code Signing, Email.
ellipticCurve	No	If the keyType chosen is **EC**, then the ellipticCurve must be specified depending on the	String	Default value - the first value

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		bitlength selected. Should be chosen from the possible values configured in the Certificate Policy.		will be chosen from the policy.
enhancedSANTypes	No	Subject alternative names for the certificate.	MS Standalone enhancedSANTypes	Value provided must be compliant with the Certificate Policy, if the policy is configured as **Strict**.

MS Standalone enhancedSANTypes

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	List of Subject Alternative names for the Certificate.	Array of String	Should be a valid domain name.
iPAddresses	No	IP addresses to be considered as Subject Alternative Names.	Array of String	Must be valid ip addresses.
directoryNames	No	List of Directory names as Subject Alternative names for the Certificate.	Array of String	Should be a valid directory name.
rfc822Names	No	List of mail addresses as Subject Alternative names for the Certificate.	Array of String	Should be a valid mail address.
registeredIDs	No	List of registered ids as Subject Alternative names for the Certificate.	Array of String	Should be a valid registered id.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
uniformResourceIdentifiers	No	List of URI as Subject Alternative names for the Certificate.	Array of String	Should be a valid URI.
otherNames	No	List of other names as Subject Alternative names for the Certificate.	Array of String	Should be a valid other name.

Sample Request/Response

- Sample Request:
- Sample Response:

Sample Request:


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Microsoft Standalone",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "MS_STD",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QWRtaW5AMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testmscert.appviewx.com"
]
}
},
"genericFields": {
"device_name_Microsoft Standalone": "",
"vs_ip_Microsoft Standalone": ""
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Note: Please refer to the "Request Structure" to identify the changeable values.

Sample Response:


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "151"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

OpenTrust

OpenTrust caConnectorInfo

Opentrust caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Digicert**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Opentrust caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Opentrust CSR Parameters
vendorSpecificDetails	(Mandatory) Data specific to the Opentrust vendor. **Type**: Opentrust vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String
certificateProfileName	(Mandatory) Name of the certificate profile configured in the CA portal.

Opentrust CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String **Constraint**: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames	(Optional) List of subject alternative names for the certificate.
`enhancedSANTypes`	**Type**: Array of String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters (continued)

Name	Description
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid mail address.

Opentrust vendorSpecificDetails

Name	Description
formFields	(Mandatory) Certificate parameters that are configured in the chosen certificate profile. **Type**: List of objects - formFields **Constraint**: CA settings must be saved after choosing the required certificate profile.
commonName1 `formFields`	Mandatory constraint depends on the profile configuration in the CA portal. Fully qualified domain name (FQDN) of the server for which certificate is requested. (Parameters can be identified in the CA portal or the certificate enrollment page in the AppViewX UI.) **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Opentrust vendorSpecificDetails (continued)

Name	Description
	Note: Multiple parameters may be configured in the Certificate Management Profile in the OpenTrust CA portal. The parameter mentioned is a sample.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "OpenTrust",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "OpenTrust",
"description": "Test certificate",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"vendorSpecificDetails": {
"formFields": {
"commonName1": "testcertot.appviewx.net",
"subjectAltNameDNS1": "testcertot1.appviewx.net"
}
},
"certificateProfileName": "server"
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "606357ec14974147f02c53ec",
"requestId": "119"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Sample Request/Response

- Sample Request:
- Sample Response:

Sample Request:


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "OpenTrust",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "OpenTrust",
"description": "Test certificate",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"vendorSpecificDetails": {
"formFields": {
"commonName1": "testcertot.appviewx.net",
"subjectAltNameDNS1": "testcertot1.appviewx.net"
}
},
"certificateProfileName": "server"
},
"certificateGroup": {
"name": "Default"
}
}
```


Sample Response:


```
{
"response": {
"resourceId": "606357ec14974147f02c53ec",
"requestId": "119"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI

Entrust MPKI Request Objects

Entrust MPKI caConnectorInfo

Name	Mandatory	Description	Field Type	Constraints
certificateAuthority	Yes	Name of the certificateAuthority that will issue the certificate.	String	Value should be Entrust MPKI.
isAutoRenewal	No	If enabled, renewal will be triggered before expiry based on renewBefore days.	Boolean	Should be disabled if autoRegenerateEnabled is true.
renewBefore	No	Specifies the no of days prior to expiry for triggering the renewal request.	Integer	Value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	No	If enabled, renewal will be triggered before expiry based on renewBefore days.	Boolean	Should be disabled if isAutoRenewal is true.
regenerateBeforeInDays	No	Specifies the no of days prior to expiry for triggering the regenerate request.	Integer	Value must be provided if autoRegenerateEnabled is true.
caSettingName	Yes	Name of the CASetting that has been created in AppViewX for the chosen Certificate Authority.	String	NA
description	No	Note about the certificate.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI caConnectorInfo (continued)

Name	Mandatory	Description	Field Type	Constraints
csrParameters	Yes	Parameters that are necessary for generating the CSR.	Entrust MPKI csrParameters	NA
vendorSpecificDetails	Yes	Details specific to the Entrust vendor.	Entrust MPKI vendorSpecificDetails	NA
name	No	Specifies the name for the caConnector	String	NA

Entrust MPKI csrParameters

Name	Mandatory	Description	Field Type	Constraints
commonName	Yes	Fully qualified domain name (FQDN) of the server for which certificate is requested.	String	Must be compliant with the common name specified in the policy, if the policy is set as ‘Strict’.
organization	No	Legal name of the organization.	String	Default value - Value configured in the policy.
organizationUnit	No	Division or department of the organization handling the certificate.	String	Default value - Value configured in the policy.
locality	No	City where the organization is located. This shouldn't be abbreviated.	String	Default value - Value configured in the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI csrParameters (continued)

Name	Mandatory	Description	Field Type	Constraints
state	No	State or region where the organization is located.This shouldn't be abbreviated.	String	Default value - Value configured in the policy.
country	No	The two-letter code for the country where your organization is located.	String	Default value - Value configured in the policy.
mailAddress	No	Email address of the organization.	String	Default value - Value configured in the policy.
hashFunction	No	Hash function to be used in the Certificate. For example, SHA160. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
keyType	No	Algorithm to be used for Key generation. For example, RSA, DSA, EC. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
bitLength	No	Bit length for the key is dependent on the key type chosen. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI csrParameters (continued)

Name	Mandatory	Description	Field Type	Constraints
certificateCategories	Yes	Purpose for which the generated certificate will be used.	Array	Possible values - Server, Client, Code Signing, Email
ellipticCurve	No	If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bitlength selected. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
enhancedSANTypes	No	Subject alternative names for the certificate.	Entrust MPKI enhancedSANTypes	Value provided must be compliant with the Certificate Policy, if the policy is configured as Strict.

Entrust MPKI vendorSpecificDetails

Name	Mandatory	Description	Field Type	Constraints
caName	Yes	Name of the CA.	String	Should be a valid CA name configured in CA Settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI vendorSpecificDetails (continued)

Name	Mandatory	Description	Field Type	Constraints
certProfile	Yes	Certificate Profile name associated with the given caName.	String	Should be a valid Certificate Profile name configured in CA Settings.

Entrust MPKI enhancedSANTypes

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	List of Subject Alternative names for the Certificate.	Array of String	NA
iPAddresses	No	IP addresses to be considered as Subject Alternative Names.	Array of String	Must be valid ip addresses.
uniformResourceIdentifiers	No	URIs to be considered as Subject Alternative Names.	Array of String	NA

• Entrust MPKI Request Objects

• Sample Request/Response

Entrust MPKI Request Objects

Entrust MPKI Request Objects

Entrust MPKI caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Entrust MPKI**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore."

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI caConnectorInfo (continued)

Name	Description
	Type: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Entrust MPKI CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the Entrust MPKI vendor.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI caConnectorInfo (continued)

Name	Description
	Type: Entrust MPKI vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String

Entrust MPKI CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) The purpose or intended use for the generated certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Entrust MPKI CSR Parameters (continued)

Name	Description
	Constraint: Possible values are - Server, Client, Code Signing, and Email.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, and uniformResourceIdentifiers.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) URIs to be considered as as subject alternative names. **Type**: Array of String

Entrust MPKI vendorSpecificDetails

Name	Description
caName	(Mandatory) Name of the CA. **Type**: String **Constraint**: It should be a valid CA name configured in CA Settings.
certProfile	(Mandatory) Certificate Profile name associated with the given "caName." **Type**: String **Constraint**: It should be a valid certificate profile name configured in CA Settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Entrust MPKI",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "Entrust MPKI",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
"iPAddresses": [],
"uniformResourceIdentifiers": []
}
},
"vendorSpecificDetails": {
"caName": "Test CA",
"certProfile": "Test CA Profile"
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"response": {
"resourceId": "5f4fcb1770040d33314f11f0",
"requestId": "184"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Sample Request/Response

- Sample Request:
- Sample Response:

Sample Request:


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Entrust MPKI",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "Entrust MPKI",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server", "Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"iPAddresses": [],
"uniformResourceIdentifiers": []
}
},
"vendorSpecificDetails": {
"caName": "Test CA",
"certProfile": "Test CA Profile"
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Note: Please refer to the "Request Structure" to identify the changeable values.

Sample Response:


```
{
"response": {
"resourceId": "5f4fcb1770040d33314f11f0",
"requestId": "184"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Common Payload Objects

genericFields

Name	Mandatory	Description	Field Type	Constraints
device_name_<certificateAuthority>	No	Device name of the Server for	String	In the field name, <certificateAuthority> has to be

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

genericFields (continued)

Name	Mandatory	Description	Field Type	Constraints
		which certificate is requested.		replaced by the value provided for `certificateAuthority` in `caConnectorInfo.`
`vs_ip_<certificateAuthority>`	No	IP address of the server for which certificate is requested.	`String`	In the field name, `<certificateAuthority>` has to be replaced by the value provided for `certificateAuthority` in `caConnectorInfo.`

Create a Certificate in Sync mode

The API sends a request for certificate creation in Sync Mode, where the certificate is generated immediately and returned in the response. The request payload differs based on the Certificate Authority (CA) for which enrollment or creation is being requested. Unlike async APIs, two parameters, "isSync" and "ttl," stand out. When "isSync" (Sync Mode) is set to true, it overrides the certificate request approval policy to create a new certificate. These parameters are applicable to all mentioned CAs in the async APIs.

Request Structure

Endpoint:	/certificate/create
Type:	POST
Sample URL:	*https://<APPVIEWX_GATEWAY_IP>:<APPVIEWX_GATEWAY_PORT>/avxapi/certificate/create?gwkey=f000ca01&gwsource=external&isSync=true&ttl=300*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
isSync *Query*	Determines whether use the sync or async APIs. If **true** - use sync and **false** - use async API. The default value is **FALSE**. **Type**: Boolean **Constraint**: Value of the parameter should be **true** or **false**.
ttl *Query*	(Mandatry) The time to live (**ttl**) is a query parameter. If the total time taken surpasses this value, the response will indicate that the request is still in progress. On the other hand, if the operation completes successfully within the TTL, the response will indicate success.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: Integer **Constraint**: It must be a positive value.
Payload	Contains all the parameters to be sent in the request body for the post request.
Body	**Type**: SyncRequestStructure

SyncRequestStructure

Name	Description
csrGenerationSource	(Optional) Specifies where the CSR is to be generated. **Type**: **Possible values:**: AppViewX, Endpoint, HSM, uploadCSR. The default value is **AppViewX**
caConnectorInfo	(Mandatory) Details related to the certificate authority (CA) and the CSR parameters. **Type**: Any of the following data: • Amazon caConnectorInfo • AppViewX caConnectorInfo • DigiCert caConnectorInfo • EJBCA caConnectorInfo • Entrust caConnectorInfo • EntrustMPKI caConnectorInfo • GlobalSign caConnectorInfo • GoDaddy caConnectorInfo • Google caConnectorInfo • InCommon caConnectorInfo • LetsEncrypt caConnectorInfo • Microsoft Enterprise caConnectorInfo • Microsoft Standalone caConnectorInfo • OpenTrust caConnectorInfo

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

SyncRequestStructure (continued)

Name	Description
	• Sectigo caConnectorInfo • Symantec caConnectorInfo • Trustwave caConnectorInfo
certificateGroup	Specifies the group (category) to which the newly created certificate should be assigned. **Type**: certificateGroup **Constraint**: Default certificate Group is "**Default**".
deviceDetails	(Optional) Information about the device or endpoint where the Certificate Signing Request (CSR) will be generated. **Type**: deviceDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **Endpoint**.
certificateHSMDetails	(Optional) Information about the Hardware Security Module (HSM) device. **Type**: certificateHSMDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **HSM**.
uploadCsrDetails	(Optional) Information about the CSR. **Type**: uploadCsrDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **uploadCSR**.
certificateFormat	(Optional) Certificate download format details. **Type**: certificateFormat

certificateGroup

Name	Mandatory
name	(Optional) Specifies the group under which the created certificate needs to be tagged. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateGroup (continued)

Name	Mandatory
	Constraint: The certificate group must be present in AppViewX.

deviceDetails

Name	Mandatory
category	(Mandatory) Specifies the device category **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor	(Mandatory) Name of the vendor for the chosen device. For example, **Apache** is a vendor for **Server** category. **Type**: String
deviceName	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
csrFileName	(Mandatory) Name of the CSR file that is generated in the device. **Type**: String
keyFileName	(Mandatory) Name of the key file that is generated in the device. **Type**: String
attributes	(Optional) Additional attributes for the chosen device as mentioned the sub-attributes - csrLocation, tenant, and partition. **Type**:
csrLocation attributes	(Optional) The location within the device where the CSR is generated. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Server** and the **deviceDetails.vendor** is **Tomcat**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

deviceDetails (continued)

Name	Mandatory
tenant attributes	(Optional) Name of the partition within the AVI device. **Type**: String
partition attributes	(Optional) Name of the partition within the device. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Friewall** and the **deviceDetails.vendor** is **Fortinet**.

certificateHSMDetails

Name	Mandatory
type	(Mandatory) Type of the HSM device. **Type**: String **Possible values**: ADC and HSM.
keyReference	(Mandatory) Reference name for the key that is mapped by the HSM device. **Type**: String
hsmSettings	(Mandatory) Configuration details for the HSM device. Contains the sub-parameters vendorType and vendorSpecificSettings **Type**: List <String>
vendorTypehsmSettings	(Mandatory) Category of the vendor. **Type**: String **Possible values**: Safenet, Thales, and Fortanix.
vendorSpecificSettingshsmSettings	(Mandatory) Settings related to HSM vendor. Contains the sub-parameter moduleId **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateHSMDetails (continued)

Name	Mandatory
moduleId `hsmSettings.vendorSpecificSettings`	(Optional) The module id. **Type**: String **Constraints**: Applicable if **hsmSettings.vendorType** is **Thales**.
vendor	(Mandatory) The name of the vendor for the chosen device e.g., F5. **Type**: String
deviceName	(Mandatory) The name of the device as per AppViewX Device Inventory. **Type**: String

uploadCsrDetails

Name	Mandatory
category	(Mandatory) Certificate category **Type**: String **Possible values**: Server, Client, and Code Signing
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

certificateFormat

Name	Mandatory
format	(Mandatory) Certificate download format. Refer to the Possible values for Certificate Download Format table. **Type**: String
password	(Optional) The field is mandatory for some parameters (refer to the table below). **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Possible values for Certificate Download Format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body params:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
resourceId `response`	Identifier of the certificate record that has been created (the resourceId in the above request can be found using the search API using commonName, serial No. or other search parameters). **Type**: String
requestId	Open work order request ID.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: String
certificateContent	Content of certificate in Base64 encoded format. response **Type**: String
encodedFormat	Certificate content encoded format. response **Type**: String
certificateName	Certificate name. response **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object

Sample Request/Response

Request Payload

```
{
"caConnectorInfo": {
"caSettingName": "",
"validityInDays": 365,
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"certificateType": "",
"csrParameters": {
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"commonName": "",
"organization": "",
"organizationUnit": "",
"locality": "",
"state": "",
"country": "",
"mailAddress": "",
"encryptedChallengePassword": "",
"hashFunction": "",
"keyType": "",
"bitLength": "",
"certificateCategories": [
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
"iPAddresses": [],
"uniformResourceIdentifiers": []
}
}
"genericFields": {
"device_name_Entrust": "",
"vs_ip_Entrust": "",
"type": "",
"owner_email": "",
"environment": "",
"partition": "",
"devices": "",
"sync_group": "",
"requestor": "",
"project": ""
},
"vendorSpecificDetails": {
"avx_requester_fullname":"",
"avx_requester_emailid":"",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"avx_requester_phoneno": "",
"additionalEmails": ""
},
"customAttributes": {
"attribute1": ""
}
},
"certificateGroup": {
"name": "Default"
},
"certificateFormat": {
"format": "PEM",
"password": ""
}
}
```


Response


```
{
"response": {
"resourceId": "<Certificate Object ID>",
"requestId": "<Certificate WF Request ID>",
"certificateContent": "<Encoded Certificate Content>",
"encodedFormat": "base64",
"certificateName": "<Name of the Certificate>"
},
"message": "Certificate create and download action performed successfully",
"appStatusCode": "<Error Code>",
"tags": {},
"headers": null
}
```


Related Information

Add Certificate Attributes

Download a Certificate

Download a Certificate by Format

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Renew a Certificate in Async mode

The API initiates a request to renew an existing certificate in asynchronous mode. Upon successful triggering of the renew certificate API, the response includes a resourceId. This resourceId can be utilized to trigger the search API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. (The resourceId in the above request can be found through the search API using commonName, serialNumber or other search parameters.) **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the renewal. **Type**: String **Constraint**: Value should be **Renew**
challengePassword	(Optional) Base64 encoded value of challenge password. **Type**: String **Constraint**: Applicable and mandatory for Symantec Certificate Authority.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the renewal request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Renew action triggered successfully. **Type**: String
message	Success message or failure description in case of error.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Renew action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the renew action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
"commonName":"testcert8g.appviewx.plus",
"serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
"action":"Renew"
}
```


Response


```
{
"response": {
"resourceId": "5f4faf3e70040d33314f1142",
"message": "Renew action triggered successfully.",
"requestId": "209"
},
"message": "Renew action has been triggered successfully",
"appStatusCode": null,
"tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Related Information

- Revoke a Certificate in Async mode.
- Reissue a Certificate in Async mode.

Renew a Certificate in Sync mode

The API initiates a certificate renewal request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for certificate renewal. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Request Structure

Endpoint:	/certificate/renew
Type:	PUT
Sample URL:	*https://<Tanent/Host_name>:<portno>/avxapi/code-signing-upload-sign-file-policy?gwsource=external*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName	(Mandatory) Username that is configured in AppViewX.
Header	**Type**: String
password	(Mandatory) Password of that user.
Header	**Type**: String
content-type	(Mandatory) Payload content-type with application/json value.
Header	**Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Mandatory) Mongo ID of the certificate in the AppViewX database. (It refers to the resourceId field in the create certificate response.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Either resourceId or serialNumber and commonName is mandatory.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
format	(Mandatory) Certificate downloadable format. **Type**: String **Constraint**: Refer to the **Possible values for certificate download format** table below.
password	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: Refer to the Possible values for certificate download format table below.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Possible values for certificate download format (continued)

Certificate Extension	Value in the Payload	Password Required
.pk12	PK12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Open work order request ID. **Type**: String
certificateContent response	Content of certificate in Base64 encoded format. **Type**: String
encodedFormat response	Certificate content in encoded format. **Type**: String
certificateName response	Name of the certificate. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

Sample Request/Response

Request Payload

```
{
 "resourceId":<Mongo ID of the certificate in AppviewX Database>,
 "commonName":<Common Name of the certificate>,
 "serialNumber":<Serial Number of the certificate>,
 "certificateFormat":{
 "format" :<Cert format - check possible values table>,
 "password" :<password>
 }
 }
```

Response

```
{
 "response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certificateContent": <Encoded Certificate file>,
 "certificateName": <Name of the certificate>,
 "encodedFormat" : "base64"
 },
 "message": "Certificate Renew action executed successfully",
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Related Information

- Reissue a Certificate in Sync mode.
- Revoke a Certificate in Sync mode.

Revoke a Certificate in Async mode

The API initiates a request to revoke an existing certificate in asynchronous mode. Refer to the After you are done section to approve and implement the request.

Before you begin

Ensure the following before attempting to revoke a certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String
	Constraint: Required if username and password are not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the param should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. It is needed only in case of multi-tenant installations and can be ignored for other type of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered (e.g. external). **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the revocation. **Type**: String **Constraint**: Value should be **Revoke**
reason	(Mandatory) Reason for revocation. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the revoke request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Revoke action triggered successfully. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Revoke action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open worker for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the revoke action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload

```
{
"resourceId":"5f4faf3e70040d33314f1142",
"commonName":"testcert8g.appviewx.plus",
"serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
"action":"Revoke",
"reason":"Superseded"
}
```

Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"response": {
 "resourceId": "5f4faf3e70040d33314f1142",
 "message": "Revoke action triggered successfully.",
 "requestId": "216"
 },
 "message": "Revoke action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Related Information

- Reissue a Certificate in Async mode.

Revoke a Certificate in Sync mode

The API initiates a certificate revoke request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate revoke. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Request Structure

Endpoint:	/certificate/revoke
Type:	PUT
Sample URL:	*https://<APPVIEWX_GATEWAY_IP>:<APPVIEWX_GATEWAY_PORT>/avxapi/certificate/revoke?gwkey=f000ca01&gwsource=external&isSync=true&ttl=300*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName	(Mandatory) Username that is configured in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
resourceId	(Mandatory) Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNunmer. or other search parameters.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
reason	(Mandatory) Reasons for revoking the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
comments	(Mandatory) Additional comments for revoking the certificate **Type**: String **Constraint**: Comments field is mandatory for some revoke reasons alone. Refer to the valid reason for CAs table below.

Valid Reason for CAs

Certificate Authority	Reasons	Comments Required
Entrust	Superseded	No
	Cessation of operation	No
	Affiliation changed	No

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Valid Reason for CAs (continued)

Certificate Authority	Reasons	Comments Required
	Key compromised	Yes

Response Structure

- **Status Code: ––––––––**
- **Message: Successful**
- **Headers:**
  - **Content-Type:** application/json

Parameters

Name	Description
response	Contains the response attributes for the revoke request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Open work order request ID. **Type**: String
certStatus response	Status of the certificate action request. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload

```
{
 "resourceId": "5fa27b7ffee3a70235a5816d",
 "reason" :"Superseded"
 }
```

Response

```
{
 "response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certStatus": "Revoked"
 },
 "message": "Certificate Revoke action executed successfully",
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

Related Information

- Reissue a Certificate in Sync mode.

Reissue a Certificate in Async mode

The API will initiate a request to reissue an existing certificate in asynchronous mode. Upon successful triggering of the "Reissue a certificate" API, the response will include a resourceId. This resourceId can be used to trigger the search API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the reissue. **Type**: String **Constraint**: Value should be **Reissue**.
reason	(Mandatory) Reason for reissue request. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reissue request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Work order request Id. **Type**: String
message response	Success message - Reissue action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Should requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open workOrder for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the reissue action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
"commonName":"testcert8g.appviewx.plus",
 "serialNumber":"08:BD:54:35:FD:81:AC:A4:45:2B:FC:9F:77:56:FE:2C",
 "action":"Reissue",
 "reason":"Superseded"
 }
```


Response


```
{
"response": {
"resourceId": "5f51f7312fa95059a12b0aee",
"message": "Reissue action triggered successfully.",
"requestId": "238"
},
"message": "Reissue action has been triggered successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Related Information

- Revoke a Certificate in Async mode.

Reissue a Certificate in Sync mode

The API initiates a certificate revoke request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate reissue. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Request Structure

Endpoint:	/certificate/reissue
Type:	PUT

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample URL:	*https://<APPVIEWX_GATEWAY_IP>:<APPVIEWX_GATEWAY_PORT>/avxapi/certificate/reissue?gwkey=f000ca01&gwsource=external&isSync=true&ttl=300*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Mandatory) Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNumber. or other search parameters.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
reason	(Mandatory) Reasons for reissuing the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
category uploadCsrDetails	(Mandatory) Certificate category. **Type**: String **Constraint**: Possible values - **Server**, **Client**, or **Code Signing**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
csrContent uploadCsrDetails	(Mandatory) The CSR content for certificate enrollment request **Type**: String
format certificateFormat	(Mandatory) Certificate download format. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.
password certificateFormat	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reissue request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Open work order request ID. **Type**: String
certificateContent response	Content of certificate in Base64 encoded format. **Type**: String
encodedFormat response	Certificate content encoded format. **Type**: String
certificateName response	Name of the Certificate. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

Sample Request/Response

Request Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"resourceId": "<Mongo ID of the certificate in AppviewX Database>",
 "commonName": "<Common Name of the certificate>",
 "serialNumber": "<Serial Number of the certificate>",
 "reason": "<Reason for reissue>",
 "uploadCsrDetails": {
 "csrContent": "",
 "additionalSANValues": {
 "dNSNames": [],
 "iPAddresses": [],
 "uniformResourceIdentifiers": []
 }
 },
 "certificateFormat": {
 "format": "<Cert format - check possible values table>",
 "password": "<password>"
 }
 }
```

Response

```
{
"response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certificateContent": <Encoded Certificate file>,
 "certificateName": <Name of the certificate>,
 "encodedFormat" : "base64"
 },
 "message": "Certificate Reissue action executed successfully"
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

Related Information

- Revoke a Certificate in Sync mode.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Regenerate a Certificate in Async mode

The API will initiate a request to regenerate an existing certificate in asynchronous mode. Upon successful triggering of the "Regenerate a certificate" API, the response will include a resourceId. This resourceId can be used to trigger the search API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password	(Mandatory) Password of that user.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String
content-type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Required if resourceId is not specified.
action	(Mandatory) Action name for the regenerate request. **Type**: String **Constraint**: Value should be **Regenerate**.
reason	(Mandatory) Reason for regenerate request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the regenerate request.
resourceId `response`	Identifier of the certificate record that has been created. **Type**: String
requestId `response`	Work order request Id. **Type**: String
message `response`	Success message - Regenerate action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Regenerate action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Trigger the request once the open workOrder for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the regenerate action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f5641a7e74e187a7e3d5266",
 "commonName":"testcert8g.appviewx.plus",
 "serialNumber":"08:BD:54:35:FD:81:AC:A4:45:2B:FC:9F:77:56:FE:2C",
 "action":"Regenerate",
 "reason":"Key compromised"
 }
```


Response


```
{
 "response": {
 "resourceId": "5f56482ce74e187a7e3d52a2",
 "message": "Regenerate action triggered successfully.",
 "requestId": "237"
 },
 "message": "Regenerate action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Regenerate a Certificate in Sync mode

The API initiates a certificate regenerate request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate regenerate. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Request Structure

Endpoint:	/certificate/regenerate
Type:	PUT
Sample URL:	*https://<APPVIEWX_GATEWAY_IP>:<APPVIEWX_GATEWAY_PORT>/avxapi/certificate/regenerate?gwkey=f000ca01&gwsource=external&isSync=true&ttl=300*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Mandatory) Mongo Id of the certificate in the AppViewX database. (It refers to the ‘resourceId’ field in the create certificate response. It can be found through the search API using commonName, serialNumber. or other search parameters.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
format certificateFormat	(Mandatory) Certificate download format. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.
password certificateFormat	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the regenerate request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Open work order request ID. **Type**: String
certificateContent response	Content of certificate in Base64 encoded format. **Type**: String
encodedFormat response	Certificate content encoded format. **Type**: String
certificateName response	Name of the Certificate. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

Sample Request/Response

Request Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
 "resourceId":<Mongo ID of the certificate in AppviewX Database>,
 "commonName":<Common Name of the certificate>,
 "serialNumber":<Serial Number of the certificate>,
 "certificateFormat":{
 "format" :<Cert format - check possible values table>,
 "password" :<password>
 }
 }
```

Response

```
{
 "response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certificateContent": <Encoded Certificate file>,
 "certificateName": <Name of the certificate>,
 "encodedFormat" : "base64"
 },
 "message": "Certificate Regenerate action executed successfully",
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

Suspend a Certificate

The API initiates a request to suspend an existing certificate. Refer to the After you are done section to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **‘application/json’**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the suspend request. **Type**: String **Constraint**: Value should be **Suspend**
reason	(Mandatory) Reason for the suspend request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the suspend certificate request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Suspend action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Suspend action has been triggered successfully.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure the following: • The CA supports the suspend action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f5641a7e74e187a7e3d5266",
 "commonName":"testcert5d.avx.com",
 "serialNumber":"7E:94:56:98:57:F2:0E:3B",
 "action":"Suspend",
 "reason":"Superseded"
 }
```


Response


```
{
"response": {
 "resourceId": "5f4e5c2e70040d33314f0e9d",
 "message": "Suspend action triggered successfully.",
 "requestId": "241"
 },
 "message": "Suspend action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Reinstate a Certificate

The API initiates a request to reinstate a suspended certificate. Refer to the After you are done section to Approve and Implement the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for reinstate request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: Value should be **Suspend**
reason	(Mandatory) Reason for the reinstate request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reinstate certificate request.
resourceId `response`	Identifier of the certificate record that has been created. **Type**: String
requestId `response`	WorkOrder request Id. **Type**: String
message `response`	Success message - Reinstate action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reinstate action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the reinstate action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f4faf3e70040d33314f1142",
 "commonName":"testcert8g.appviewx.plus",
 "serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
 "action":"Reinstate",
 "reason":"Test"
 }
```


Response


```
{
 "response": {
 "resourceId": "5f4faf3e70040d33314f1142",
 "message": "Reinstate action triggered successfully.",
 "requestId": "216"
 },
 "message": "Reinstate action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Search/ Get Certificate Inventory

The API enables users to search for one or more certificates based on the provided searchable inputs. It returns full details of the matching certificate(s).

Request Structure

Endpoint:	/certificate/search
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Name	Description
input	(Mandatory) Search parameters such as keyword or free text search.
category input	(Optional) Specifies the certificate category. Possible categories are Server, Client, Code Signing, and Device. **Type**: String **Constraint**: Possible values are Server, Client, Code Signing and Device. The default value is Server.
resourceId input	(Optional) Id of the certificate. **Type**: String
freeSearch input	(Optional) Key for free text search. Search will be performed on all cert fields based on the free text input provided. **Type**: String **Constraint**: Value should be **Suspend**
keywordSearch input	(Optional) Search by certificate attributes based on the predefined key words.. **Type**: String
subject:o	(Optional) Subject organization name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
input. keywordSearch	**Type**: String
subject:ou	(Optional) Subject organization unit.
input. keywordSearch	**Type**: String
subject:cn	(Optional) Subject common name.
input. keywordSearch	**Type**: String
subject:l	(Optional) Subject location.
input. keywordSearch	**Type**: String
subject:st	(Optional) Subject state.
input. keywordSearch	**Type**: String
subject:c	(Optional) Subject country.
input. keywordSearch	**Type**: String
certversion	(Optional) Certificate version.
input. keywordSearch	**Type**: String
certserialno	(Optional) Certificate serial number.
input. keywordSearch	**Type**: String **Constraint**: Serial number of the certificate to be specified in the same format as in example- 1C:DB:14:3D:5C:98:EC:00:D0:C1:D1:63:78:B4:AA:42
certissuer	(Optional) Issuer common name.
input. keywordSearch	**Type**: String
certstatus	(Optional) Certificate status.
input. keywordSearch	**Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Possible values are Managed, New Certificate, Monitored, and Discovered
certgroup input. keywordSearch	(Optional) Certificate group. **Type**: String
expirydate input. keywordSearch	(Optional) Certificate expiry date in MM/DD/YYYY format, e.g. 03/26/2022 **Type**: String
expiryyear input. keywordSearch	(Optional) Certificate expiry year, e.g. 2022 **Type**: String
expirymonth input. keywordSearch	(Optional) Certificate expiry month., e.g. 03 **Type**: String
discoverysource input. keywordSearch	(Optional) The device name for certificates discovered from device OR for the certificates discovered from CA, the value will be **<<CA name>>::<<CA setting name>>**, e.g. if the CA name is **EJBCA** and the CA setting name is **Setting1**, then the value is **EJBCA:: Setting1**. **Type**: String
ca input. keywordSearch	(Optional) Certificate Authority name. **Type**: String
application input. keywordSearch	(Optional) CA name / Auto-enrollment protocol name / device vendor name. **Type**: String **Constraint**: Applicable for certificates discovered from CA/device and also the certificates enrolled via auto enrollment protocols. Possible values are SCEP, EST, ACME, and SCEP_MS_INTUNE.
issuer	(Optional) Issuer Common Name. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
input. keywordSearch	**Constraint**: Obtained from the AppViewX certificate inventory or the certificate data.
hash input. keywordSearch	(Optional) Hash function. **Type**: String **Constraint**: Possible values - SHA160, SHA224, SHA256, SHA384, SHA512
key input. keywordSearch	(Optional) Key Type. **Type**: String **Constraint**: Possible values - RSA, EC, DSA
keylength input. keywordSearch	(Optional) Bit length depending on the key type chosen. **Type**: String **Constraint**: Possible values - to be taken from the defined CA policy.
caSettings input. keywordSearch	(Optional) CA setting name. **Type**: String **Constraint**: Possible values - to be taken from the defined CA policy.
ellipticcurve input. keywordSearch	(Optional) Elliptic curve name. **Type**: String **Constraint**: Possible values - to be taken from the defined CA policy.
filter	(Mandatory) Pagination and sort parameters for the search.
max filter	(Optional) The number of entries from the start index to be made available. E.g., if the response is expected to have skipped the first 100 and show the next 50, then the start index has to be 101 and max has to be 50. **Type**: Integer **Constraint**: Default value is 100.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
start filter	(Optional) Start index from which the response has to be available. E.g., if the response has to skip the first 100 and show the next 50, then the start index has to be 101. **Type**: Integer **Constraint**: Default value is 0.
sortOrder filter	(Optional) Ascending or descending order of sort. **Type**: String **Constraint**: Possible values - **asc** or **desc**. Default value is **asc**.
sortColumn filter	(Optional) Sort by column. **Type**: String **Constraint**: Default value is _**id**.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
response response	Contains the inventory response attributes.
objects response.response	Certificate metadata. **Type**: Array of Certificate json.
totalRecords response.response	Total number of records matching the search criteria. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
obtainedRecords `response.response`	Number of records fetched for the query. **Type**: String
obtainedRecordRange `response.response`	Index of the records fetched.
start `response.response.obtainedRecordRange`	Start index of the fetched record. **Type**: String
end `response.response.obtainedRecordRange`	End index of the fetched record. **Type**: String
message `response`	Success message - Suspend action triggered successfully. **Type**: String
message	If matching records are found for the search query - **Matching results found for the given input.** If no records are available for the search query - **No matching records found for the given input.** **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	If matching records are found for the search query - **Matching results found for the given input.**
404 Not Found	NA	If no records are available for the search query - **No matching records found for the given input.**
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as the header parameter.
400 Bad Request	INVALID_REQUEST	Please input a valid sort order. **Remediation**: Ensure that valid value is provided for sortOrder.
400 Bad Request	INVALID_REQUEST	Invalid request specified. **Possible Causes**: • Either **filter** is not available or the filter value is invalid in the payload. • Value provided for **filter.max** is invalid.

Sample Request/Response

Request Payload

```
{
 "input":{
 "category":"Server",
 "keywordSearch" : {
 "certserialno":"7E:94:56:98:57:F2:0E:3B"
 }
 },
 "filter":{
 "max":"100",
 "start":"1",
 "sortColumn":"commonName",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"sortOrder":"desc"

}

}
```


Response


```
{

"response": {

"httpStatusCode": 200,

"response": {

"objects": [

{

"commonName": "testcert5d.avx.com",

"serialNumber": "7E:94:56:98:57:F2:0E:3B",

"issuerCommonName": "Ejbca New Intermediate CA",

"status": "Managed",

"associatedObjects": [],

"discoverySources": [],

"subjectOrganization": "AppViewX",

"subjectOrganizationUnit": "PE",

"subjectLocality": "Plano",

"subjectState": "Texas",

"subjectCountry": "US",

"issuerOrganization": "",

"issuerOrganizationUnit": "",

"issuerLocality": "",

"issuerState": "",

"issuerCountry": "",

"version": "3",

"validFrom": 1598943490000,

"validTo": 1607583490000,

"validFor": "90 day(s) 18 hr(s) 8 min(s)",

"keyAlgorithmAndSize": "RSA 2048",

"signatureAlgorithm": "SHA256withRSA",

"signatureHashAlgorithm": "SHA256",

"keyUsage": "DigitalSignature, NonRepudiation, KeyEncipherment",

"extendedKeyUsage": "Client Authentication(1.3.6.1.5.5.7.3.2) Server Authentication(1.3.6.1.5.5.7.3.1) ",

"basicConstraints": "Subject Type=End entity, Path Length=none",

"group": "Default",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"subjectAlternativeNames": [
"URL : http://testcert5.avx.com",
"Email address : test@testcert5.avx.com",
"DNS : testcert5.avx.com",
"IP Address : 192.168.142.162"
],
"complianceStatus": "Compliant",
"applications": [],
"expiryStatus": "Valid",
"permission": "RW",
"category": "Server",
"uuid": "4f4e23cefea2297a4e7d6b202ceee5ba47a20c89",
"certificateAuthority": "Ejbca",
"authorityKeyIdentifier": "69:15:BC:24:60:6B:73:96:8B:F3:3A:ED:C4:38:EB:58:A6:3F:4B:5B",
"subjectKeyIdentifier": "0D:31:76:0B:F1:41:AD:A6:39:6B:79:A6:43:8D:62:07:CC:F5:94:FB",
"authorityInfoAccess": [],
"certificatePolicies": [],
"crlDistributionPoints": [
"CrlDistributionPoint : [ name : , url : http://192.168.12.139:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=Ejbca%20New%20Intermediate%20CA ]"
],
"thumbprintAlgorithm": "SHA-1",
"thumbPrint": "9F:8E:0D:B6:A6:25:D4:05:E3:2B:5E:F7:85:1B:79:83:CB:EA:3C:DB",
"type": "Others",
"genericFields": {
"vs_ip_Ejbca": "192.168.142.162",
"device_name_Ejbca": "test_device"
},
"csrGenerationSource": "appviewx",
"newConnectors": [],
"csrAvailable": true,
"autoRenewDate": "",
"missingParamsForAutoRenew": "CSR parameters are available for certificate renewal",
"suspendedCertificate": false,
"mailAddress": "test@test.com",
"streetAddress": "",
"postalCode": "",
"requestIds": [
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"R147",
"R241"
],
"publicKey":
"30:82:01:0A:02:82:01:01:00:8B:64:08:1A:2B:40:B9:2F:7C:48:65:78:98:B3:A6:87:9D:E2:49:CF:25:A5:27:14:EE:A0:45:CE:E3:32:21:DC:8D:A5:AE:78:36:EF:5A:9
1:D6:7E:D9:F4:04:C5:A9:9A:38:F7:D4:C6:50:B2:4C:96:1C:AE:69:23:19:7C:45:87:07:37:4C:2C:07:25:87:6C:93:D0:B6:D0:5D:55:FC:29:A0:48:6A:75:CF:12:6C:41
:AE:90:BD:E7:89:C5:C4:8D:81:78:3D:DD:0B:29:61:92:55:0E:5A:8F:44:8F:44:CE:07:D8:11:95:7F:03:33:DD:86:E0:9A:69:42:AD:C9:67:44:91:FF:B2:02:ED:1A:16:
9C:B5:CC:03:92:3B:1A:17:52:D5:32:56:BF:52:D1:7C:8F:96:43:18:6E:43:22:55:32:01:4D:44:AA:52:13:6A:BB:B6:1B:DD:8D:76:D3:C6:C2:D0:D9:E0:9E:B8:4C:DD:
0A:8D:5C:5E:20:02:79:20:26:84:7F:35:B7:EF:E0:98:D1:FC:37:D4:1B:B8:4C:07:64:00:E8:18:DC:63:98:85:56:F3:D0:F7:E4:EF:F1:C1:0F:B3:F2:86:48:73:36:A5:5D
:AC:A9:A9:DE:F9:62:44:D0:C8:8D:F1:03:5F:3E:03:08:C8:0C:92:00:CF:72:55:02:03:01:00:01",
"issuedByRootCertificate": false,
"privatekeyAvaliable": true,
"resourceId": "5f4e5c2e70040d33314f0e9d"
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange": {
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null
},
"message": null,
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Add Certificate Attributes

The add certificates attributes API initiates the addition of various attributes like name, label, etc. to the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/attribute
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource	(Mandatory) Source from which the request is triggered

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. It consists of an array of attributes listed below. The array cannot be empty; a minimum of one entry must be present. **Type**: Payload

Payload

Name	Description
name	(Mandatory) The name of the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
label	(Mandatory) The label to be shown on the UI for the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
value	(Optional) Default value for the attribute. **Type**: String
mandatory	(Optional) Indicates whether the attribute is mandatory or optional. **Type**: Boolean
helpInfo	(Optional) Help information about the field. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
successfullFields response	List of fields that have been added successfully. **Type**: Array of CertificateGenericField
failedFields response	List of fields that have not been added successfully. **Type**: Array of CertificateGenericField
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 Accepted	NA	The response messages are as follows: • If all fields are added - **Certificate attribute added successfully** • If the addition of some fields have failed - **Certificate attribute added successfully. Failed fields are [<<failed field names>>]** • If the addition of all fields failed - **Certificate attribute addition failed.**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation Validate the inputs based on the following failure reasons: • Name or label are not provided for the failed field. • Value provided for the name or label does not meet the expected pattern. • Attributes with the provided name already exists.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - payload. **Remediation**: Payload array cannot be empty. At least one attribute must be provided.
400 Bad Request	avx-common-028	Invalid / Incorrect payload. **Remediation**: Check and ensure that the values provided for all the fields in the payload are accurate.

Sample Request/Response

Request Payload

```
[
{
"name": "externalemail",
"label": "External_Email",
"value": "test@test.com",
"mandatory": true,
"helpInfo":"The external email id"
},
{
"name": "priority",
"label": "priority",
"value": "1",
"mandatory": false
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
}

]
```


Response


```
{

"response": {

"failedFields": [],

"successfullFields": [

{

"id": "externalemailcustomAttributecustomAttribute",

"type": "text",

"value": "test@test.com",

"values": null,

"label": "External_Email",

"searchKey": "externalemail",

"errorCode": null,

"mandatory": true,

"validation": null,

"divClasses": null,

"classNames": null,

"category": "certAttributes",

"certificateAuthority": null,

"regexValue": null,

"helpInfo": "The external email id",

"name": "externalemail",

"mandatoryFor": null,

"_id": "externalemail"

},

{

"id": "prioritycustomAttributecustomAttribute",

"type": "text",

"value": "1",

"values": null,

"label": "priority",

"searchKey": "priority",

"errorCode": null,

"mandatory": false,

"validation": null,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": null,
"name": "priority",
"mandatoryFor": null,
"_id": "priority"
}
]
},
"message": "Certificate attribute added successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Related Information

Get Certificate Attributes

Update Certificate Attributes

The update certificates attributes API initiates a request to update the existing certificate attributes.

Request Structure

Endpoint:	/certificate/attribute
Type:	PUT
Sample URL:	
Headers	
Content-Type:	application/json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. The array cannot be empty; a minimum of one entry must be present. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
name	(Mandatory) The name of the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
label	(Mandatory) The label to be shown on the UI for the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
value	(Optional) Default value for the attribute. **Type**: String
mandatory	(Optional) Indicates whether the attribute is mandatory or optional. **Type**: Boolean
helpInfo	(Optional) Help information about the field. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
successfullFields `response`	List of fields that have been added successfully. **Type**: Array of CertificateGenericField
failedFields	List of fields that have not been added successfully.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: Array of CertificateGenericField
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate attribute updated successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - payload. **Remediation**: Payload array cannot be empty. At least one attribute must be provided.
400 Bad Request	avx-common-028	Invalid / Incorrect payload. **Remediation**: Check and ensure that the values provided for all the fields in the payload are accurate.

Sample Request/Response

Request Payload

```
[
 {
 "name": "approver",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"label": "approver",
"value": "cert approver",
"mandatory": true
}
]
```


Response


```
{
"response": {
"updatedGenericFields": [
{
"id": "approvercustomAttribute",
"type": "text",
"value": "cert approver",
"values": null,
"label": "approver",
"searchKey": "approver",
"errorCode": null,
"mandatory": true,
"validation": null,
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": null,
"name": "approver",
"mandatoryFor": null,
"_id": "approver"
}
],
"failedGenericFields": [],
"addedGenericFields": []
},
"message": "Certificate attribute updated successfully",
"appStatusCode": null,
"tags": {},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Related Information

Delete Certificate Attributes

Get Certificate Attributes

The get certificates attributes API fetches all the certificate attributes.

Request Structure

Endpoint:	/certificate/attribute
Type:	GET
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes. **Type**: Array of CertificateGenericField
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 Accepted	NA	Certificate attributes fetched successfully. OR No certificate attributes available.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.

Sample Request/Response

Request Payload

No payload for GET request

Response


```
{
 "response": [
 {
 "id": "approvercustomAttributecustomAttribute",
 "type": "text",
 "value": "cert approver",
 "values": null,
 "label": "approver",
 "searchKey": "approver",
 "errorCode": null,
 "mandatory": true,
 "validation": null,
 "divClasses": null,
 "classNames": null,
 "category": "certAttributes",
 "certificateAuthority": null,
 "regexValue": null,
 "helpInfo": null,
 "name": "approver",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"mandatoryFor": null,
"_id": "approver"
}
],
"message": "Certificate attributes fetched successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Related Information

Update Certificate Attributes

Delete Certificate Attributes

The delete certificates attributes API initiates a request to delete the existing certificate attributes.

Request Structure

Endpoint:	/certificate/attribute
Type:	DELETE
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String
	Constraint: Required if username and password are not provided.
username	(Mandatory) AppViewX login username.
Header	**Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
name *Query*	(Mandatory) Name of the certificate attribute that has to be deleted. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Message indicating whether the field has been successfully deleted or not. **Message**: *Deleted Successfully - [approver1]. Failed to delete - []*
message	Success message or failure description in case of error.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate attribute deleted successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 No Records Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the value provided for the name query parameter is accurate.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - name. **Remediation**: Ensure that the name query parameter is available in the request.

Sample Request/Response

Request Payload

No payload for DELETE request.

Response


```
{
 "response": "Deleted Successfully - [approver2]. Failed to delete - []",
 "message": "Certificate attribute deleted successfully",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Download a Certificate

The download certificate API can download a certificate in PEM format. If desired, the user can also request the certificate to be downloaded along with the key.

Request Structure

Endpoint:	
Type:	GET
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
resourceId *Query*	(Mandatory) Unique Id of the certificate to be downloaded. **Type**: String
keyRequired *Query*	(Optional) Indicates whether the private key needs to be downloaded. **Type**: Boolean
isCACertificate *Query*	(Optional) Indicates whether the certificate being downloaded is a CA certificate. **Type**: Boolean

Response Structure

Status Code:	200 OK
Error Response:	The error response will have the parameters described below.
Headers	
Content-Type:	application/octet-stream

Error response parameters

Name	Description
message	Failure description. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error response parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	The attachment of the **.pem** type certificate.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Ensure that the value provided for resourceId parameter refers to the id of an existing certificate.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - resourceId. **Remediation**: Ensure that the resourceId parameter is available in query parameter.
417 Expectation Failed	NOT_A_VALID_CERT	Invalid certificate. **Remediation**: Certificates that have not yet been issued cannot be downloaded. Ensure that the resourceId refers to the certificate that has been issued.
417 Expectation Failed	CERT-KEY-0006	Private key access is restricted in <<Default>> policy. **Remediation**: Retry downloading the certificate after enabling the flag **Enable Access to Private Key** in the Certificate Policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Response

The downloaded file is a **pem** file and the content of the downloaded file is as mentioned in the example below:


```
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
b24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAlthtOgQ3pOsqTQNroBvo3bSMgHFzZM
9O6II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
VOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
93FcXmn/6pUCyziKrlA4b9v7LWIbxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
A4IBAQCY8jdaQZChGsV2USggNiMOruYou6r4lK5IpDB/G/wkjUu0yKGX9rbxenDI
U5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
N+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
o/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
rqXRfboQnoZsG4q5WTP468SQvvG5
-----END CERTIFICATE-----
```


Download a Certificate by Format

The download certificate by format API initiates a request to download a certificate in the requested format. The user can request the private key to be downloaded in the specified format as well. The key can be requested with or without encryption. Additionally, the user can specify whether the complete certificate chain needs to be downloaded.

Request Structure

Endpoint:	/certificate/download/format
Type:	POST
Sample URL:	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	The payload contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
format	(Mandatory) The format of the certificate to be downloaded. **Type**: String **Constraint**: The possible certificate formats are - **CRT**, **CERT**, **CER**, **PEM**, **DER**, **DERCER**, **P7B**, **P7C**, **PK8**, **P12**, **PFX**, and **JKS**.
password	(Optional) Password for the certificate. It is applicable for the following certificate formats: **P12**, **PFX**, **JKS**, and **PK8**. (Mandatory) Password is mandatory for the following certificate formats: **P12**, **PFX**, and **JKS**. **Type**: String
commonName	(Mandatory) Common name of the certificate. **Type**: String
serialNumber	(Mandatory) Serial number of the certificate. **Type**: Boolean
isChainRequired	(Optional) Indicates whether to download the complete certificate chain or only the end certificate. **Type**: Boolean
isKeyEncryptionRequired	(Optional) Indicates whether the private key should be encrypted using a password. **Type**: Boolean **Constraint**: This is applicable for PK8 format. If the value is **true**, • Ensure that the certificate policy allows private key access. • The password must be provided in the request payload.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

Status Code:	200 OK
Error Response:	The error response will have the parameters described below.
Headers	
Content-Type:	application/octet-stream

Error response parameters

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	The attachment of the **.pem** type certificate.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Ensure that the value provided for commonName and serialNumber pertain to that of a valid existing certificate.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field>>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the **<<field>>** is available in the request payload.
400 Bad Request	INVALID_FORMAT	Invalid format specified. **Remediation**: Ensure that a valid value is provided in the format field of the request.
417 Expectation Failed	NOT_A_VALID_CERT	Invalid certificate. **Remediation**: Certificates that have not yet been issued cannot be downloaded. Ensure that the resourceId refers to the certificate that has been issued.
417 Expectation Failed	CERT-KEY-0006	Private key access is restricted in <<Default>> policy. **Remediation**: Retry downloading the certificate after enabling the flag **Enable Access to Private Key** in the Certificate Policy.
417 Expectation Failed	CERT-HLST-0007	Failed to download as the given extension is not supported. **Remediation**: Ensure that a valid value is provided for the format field in the request.
417 Expectation Failed	PASSWORD_FORMAT_WRONG	Password must have at least eight characters and contain at least one lowercase letter, one uppercase letter, one numeric digit, and one special character. **Remediation**: Password provided in the request payload must have at least eight characters and contain at least one lowercase letter, one uppercase letter, one numeric digit, and one special character.

Sample Request/Response

Request Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
"commonName" : "testcert7a.appviewx.com",
"serialNumber" : "07:2B:84:01:27:5A:77:63:38:C8:72:09:BE:CD:1F:D9:78:BA:BD",
"format" : "P12",
"password":"Password@123",
"isChainRequired":true,
"isKeyEncryptionRequired":false
}
```

Response

File is downloaded in the requested format.

Common Response Objects

This page contains fields that are used in APIs for add, update, and get certificate attributes. These fields are grouped together here because they are common to these APIs.

Parameters for CertificateGenericField

Name	Description
_id	Unique identifier for the attribute. **Type**: String
name	Name of the attribute. **Type**: String
type	Type of the attribute. **Type**: String
value	Default value for the attribute. **Type**: String
label	Label to be shown in the UI for the custom attribute. **Type**: String
searchKey	Keyword for searching the certificate based on the attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters for CertificateGenericField (continued)

Name	Description
	Type: String
mandatory	Indicates whether the attribute is mandatory or optional. **Type**: Boolean
category	The category of the attribute will always be "certAttributes" for certificate attributes. **Type**: String
helpInfo	Help information about the field. **Type**: String

Push and Bind Certificate to a Firewall Profile

The push and bind certificate to a firewall profile API uploads the certificate and its private keys to the firewall profile and links them to the server profiles. Refer to After you are done section to Approve and Implement the request.

Before you Begin

Ensure the following before attempting to push and bind certificate to a firewall profile through AppViewX:

- Firewall devices must be configured in AppViewX.
- The devices should be in the Managed state.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample URL:
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String
selectedProfiles	(Mandatory) Firewall profile id. **Type**: String **Constraint**: If the profile connector is specified then certificate is **pushed** and **bound** to the profile, but if a default connector is specified then the certificate is only **pushed**.
certificateDetails	(Mandatory) Certificate details for the Firewall devices. **Type**: Any of the following type (as per the firewall device) - Refer the Fortinet certificate details OR PaloAlto certificate details tables respectively.
pushDetails	(Optional) Other push details.
preValidationScriptPath pushDetails	(Optional) Location of the pre push script. **Type**: String
postValidationScriptPath pushDetails	(Optional) Location of the post push script. **Type**: String
overwrite pushDetails	(Optional) Indicates whether the certificate needs to be overwritten if already available. **Type**: Boolean
pushAutomatically pushDetails	(Optional) Indicates whether the certificate needs to be pushed automatically when renewed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Boolean

Fortinet certificate details

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: Value should be **PEM-.pem**.
certificateName	(Mandatory) Certificate name i.e. the name in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . It should not be the same as intermediate file name and CA file name.
privateKeyPassword	(Optional) Password for the private key pushed to the firewall device. **Type**: String
pushRootAndIntermediateCertificate	(Mandatory) Indicates whether the Root and Intermediate certificate are to be pushed to the firewall device. **Type**: Boolean **Constraint**: The value is either true or false.
rootCertificateFileName	(Mandatory) Root certificate name i.e. the name in which the root certificate is to be pushed to the firewall device. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Fortinet certificate details (continued)

Name	Description
	Constraint: The root certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.
intermediateCertificateFileName	(Mandatory) Intermediate certificate name i.e. the name in which the intermediate certificate is to be pushed to the firewall device. **Type**: String (multiple values) **Constraint**: The intermediate certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.

PaloAlto certificate details

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: Value should be **PEM-.pem** or **PKCS12-.p12**.
certificateName	(Mandatory) Certificate name i.e. the name in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . It should not be the same as intermediate file name and CA file name.
pushRootAndIntermediateCertificates	(Mandatory) Indicates whether the Root and Intermediate certificate are to be pushed to the firewall device. **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

PaloAlto certificate details (continued)

Name	Description
	Constraint: The value is either true or false.
rootCertificateFileName	(Mandatory) Root certificate name i.e. the name in which the root certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The root certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.
intermediateCertificateFileName	(Mandatory) Intermediate certificate name i.e. the name in which the intermediate certificate is to be pushed to the firewall device. **Type**: String (multiple values) **Constraint**: The intermediate certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for push action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	The selectedProfiles parameter is already available in the specified certificate. **Remediation**: Provide a different value for the selectedProfiles field.
404 Not Found	NO_RECORDS_FOUND	No matching records found - certificate not found. **Remediation**: Provide a correct value for the field certificateId.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0016	Connector with profiles {} already exists. **Remediation**: A profile connector is already available for the selected certificate. Change the certificateId or delete the existing connector.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload


```
{
 "certificateDetails": {
 "certificateType": "PEM-.pem",
 "certificateName": "testfile",
 "pushRootAndIntermediateCertificates": true,
 "rootCertificateFileName": "testrootfile.pem",
 "intermediateCertificateFileName": [
 "testinterfilelevel1.pem"
 ]
 },
 "pushDetails": {
 "preValidationScriptPath": "",
 "postValidationScriptPath": "",
 "overwrite": false,
 "pushAutomatically": false
 },
 "certificateId": "5f5b1fac77534426423bab57",
 "selectedProfiles": [
 "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST"
 ]
 }
```


Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
 "response": [
 {
 "requestId": "3",
 "connectorId": "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST:@389ed6f96387e3002cc6ac0678c07ffe70459abf"
 }
 ],
 "message": "1 connector(s) saved and push opertaion has been triggered.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Rollback certificate to firewall profile

The rollback certificate to a firewall profile API rolls back the certificate and its private keys to the firewall profile and links them to the server profiles. Refer to the After you are done section to Approve and Implement the request.

Before you begin

Ensure the following before attempting to rollback certificate to a firewall profile through AppViewX:

- Firewall devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/rollback
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
autoApproval *Query*	Indicates whether the auto-approval is needed for the action. **Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload	Contains all the parameters to be sent in the request body for the POST request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Body	**Type**: Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector id. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for rollback action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission. **Remediation**: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LIST_RETRIEVAL_FAILED	Unable to retrieve connector information. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	Application connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
"applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
}
```

Response

```
{
"response": "Success",
"message": "App connector rollback action initiated for 1 connector(s).",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Get Available Server Profiles

The get available server profiles API fetches the available profile details for the particular server device.

Before you begin

Ensure the following before attempting to fetch available profiles for a particular server device through AppViewX:

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.

Request Structure

Endpoint:	
Type:	GET

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample URL:	*https://<APPVIEWX_GATEWAY_IP:<APPVIEWX_GATEWAY_PORT/avxapi/certificate/profiles?gwkey=f000ca01&gwsource=external&category=Server&vendor=<Vendor>&certificateUuid=<resourceI*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
category	(Mandatory) It specifies the device category.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String **Constraint**: Required if sessionId is not provided.
vendor *Query*	Vendor for the chosen device. For example, **Apache** is a vendor for the Server category. It is a mandatory field. **Type**: String
certificateUuid *Query*	Uuid of the certificate. **Type**: String
deviceName *Query*	Name of the device as per AppViewX Device Inventory. **Type**: String
inventory *Query*	Name of AppViewX inventory where the certificate is present.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the fetch profiles request.
objects response	List of available device profile Ids. **Type**: String
totalRecords response	Total number of profiles fetched. **Type**: Integer
obtainedRecords	Total number of profiles fetched.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: Integer
obtainedRecordRange	Range of record found. **Type**: Object
response	
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	<<No. of profile Ids>> record(s) found
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	The mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Provide correct values for all the fields.
500 Internal Server Error	avx-common-011	Error while processing.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload

No payload for GET request

Response


```
{
"response":{
"objects":[
"ApacheLinux",
"ApacheLinux:@/etc/apache2:@xxx.xxx.xxx.xxx:@443:@/etc/apache2/sites-enabled/test.conf",
"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf",
"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-enabled/random-ssl.conf"
],
"totalRecords":4,
"obtainedRecords":4,
"obtainedRecordRange":{
"start":0,
"end":0
}
},
"message":"4 record(s) found",
"appStatusCode":null,
"tags":{

},
"headers":null
}
```


Push and Bind Certificate to a server profile

The push and bind certificate to a server profile API uploads the certificate and its private keys to the server device and links them to the server profiles. Refer to After you are done section to Approve and Implement the request.

Before you Begin

Ensure the following before attempting to push and bind certificate to a firewall profile through AppViewX:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String
selectedProfiles	(Mandatory) Server profile id. **Type**: String **Constraint**: If the profile connector is specified then certificate is **pushed** and **bound** to the profile, but if a default connector is specified then the certificate is only **pushed**.
certificateDetails	(Mandatory) Certificate details for the Firewall devices.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Any of the following type (as per the server device) - Refer the following: • Certificate details for IIS Server • Certificate details for Microsoft PC Server • Certificate details for Microsoft Server • Certificate details for Apache Linux Server • Certificate details for Tomcat Server • Certificate details for Weblogic Server • Certificate details for Websphere Server • Certificate details for IPlanet Server
pushDetails	(Optional) Other push details.
preValidationScriptPath pushDetails	(Optional) Location of the pre push script. **Type**: String
postValidationScriptPath pushDetails	(Optional) Location of the post push script. **Type**: String
overwrite pushDetails	(Optional) Indicates whether the certificate needs to be overwritten if already available. **Type**: Boolean **Constraint**: Enabled by default for IIS vendor.
pushAutomatically pushDetails	(Optional) Indicates whether the certificate needs to be pushed automatically when renewed. **Type**: Boolean

Certificate details for IIS Server

Name	Description
locationType	(Mandatory) Specifies whether the certificate should be uploaded to the certificate store or the centralized file system.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for IIS Server (continued)

Name	Description
	Type: String **Constraints**: The allowed values are **Certificate store** or **File system**.
keyStoreLocation	(Mandatory) When the locationType "Certificate store" is chosen, the keyStoreLocation determines the sub-store under which the certificate should be uploaded. **Type**: String **Constraints**: The allowed values are **Personal** or **Web Hosting**.
certificateLocation	(Optional) When the locationType "File system" is chosen, the certificateLocation specifies the actual folder location where the PFX file should be placed. **Type**: String **Constraints**: It is applicable only if the IIS server is managed with the centralized "file system". If the certificateLocation is left blank, the location specified during IIS server device addition is taken as the location.
certificateFileName	(Mandatory) The "certificate friendly name" under which the certificate should be stored in the Certificate store. In the case of a file system, it is the "certificate file name" with which the certificate should be stored in the file system. **Type**: String **Constraints**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, .
bindType	(Optional) Specifies whether the binding type is Update certificate binding only, Create new site binding, or Update site binding (port, hostname, SNI). **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for IIS Server (continued)

Name	Description
	Constraints: It is applicable for locationType as "Certificate store". The allowed values are **Update certificate only**, **Update site binding**, and **Create new site binding**.
IsSNIEnabled	(Optional) The Server Name Indication option to be mapped in IIS site binding. **Type**: Boolean **Constraints**: It is applicable when bindType is **Update site binding** or **Create new site binding**. It is also applicable for IIS versions >= 8.0.
hostName	(Optional) The hostname of the server that has to be updated in the site binding. **Type**: String **Constraints**: It is applicable when bindType is **Update site binding** or **Create new site binding**.
port	(Optional) The server port number that has to be updated in the site binding. **Type**: String **Constraints**: • It is applicable when bindType is **Update site binding** or **Create new site binding**. • This field is **mandatory** for for bindType **Create new site binding**. • The allowed values are between 1-65535.
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft PC Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The allowed values are **PKCS12-.pfx**.
certificateFileName	(Mandatory) The "certificate friendly name" under which the certificate should be stored in the Certificate store. **Type**: String **Constraints**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, .
pfxPassword	(Mandatory) The temporary password used during a certificate push. **Type**: String **Constraints**: The value must be base64 encoded.
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Certificate details for Microsoft Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, **DER-.cer**, **DER-.der**, **JKS-.jks**, **PKCS7-.p7b**, **PKCS7-.p7c**, **PKCS12-.p12**, and **PKCS12-.pfx**.
pushLocation	(Mandatory) The folder location in which certificate and private key are pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft Server (continued)

Name	Description
	Type: String
certificateFileName	(Mandatory) A user-defined file name for pushing the certificate into the Microsoft server. **Type**: String **Constraints**: The file name must be suffixed with the certificate format to be pushed e.g.: test.appviewx.com.pfx.
privateKeyFileName	(Mandatory) A user-defined file name for pushing the certificate into the Microsoft server. **Type**: String **Constraints**: The file name must be suffixed with the certificate format to be pushed, e.g.: test.appviewx.com.key. It is only applicable for types **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, **DER-.cer**, **DER-.der**, **PKCS7-.p7b**, and **PKCS7-.p7c**.
pfxPassword	(Optional) The password of pfx/p12 file. **Type**: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is only applicable for **JKS-.jks**certificate type.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
privateKeyPassword	(Optional) The private key entry password for the jks file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft Server (continued)

Name	Description
	Type: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean **Constraints**:
rootCertificateFileName	(Mandatory) A user-defined file name for pushing the root certificate into the Microsoft server. **Type**: String **Constraints**: The root certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The root certificate file name should also be different from both the CA file name and the intermediate certificate file name.
intermediateCertificateFileName	(Mandatory) A user-defined file name for pushing the intermediate certificate into the Microsoft server. **Type**: String **Constraints**: The intermediate certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The intermediate certificate file name should also be different from both the certificate file name and the CA file name.

Certificate details for Apache Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Apache Server (continued)

Name	Description
	Type: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, and **PEM-.pem**.
certificateLocation	(Mandatory) A user-defined directory name in which certificate and private key are pushed. **Type**: String **Constraints**: Mandatory if “isManualPush” is true.
certificateFileName	(Mandatory) A user-defined file name for pushing the certificate into the Apache server. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The CA file name should also be different from both the certificate file name and the CA file name.
keyLocation	(Optional) A user-defined directory for pushing the keys into the Apache server. **Type**: String **Constraints**: Mandatory if “isManualPush” is true.
privateKeyFileName	(Mandatory) A user-defined file name for pushing the keys into the Apache server. **Type**: String **Constraints**: The key file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Apache Server (continued)

Name	Description
	<, >, (,), ;, . The CA file name should also be different from both the certificate file name and the CA file name.
isRestartRequired	(Optional) Option to restart the service after the push operation. **Type**: Boolean
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
trustLocation	(Mandatory) A user-defined directory for pushing the root and intermediate certificate into the Apache server. **Type**: String **Constraints**: The root certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The CA file name should also be different from both the certificate file name and the CA file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Apache server. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. The root certificate file or bundle name should not begin or end with special characters. The special characters allowed are -, _, .. The root certificate file name should also be different from the certificate and intermediate certificate file name.
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Apache server. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Apache Server (continued)

Name	Description
	Constraints: Mandatory when “pushRootAndIntermediateCertificates” is true. The intermediate certificate file or bundle name should not begin or end with special characters. The special characters allowed are -, _, .. The intermediate certificate file name should also be different from the certificate and root certificate file name.
privateKeyInDevice	(Optional) Determines whether users need to push the private key into the device. **Type**: Boolean

Certificate details for Tomcat Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, and **JKS-.jks**.
certificateLocation	(Mandatory) A user-defined directory name in which certificate is pushed. **Type**: String
certificateFileName	(Mandatory) A user-defined file name for pushing the certificate into the Tomcat server. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The CA file name should also be different from both the CA file name and the intermediate certificate file name.
keyLocation	(Mandatory) A user-defined directory for pushing the keys into the Tomcat server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat Server (continued)

Name	Description
	Type: String
privateKeyFileName	(Mandatory) A user-defined file name for pushing the keys into the Tomcat server. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. . The private key file name should be same as the certificateFileName.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the Tomcat server. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**. Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Mandatory) The .jks file password. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean **Constraints**: It is applicable for certificate type **JKS-.jks**.
privateKeyLocation	(Optional) A user-defined directory for pushing the private keys into the Tomcat server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat Server (continued)

Name	Description
	Type: String **Constraints**: It is mandatory if “privateKeyInDevice” is true and is applicable only for certificate type **JKS-.jks**.
pushRootAndIntermediateCertificates	(Optional) Determines whether the root and intermediate certificate needs to be pushed to the device. **Type**: Boolean **Constraints**: It is applicable for all certificate types.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Tomcat server. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. The root certificate file or bundle name should not begin or end with special characters except -, _, .. The root certificate file name should also be different from the certificate and intermediate certificate file name.
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Apache server. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. The intermediate certificate file or bundle name should not begin or end with special characters except -, _, .. The intermediate certificate file name should also be different from the certificate and root certificate file name.
trustStoreLocation	(Optional) A user-defined store location for pushing the CA certificates into the device. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat Server (continued)

Name	Description
	Constraints: Mandatory when “pushRootAndIntermediateCertificates” is true. It is applicable for certificate type JKS-.jks. Provide the truststore location with the extension as **.jks** or **.truststore**.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: It is applicable for certificate type JKS-.jks.

Certificate details for Websphere Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **JKS-.jks**, and **PKCS12-.p12**.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the server device. **Type**: String **Constraints**: Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: Keystore password must have at least 6 characters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Websphere Server (continued)

Name	Description
trustStoreLocation	(Mandatory) A user-defined store location for pushing the CA certificates into the server device. **Type**: String **Constraints**: Provide the truststore location with the extension as **.jks** or **.truststore**. It is applicable only for certificate type JKS-.jks.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: Truststore password must have at least 6 characters. It is applicable only for certificate type JKS-.jks.
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.

Certificate details for Weblogic Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Weblogic Server (continued)

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **JKS-.jks**.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the server device. **Type**: String **Constraints**: Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: Keystore password must have at least 6 characters.
trustStoreLocation	(Mandatory) A user-defined store location for pushing the CA certificates into the server device. **Type**: String **Constraints**: Provide the truststore location with the extension as **.jks** or **.truststore**. It is applicable only for certificate type JKS-.jks.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: Truststore password must have at least 6 characters.
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Weblogic Server (continued)

Name	Description
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.

Certificate details for IPlanet Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PKCS12-.pfx**.
dbPath	(Mandatory) The database location for pushing the certificates into the server device. **Type**: String
dbPassword	(Optional) Password required to import certificates to database in server. **Type**: String
isRestartRequired	(Optional) Option to restart the service after the push operation. **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for IPlanet Server (continued)

Name	Description
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for push action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	selectedProfiles parameter is already available in the specified certificate. **Remediation**: Provide a different value for the selectedProfiles field.
404 Not Found	NO_RECORDS_FOUND	No matching records found - certificate not found. **Remediation**: Provide a correct value for the field certificateId.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0016	Connector with profiles {} already exists. **Remediation**: A profile connector is already available for the selected certificate. Change the certificateId or delete the existing connector.
500 Internal Server Error	avx-common-011	Error while processing.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
 "certificateDetails": {
 "certificateType": "PEM-.pem",
 "certificateName": "testfile",
 "pushRootAndIntermediateCertificates": true,
 "rootCertificateFileName": "testrootfile.pem",
 "intermediateCertificateFileName": [
 "testinterfilelevel1.pem"
 ]
 },
 "pushDetails": {
 "preValidationScriptPath": "",
 "postValidationScriptPath": "",
 "overwrite": false,
 "pushAutomatically": false
 },
 "certificateId": "5f5b1fac77534426423bab57",
 "selectedProfiles": [
 "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST"
 ]
 }
```


Response


```
{
 "response": [
 {
 "requestId": "3",
 "connectorId": "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST:@389ed6f96387e3002cc6ac0678c07ffe70459abf"
 }
 ],
 "message": "1 connector(s) saved and push operation has been triggered.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response for Apache Server

Request Payload


```
{
"certificateDetails": {
"certificateType": "PEM-.pem",
"certificateLocation": "/opt/automation",
"certificateFileName": "apachecertkeytest",
"keyLocation": "/opt/automation",
"privateKeyFileName": "apachecertkeytest.key",
"isRestartRequired":true,
"pushRootAndIntermediateCertificates": true,
"trustLocation":"/opt/automation",
"rootCertificateFileName": "apacheroottest.pem",
"intermediateCertificateFileName": [
"apacheintermediatetest.pem"
],
"privateKeyInDevice":true
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf"
]
}
```


Response


```
{
"response":[
{
"requestId":"54",
"connectorId":"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

"headers":null

}

Note:

- The above sample request and response can be followed for all three certificate types (PEM-.crt, PEM-.cer, PEM-.pem) for the Apache server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for IPlanet Server

Request Payload

{

"certificateDetails": {

"isManualPush":true,

"certificateType": "PKCS12-.pfx",

"dbPath": "/opt/automation/db",

"dbPassword": "YXBwd==26",

"isRestartRequired":false,

"privateKeyInDevice": true,

"privateKeyLocation":"/opt/automation/keys",

},

"certificateId": "605dbd66ccb1c49e108e67e6",

"selectedProfiles": [

"iPlanet:@8443:@localhost:@localhost:"

]

}

Response

{

"response":[

{

"requestId":"60",

"connectorId":"iPlanet:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"

}

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed PKCS12 certificate type (PKCS12-.pfx) for the IPlanet server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Tomcat Server

Request Payload


```
{
"certificateDetails": {
"certificateType": "PEM-.pem",
"certificateLocation": "/opt/automation",
"certificateFileName": "tomcatcertkeytest",
"keyLocation": "/opt/automation",
"privateKeyFileName": "tomcatcertkeytest.key",
"pushRootAndIntermediateCertificates": true,
"rootCertificateFileName": "tomcatroottest.pem",
"intermediateCertificateFileName": [
"tomcatintermediatetest.pem"
]
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"TomcatLinux:@8443:@localhost:@localhost:"
]
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response


```
{
"response":[
{
"requestId":"57",
"connectorId":"TomcatLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for all three certificate types (PEM-.crt, PEM-.cer, PEM-.pem) for the Tomcat server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Weblogic Server

Sample Request


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "JKS-.jks",
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"trustStoreLocation": "/opt/automation/trust.jks",
"trustStorePassword": "YXBwd==26"
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"Weblogic:@8443:@localhost:@localhost:"
]
}
```


Sample Response


```
{
"response":[
{
"requestId":"58",
"connectorId":"Weblogic:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for JKS certificate type (JKS.jks) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Websphere Server

Request Payload


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "JKS-.jks",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"trustStoreLocation": "/opt/automation/trust.jks",
"trustStorePassword": "YXBwd==26"
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"WebsphereLinux:@8443:@localhost:@localhost:"
]
}
```


Response


```
{
"response":[
{
"requestId":"58",
"connectorId":"WebsphereLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for JKS certificate type (JKS.jks) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Payload


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "PKCS12-.p12",
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
},
"pushDetails": {
"preValidationScriptPath": "",
"postValidationScriptPath": "",
"pushAutomatically": false
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"WebsphereLinux:@8443:@localhost:@localhost:"
]
}
```


Response


```
{
"response":[
{
"requestId":"59",
"connectorId":"WebsphereLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note:

- The above sample request and response can be followed for PKCS12 certificate type (PKCS12-.p12) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Rollback Certificate to server profile

The rollback certificate to a server profile API rolls back the certificate and its private keys to the server profile and links them to the server profiles. Refer to the After you are done section to Approve and Implement the request.

Before you begin

Ensure the following before attempting to rollback certificate to a server profile through AppViewX:

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/rollback
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
autoApproval *Query*	(Mandatory) Indicates whether the auto-approval is needed for the action. **Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload	Contains all the parameters to be sent in the request body for the post request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Body	**Type**: Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector id. **Type**: List <String>

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for rollback action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission. **Remediation**: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LIST_RETRIEVAL_FAILED	Unable to retrieve connector information. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	Application connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
 "applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```

Note: Please refer to the "Request Structure" to identify the changeable values.

Response

```
{
 "response": "Success",
 "message": "App connector rollback action initiated for 1 connector(s).",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

After you are done

- Once an action has been triggered, a request will be created for that.
- Requests have to be approved using the Approve request action.
- Requests have to be approved using the Implement request action.
- Approve a Request
- Implement Request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Approve a Request

The approve a request API approves the certificate request.

Request Structure

Endpoint:	/certificate/workorder/update
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**.
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: String
gwsource	(Mandatory) Source from which the request is triggered. (E.g. external)
Query	**Type**: String
Payload	Contains all the parameters to be sent in the request body for the POST request.
Body	**Type**: Payload

Payload

Name	Description
data	(Mandatory) Contains the action data.
	Type: String
task_action	(Mandatory) Action to be performed.
data	**Type**: Number
	Constraint: Values are **1** for approve and **2** for reject.
header	(Mandatory) Contains the request details.
	Type: String
request_id	Id of the request.
header	**Type**: String
workorder_id	Id of the workorder.
header	**Type**: String
	Constraint: Value should be **0**.
task_id	Id of the task to be performed.
header	**Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Value should be **review_1**.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the approve request.
requestId response	Request id for approve action for the application connector. **Type**: String
message response	Success message of the action or a failure description in case of an error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Request submitted to workflow engine for processing workflow request 14.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 Not Found	engine-db-011	Request not found. **Remediation**: Ensure that a valid value is provided for the request_id field in the request.

Sample Request/Response

Request Payload


```
{
 "data": {
 "task_action": 1
 },
 "header": {
 "request_id": "14",
 "workorder_id": "0",
 "task_id": "review_1"
 }
 }
```


Response


```
{
 "response": {
 "message": "Request submitted to workflow engine for processing workflow request 14",
 "requestId": "14"
 },
 "message": "Success",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


- Request Structure
- Response Structure

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Status codes
- Sample Request/Response

Request Structure

URL: */certificate/workorder/update*

Type: `POST`

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if `username` and `password` are not provided.
`username`	Header	AppViewX login username.	`String`	Required if `sessionId` is not provided.
`password`	Header	AppViewX login password.	`String`	Required if `sessionId` is not provided.
`Content-Type`	Header	Specifies the nature of the data in the payload.	`String`	Value of the param should be '**application/json**'.
`gwkey`	Query	Tenant Key. This is needed only in case of multi tenant installations and can be ignored in other type of installations.	`String`	NA
`gwsource`	Query	Source from which the request is triggered (E.g. external).	`String`	NA
`Payload`	Body	Contains all the params to be sent in the request body for the post request.	`Payload`	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
`data`	Yes	Action data.	`Data`	NA
`header`	Yes	Request details.	`Header`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Data

Name	Mandatory	Description	Field Type	Constraints
task_action	Yes	Action to be performed.	Number	1 - approve 2 - reject

Header

Name	Mandatory	Description	Field Type	Constraints
request_id	Yes	Id of the request.	String	NA
workorder_id	Yes	Id of the work order.	String	Value should be **0**.
task_id	Yes	Id of the task to be performed.	String	Value should be **review_1**.

Response Structure

202 Accepted returns string of type application/json with the following body params.

Name	Description	Field Type
response	Contains the response attributes for the approve request.	response
message	Success message of the action or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

response

Name	Description	Field Type
requestId	Request Id for approve action for the application connector.	String
message	Success message of the action or failure description in case of error.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status codes

HTTP Status code	appStatusCode	Message	Possible remediation
200 OK	NA	Request submitted to workflow engine for processing workflow request 14.	NA
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.	Ensure that valid `username` and `password` or valid `sessionId` is provided as header param.
404 Not Found	engine-db-011	Request not found.	Check and ensure that valid value is provided for `request_id` field in the request.

Sample Request/Response

- Sample Request:
- Sample Response:

Sample Request:

```
{
"data": {
"task_action": 1
},
"header": {
"request_id": "14",
"workorder_id": "0",
"task_id": "review_1"
}
}
```

Note: Please refer to the "Request Structure" to identify the changeable values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Response:


```
{
"response": {
"message": "Request submitted to workflow engine for processing workflow request 14",
"requestId": "14"
},
"message": "Success",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Implement Request

The implement request API implements the request for the certificate.

Request Structure

Endpoint:	/certificate/workorder/update
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the POST request. **Type**: Payload

Payload

Name	Description
data	(Mandatory) Contains the action data. **Type**: String
task_action data	(Mandatory) Action to be performed. **Type**: Number **Constraint**: Values are **1** for approve and **2** for reject.
header	(Mandatory) Contains the request details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
request_id	Id of the request.
header	**Type**: String
workorder_id	Id of the workorder.
header	**Type**: String
	Constraint: Value should be **0**.
task_id	Id of the task to be performed.
header	**Type**: String
	Constraint: Value should be **review_1**.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the implement request.
requestId	Request id for implement action for the application connector.
response	**Type**: String
message	Success message of the action or a failure description in case of an error.
response	**Type**: String
message	Success message or failure description in case of error.
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Request submitted to workflow engine for processing workflow request 14.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 Not Found	engine-db-011	Request not found. **Remediation**: Ensure that a valid value is provided for the request_id field in the request.

Sample Request/Response

Request Payload


```
{
 "data": {
 "task_action": 1
 },
 "header": {
 "request_id": "14",
 "workorder_id": "0",
 "task_id": "review_2"
 }
 }
```


Response


```
{
"response": {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"message": "Request submitted to workflow engine for processing workflow request 14",
"requestId": "14"
},
"message": "Success",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


- Request Structure
- Response Structure
- Status codes
- Sample Request/Response

Request Structure

URL: */certificate/workorder/update*

Type: `POST`

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if `username` and `password` are not provided.
`username`	Header	AppViewX login username.	`String`	Required if `sessionId` is not provided.
`password`	Header	AppViewX login password.	`String`	Required if `sessionId` is not provided.
`Content-Type`	Header	Specifies the nature of the data in the payload.	`String`	Value of the param should be '**application/json**'.
`gwkey`	Query	Tenant Key. This is needed only in case of multi tenant installations and can be ignored in other type of installations.	`String`	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
gwsource	Query	Source from which the request is triggered (E.g. external).	String	
Payload	Body	Contains all the params to be sent in the request body for the post request.	Payload	

Payload

Name	Mandatory	Description	Field Type	Constraints
data	Yes	Action data.	Data	
header	Yes	Request details.	Header	

Data

Name	Mandatory	Description	Field Type	Constraints
task_action	Yes	Action to be performed.	Number	1 - implement 2 - reject

Header

Name	Mandatory	Description	Field Type	Constraints
request_id	Yes	Id of the request.	String	
workorder_id	Yes	Id of the work order.	String	Value should be **0**.
task_id	Yes	Id of the task to be performed.	String	Value should be **review_1**.

Response Structure

202 Accepted returns string of type application/json with the following body params.

Name	Description	Field Type
response	Contains the response attributes for the implement request.	response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
message	Success message of the action or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	

response

Name	Description	Field Type
requestId	Request Id for implement action for the application connector.	String
message	Success message of the action or failure description in case of error.	String

Status codes

HTTP Status code	appStatusCode	Message	Possible remediation
200 OK	-	Request submitted to workflow engine for processing workflow request 14.	-
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.	Ensure that valid username and password or valid sessionId is provided as header param.
404 Not Found	engine-db-011	Request not found.	Check and ensure that valid value is provided for request_id field in the request.

Sample Request/Response

- Sample Request:
- Sample Response:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request:


```
{
"data": {
"task_action": 1
},
"header": {
"request_id": "14",
"workorder_id": "0",
"task_id": "review_2"
}
}
```


Note: Please refer to the "Request Structure" to identify the changeable values.

Sample Response:


```
{
"response": {
"message": "Request submitted to workflow engine for processing workflow request 14",
"requestId": "14"
},
"message": "Success",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Download Private Key of a Certificate

The download private key of a certificate API downloads the private key of a certificate in the password protected PEM format. Users can also request for a private key.

Request Structure

Endpoint:	/certificate/privatekey/download
Type:	POST

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample URL:
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
uuId	(Mandatory) Format required. **Type**: String **Constraint**: Uuid of the certificate
password	(Optional) Password for encrypting the private key in the response. **Type**: String

Response Structure

Error Response Parameters

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
privateKeyPemEncoded	Private key of certificate in password encrypted pem. **Type**: String
success	**True** if download is successful and **False** if error in downloading. **Type**: Boolean
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-GEN-0015	Field cannot be null/empty.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure the mandatory fields have valid value in the request. It should not be null or empty.
417 Expectation failed	CERT-KEY-0006	Private key access is restricted in <policy> policy. **Remediation**: Enable private key access in the mentioned policy.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid. **Remediation**: Ensure all the mandatory fields have valid value in the request.
500 Internal Server Error	CERT-GEN-0027	Certificate private key download failed.

Sample Request/Response

Request Payload

```
{


}
```

Success Response


```
{
 "response": {
 "status": "Success",
 "zipFileName": null,
 "certContents": null,
 "privateKeyPemEncoded": "-----BEGIN ENCRYPTED PRIVATE
 KEY-----\nMIIE9jAoBgoqhkiG9w0BDAEDMBoEFEC4EngLMd1kbUJjHxgNyvApBAMFAgIIAASC\nBMhv4AkofevTbEa0BZ3HLOI/WIHelmYmHtwC26SDI1JGJWK
UN1O0W52rIn30mjZG\niUxiu7F3ozQgrKBCHuM+lKxx4zYbmgukyodJtbzJ4EohmapiZQHJSf4DiJiHHa8X\nZ/r
+sfNoRunhy3r/0SS0lNZqQvnM5dqSATkHTtrcD82NsKIx4GScFfG5yKhoAsS6\nEJQag7THPAbwaRPml54UZBsFnjmkG638utC511EWdbD0Z12L4zxhzPNxgnYF
NQEg\n12552kjj5jGNZgojxZ52BpWe0ZfDkH+bvt7LC9M62n4d5vrivlfBd6R7ZMjDAD0M\nn2vtltgoKe9Nbxq/5oraGJt+8ql/sWlGWehx/L8Ue/weCzXtmectQd69M4id
K7QQ\nAwOh/cdosut6uQUGzIrH3n59INWbkJ0HzlunJjLcvJzrhr191SYmMU0HNPjaVptD\n
+UErWYqs4y1XEwOn1jrNQ8cBA0VvkwhAu1juWc0hoY9s6tv573dnljrNAtiVOtw4\nl3CsQlNMAXSHizpaM6pKXh8mCHfgZqzDmbmDTTDc9A37ekgnDfSRCEgzR
KQl4bJT\noXYRJFTyjGqT4HdC9pKaj3B+IHfWae5iWOB5kCdaE9qCc9NjN8WzPed3U3ltNNzC\neW3mYihP+
+XCB9uNHyLZ9jCXh42RCCW/omVlgZR9VBvhrq3tmk8MCYp+cFdo2KsH\nlC+MAVL6NPI4jcGBNt2JUMG5coPXttF2OsHqucH95WqUDUBF5+ZmpvJSuCFb8
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
SEc\nvAH35lwJnanZs4hPIlgywkRcIdu+Mv
+lseOqFQvRypeRKPLGlWqZQZ83J5P2ENhv\nhQLv9hrYLKzpo4oMk4GTFeLNvYnayAa5sqAOACoI8QZRmjUPVffG3KEQ6F3vOTdX\n1BrpeSH6rbolqEUTcBpc
agf+1XdoZ4f3h76K0yVH1KVE8Gz2uQvWqm33UThVU2ra\n0kWLxO2tz3tN0m21MLQhU4bWDMT5Yz5GdsLLQQgkiIzZ7vwfnYT6xtTPTJLre0X+
\n927vNJnhVgtdydutSIMf+m
+tH3knZ35K8MCBH7lLV+Ov0dj4DSbD/44eMuBOP7KW\n8u4FK0Mys4EeBc2nH9tQ/HTSDCRJGj8sycRHZGGCRRAuFtIBXy0F9lnbaoTCNnIS\ngeW/ZjuSBHH0
csNxvJZS3rr62Pnl14IOueM5cklLa02LqON/gdRZwXQm7i0sOTEC\nvhX4Y3RgJ8+IZYx3MyeNKuUBFOuyRcl3my/C6K9okMyQhAgXr16YR/v/ioKihX8/\nRH0RC9
OrSy6ad0lLRhye9/giEJ2JBfKq8QwwRUO1peD7lrzsde6gD8c9XRmbshgu\ndU00dmL0a26H/h
+/T9UnS5D1KJUROHXeCX2ywakw/k1hR9xfiQsYJ6FVXGC38POW\nVnOK4gmRnGQPfDsqZJ32bm+cyqQ2nmXYHxGQO1S0k+U5JlmPk9EruaWal2rud8wO\nd
AcT/ZUxaBXXjwRnOAr142Hh939KuMcb7lK7as0Ku2xoBxLSGFIkaQXCnLVavs1C\nGNs0ZrN9rDwua7e7VTug08oI0H0Fvqt5cgQAaFTDjM6Usy7AoKJVoP4jl4Us
W78m\nTRAnJLIfDxCBX5b315bMMg5uTpZRDcIybY0=\n-----END ENCRYPTED PRIVATE KEY-----\n",
 "success": true,
 "log": false
 },
 "message": "private key downloaded successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Delete Certificate using UUID

The delete certificate using UUID API deletes the certificates using the Universal Unique Identifier (UUID). The UUID is a unique id for each certificate. This id remains the same even if the certificate is generated numerous times. It is generated based on certain attributes and properties of the certificate.

Request Structure

Endpoint:	/certificate/delete
Type:	DELETE
Sample URL:	https://192.168.150.63:31443/avxapi/certificate/delete? gwsource=external&commonName={commonName}&serialNumber={serialNumber}
Headers	
Content-Type:	application/json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Name	Description
certIds	(Mandatory) Format required.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Array **Constraint**: Uuid of the certificate to be deleted.

Response Structure

Error Response Parameters

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-CA-0047	Cert Ids cannot be empty. **Remediation**: Provide UUIDs in the request to delete certificates.
417 Expectation failed	CERT-HLST-0019	The operation cannot be completed as {} selected certificate(s) are in Read-Only access groups. **Remediation**: Change the permissions in the required access group.
400 Not Found	CERT-INV-0021	Requested certificate is not available in the inventory. **Remediation**: Provide uuids that are available in the inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
500 Internal Server Error	CERT-GEN-0028	Certificate Limit Exceed. **Remediation**: Cannot delete more than 100 certificates.

Sample Request/Response

Request Payload

```
{


}
```

Success Response

```
{
 {
 "response": {
 "code": "CERTIFICATE_DELETION_SUCCESSFULL",
 "message": "Selected certificate(s) has been deleted successfully from AppViewX inventory."
 },
 "message": null,
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```

CERT+ ADC API

- Push and Bind Certificate to a ADC Profile
- Push and Bind Certificate to ADC Devices
- Rollback to ADC profile

Push and Bind Certificate to a ADC Profile

The API initiates a push of the certificate along with the private keys to the ADC devices and associates them to the device profiles.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before You Begin

Ensure the following before attempting to push a certificate to a particular ADC device through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state.

Fetch Available Profiles API

Endpoint:	/certificate/profiles
Type:	GET
Sample URL:	*https://<appviewx node ip>:<gateway port>/avxapi/certificate/profiles?gwkey=f000ca01&category=ADC&vendor=F5&deviceName=F5_device&gwsource=external*
Headers	
Content-Type:	application/json

Request Details - Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters (continued)

Name	Description
	Constraint: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
category *Query*	(Mandatory) Specifies the device category. **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor *Query*	(Mandatory) Vendor for the chosen device. For example, **F5** is a vendor for the ADC category. **Type**: String **Possible values**: F5, Citrix, AVI, A10, AmazonELB, NginxPlus, and HAProxy.
certificateUuid *Query*	(Mandatory) Resource id of the certificate. **Type**: String **Constraints**: This can be obtained from search API.
deviceName *Query*	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
inventory *Query*	(Mandatory) Name of AppViewX inventory where the certificate is present. **Type**: String **Possible values**: Server, Client, Code Signing, and Device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Parameters

Name	Description
response	Contains the following response attributes for the fetch profiles request: objects, totalRecords, obtainedRecords, and obtainedRecordRange.
objects response	List of available device profile Ids. **Type**: List of String
totalRecords response	Total number of profiles fetched. **Type**: Integer
obtainedRecords response	Total number of profiles fetched. **Type**: Integer
obtainedRecordRange response	Range of record found. **Type**: Object
message	Success message of the action or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Response


```
{
 "response": {
 "objects": [
 "device_name",
 "device_name:@apm-default-serverssl:@Common",
 "device_name:@clientssl-insecure-compatible:@Common",
 "device_name:@clientssl-secure:@Common",
 "device_name:@clientssl:@Common",
 "device_name:@crypto-client-default-serverssl:@Common",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description

"device_name:@crypto-server-default-clientssl:@Common",

"device_name:@pcoip-default-serverssl:@Common",

"device_name:@serverssl-insecure-compatible:@Common",

"device_name:@serverssl:@Common",

"device_name:@splitsession-default-clientssl:@Common",

"device_name:@splitsession-default-serverssl:@Common",

"device_name:@wom-default-clientssl:@Common",

"device_name:@wom-default-serverssl:@Common"

],

"totalRecords": 14,

"obtainedRecords": 14,

"obtainedRecordRange": {

"start": 0,

"end": 0

}

},

"message": "14 record(s) found",

"appStatusCode": null,

"tags": {},

"headers": null

}

Request Structure for Push and Bind ASYNC API

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: Optional if the Uuid of the certificate is present.
ceritifcateUuid	(Optional) Certificate UUid **Type**: String **Constraint**: Mandatory only if certificateId is not present.
selectedProfiles	(Mandatory) ADC device profile id. **Type**: String **Constraint**: These can be obtained from Fetch Available Profiles API • If a Profile connector is specified, then the certificate will be pushed and bound to the profile. • If a Default connector specified, then the certificate will be only pushed.
certificateDetails	(Mandatory) Certificate details for the server devices to be pushed. **Type**: Any of the following server devices: • Certificate details for F5 • Certificate details for Citrix • Certificate details for AVI • Certificate details for A10 • Certificate details for AmazonELB • Certificate details for NignixPlus • Certificate details for HAProxy

Certificate details for F5

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description
	Possible Certificate types: PEM-.crt
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into an F5 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into an F5 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user defined file name for pushing the intermediate and root certificates into in a F5 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles": [
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description


```
"device_name:@default:@clientssl"

],

"certificateDetails": {

"certificateFileName": "test123.crt",

"certificateType": "PEM-.crt",

"privateKeyFileName": "test123.key",

"pushRootAndIntermediateCertificates": true,

"rootCertificateFileName": "test123_root.crt"

}

}
```


Response


```
{

"response": [

{

"requestId": "156",

"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"

}

],

"message": "1 connector(s) saved and push opertaion has been triggered.",

"appStatusCode": null,

"tags": {},

"headers": null

}
```


Certificate details for Citrix

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.crt, PEM-.cer, PEM-.pem, DER-.der, and DER-.cer

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the Citrix device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the Citrix device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
	Constraints: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload


```
{
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles": [
"device_name:@default:@sslvs"
],
"certificateDetails": {
"certificateFileName": "test123.crt",
"certificateKeyPairName": "test123",
"certificateType": "PEM-.crt",
"intermediateCertificateFileName": [
"test123_inter.crt"
],
"privateKeyFileName": "test123.key",
"pushRootAndIntermediateCertificates": true,
"rootCertificateFileName": "test123_root.crt",
"sniCert": "false",
"sniStatus": "false"
}
}
```


Response


```
{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
"tags": {}, "headers": null }	

Certificate details for AVI

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the AVI device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the AVI device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
	Type: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PEM-.pem”,
 "certificateFileName":"certificate_push.pem",
 "privateKeyFileName":"certificate_push.key",
 "pushRootAndIntermediateCertificates": true,
 “intermediateCertificateFileNames”:[“test_cert_inter.crt”],
 "rootCertificateFileName": "test_cert_ca.crt"
 }
 }
```

Response

```
{
"response": [
 {
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
"requestId": "156", "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e" }], "message": "1 connector(s) saved and push opertaion has been triggered.", "appStatusCode": null, "tags": {}, "headers": null }	

Certificate details for A10

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, PEM-.cer, DER-.der, DER-.cer, PKCS#7-.p7b, PKCS#7-.p7c, PKCS#7-.p12, and PKCS#7-.pfx
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the A10 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the A10 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
pfxPassword	(Optional) Password for the **pfx** and **pkcs12** file type. It is **mandatory** only if the certificate file type is **.pfx** or **.pkcs12**. **Type**: Boolean **Constraints**: The password should be Base64 encoded.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the A10 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request payload for non pfx and p12 cert types

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.crt”,
"certificateFileName":"certificate_push.crt",
"privateKeyFileName":"certificate_push.key",
"pushRootAndIntermediateCertificates": true,
"intermediateCertificateFileNames":[ "test_cert_ca.crt"]
}
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory

Request payload for pfx and p12 cert types


```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PKCS-.pfx”,
"certificateFileName":"certificate_push.pfx",
"pushRootAndIntermediateCertificates": true,
"intermediateCertificateFileNames":[ "test_cert_ca.crt"],
“pfxPassword”:”cGFzc3dvcmQ=”
}
}
```


Response


```
{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Certificate details for AmazonELB

Name	Mandatory
certificateType	(Mandatory) Type of the certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory
	Type: String **Possible Certificate types**: PEM-.pem
certificateLocation	(Mandatory) Location of the certificate. Values are **ACM** or **IAM**. **Type**: String
certCAReferenceId	(Optional) Reference ID to input the certificate location. It is **mandatory** if certificateLocation is **ACM**. **Type**: String **Constraints**: The special characters allowed are ('=', '/', ',', '.', '@', '-').
certificateFileName	(Optional) A user defined file name for pushing the certificate into the AmazonELB device. It is **mandatory** if certificateLocation is **IAM**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the CA file name and intermediate certificate file name.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Request payload if certificateLocation is ACM

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certCAReferenceId”: "arn:aws:iam::2313:amazonELB"
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory
“certificateLocation”: "ACM" “certificateType”: "PEM-.pem" “pushRootAndIntermediateCertificates”: true }	

Request payload if certificateLocation is IAM

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateFileName: "sample.pem",
 “certificateLocation”: "IAM",
 “certificateType”: "PEM-.pem",
 “pushRootAndIntermediateCertificates”: true
 }
```

Response

```
{
"response": [
 {
 "requestId": "156",
 "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
 }
 ],
 "message": "1 connector(s) saved and push opertaion has been triggered.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, and PEM-.cer
certificateLocation	(Mandatory) A user defined file name for pushing the certificate into the NginxPlus device. **Type**: String **Constraints**: The certificate file name should not begin and end with special characters except -, ., _. It should not be the same as CA file name and intermediate file name.
keyLocation	(Mandatory) A user defined file for pushing the key into the NginxPlus device. **Type**: String **Constraints**: The key file name should not begin and end with special characters except -, ., _. Key file name should be same as certificateFileName.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean

Request Payload

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateLocation":"/home/appviewx",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus (continued)

Name	Mandatory
"keyLocation":"/home/appviewx", "privateKeyInDevice": true } }	

Response


```
{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Certificate details for HAProxy

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the HAProxy device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy (continued)

Name	Mandatory
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean
privateKeyLocation	(Mandatory) A user defined file name for pushing the keys into the HAProxy device. It is **mandatory** if privateKeyInDevice is **true**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.

Request Payload

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PEM-.pem”,
 "certificateFileName":"/opt/haproxy/certificate_push.pem",
 "privateKeyLocation": true,
 "privateKeyLocation": "/opt/haproxy/test_cert.key"
 }
 }
```

Response

```
{
 "response": [
 {
 "requestId": "156",
 "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
 }
 ],
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy (continued)

Name	Mandatory
"message": "1 connector(s) saved and push opertaion has been triggered.", "appStatusCode": null, "tags": {}, "headers": null }	

Response Structure for Push and Bind ASYNC API

Note: The response details/parameters are common for all vendor devices.

Parameters

Name	Description
response	Contains Request id and connector id. **Type**: Object
requestId response	Request Id for push action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success or failure messages **Type**: String
appStatusCode	Application specific status code for the response. **Type**: String
tags	More info in case of failure response **Type**: Object
headers	Details of the response headers if any

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: Object

Sample Response (common for all vendors)


```
{
 "response": [
 {
 "requestId": "156",
 "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
 }
 ],
 "message": "1 connector(s) saved and push opertaion has been triggered.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Push and Bind Certificate to ADC Devices

This API initiates a push of the certificate to ADC devices [F5, Citrix, AVI, A10, AmazonELB, NginxPlus, HAProxy] and bind it to a profile or virtual server depending on the ADC device.

Before you begin

Ensure the following before attempting to push a certificate to a particular ADC device through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state.
- A valid certificate should be used to push the certificate.
- Profiles or virtual servers should be available. This can be fetched using **Fetch Available Profiles API** (refer section below).

Fetch available profiles API

Endpoint:	/certificate/profiles

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Type:	GET
Sample URL:	*https://<appviewx node ip>:<gateway port>/avxapi/certificate/profiles?gwkey=f000ca01&category=ADC&vendor=F5&deviceName=F5_device&gwsource=external*
Headers	
Content-Type:	application/json

Request Details - Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters (continued)

Name	Description
category *Query*	(Mandatory) Specifies the device category. **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor *Query*	(Mandatory) Vendor for the chosen device. For example, **F5** is a vendor for the ADC category. **Type**: String **Possible values**: F5, Citrix, AVI, A10, AmazonELB, NginxPlus, and HAProxy.
certificateUuid *Query*	(Mandatory) Resource id of the certificate. **Type**: String **Constraints**: This can be obtained from search API.
deviceName *Query*	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
inventory *Query*	(Mandatory) Name of AppViewX inventory where the certificate is present. **Type**: String **Possible values**: Server, Client, Code Signing, and Device.

Response Parameters

Name	Description
response	Contains the following response attributes for the fetch profiles request: objects, totalRecords, obtainedRecords, and obtainedRecordRange. **Type**: List of Objects
objects response	List of available device profile Ids. **Type**: List of String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
totalRecords response	Total number of profiles fetched. **Type**: Integer
obtainedRecords response	Total number of profiles fetched. **Type**: Integer
obtainedRecordRange response	Range of record found. **Type**: Object
message	Success message of the action or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Response


```
{
 "response": {
 "objects": [
 "device_name",
 "device_name:@apm-default-serverssl:@Common",
 "device_name:@clientssl-insecure-compatible:@Common",
 "device_name:@clientssl-secure:@Common",
 "device_name:@clientssl:@Common",
 "device_name:@crypto-client-default-serverssl:@Common",
 "device_name:@crypto-server-default-clientssl:@Common",
 "device_name:@pcoip-default-serverssl:@Common",
 "device_name:@serverssl-insecure-compatible:@Common",
 "device_name:@serverssl:@Common",
 "device_name:@splitsession-default-clientssl:@Common",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description

"device_name:@splitsession-default-serverssl:@Common",
"device_name:@wom-default-clientssl:@Common",
"device_name:@wom-default-serverssl:@Common"
],
"totalRecords": 14,
"obtainedRecords": 14,
"obtainedRecordRange": {
"start": 0,
"end": 0
}
},
"message": "14 record(s) found",
"appStatusCode": null,
"tags": {},
"headers": null
}	

Request Structure for Push and Bind SYNC API

Endpoint:	/certificate/profiles/push
Type:	POST
Sample URL:	*https://<appviewx node id>:<gateway port>/avxapi/certificate/profiles/push?gwkey=f000ca01&gwsource=external&ttl=120*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String **Constraint**: Required if username and password are not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
ttl *Query*	(Mandatry) The time to live (**ttl**) is a query parameter. If the total time taken surpasses this value, the response will indicate that the request is still in progress. On the other hand, if the operation completes successfully within the TTL, the response will indicate success. **Type**: Integer
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String **Constraint**: Optional if the Uuid of the certificate is present.
ceritifcateUuid	(Optional) Certificate UUid **Type**: String **Constraint**: Mandatory only if certificateId is not present.
selectedProfiles	(Mandatory) ADC device profile id. **Type**: List of String **Constraint**: These can be obtained from Fetch Available Profiles API. • If a Profile connector is specified, then the certificate will be pushed and bound to the profile. • If a Default connector specified, then the certificate will be only pushed.
certificateDetails	(Mandatory) Certificate details for the server devices to be pushed. **Type**: Any of the following server devices: • Certificate details for F5 • Certificate details for Citrix • Certificate details for AVI • Certificate details for A10 • Certificate details for AmazonELB • Certificate details for NignixPlus • Certificate details for HAProxy

Certificate details for F5

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description
	Possible Certificate types: PEM-.crt
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into an F5 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the CA file name and intermediate certificate file name.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into an F5 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user defined file name for pushing the intermediate and root certificates into in a F5 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description

"selectedProfiles": [
"device_name:@default:@clientssl"
],
"certificateDetails": {
"certificateFileName": "test123.crt",
"certificateType": "PEM-.crt",
"privateKeyFileName": "test123.key",
"pushRootAndIntermediateCertificates": true,
"rootCertificateFileName": "test123_root.crt"
}
}	

Certificate details for Citrix

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.crt, PEM-.cer, PEM-.pem, DER-.der, and DER-.cer
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the Citrix device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the Citrix device. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
	Constraints: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
sniCert	(Optional) Enables the SNI push for certificate. **Type**: Boolean
sniStatus	(Optional) Enables SNI in the virtual server. **Type**: Boolean

Request Payload


```
{
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles": [
 "device_name:@default:@sslvs"
 ],
 "certificateDetails": {
 "certificateFileName": "test123.crt",
 "certificateKeyPairName": "test123",
 "certificateType": "PEM-.crt",
 "intermediateCertificateFileName": [
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
"test123_inter.crt"], "privateKeyFileName": "test123.key", "pushRootAndIntermediateCertificates": true, "rootCertificateFileName": "test123_root.crt", "sniCert": "false", "sniStatus": "false" } }	

Certificate details for AVI

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the AVI device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the AVI device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PEM-.pem”,
 "certificateFileName":"certificate_push.pem",
 "privateKeyFileName":"certificate_push.key",
 "pushRootAndIntermediateCertificates": true,
 “intermediateCertificateFileNames”:[”test_cert_inter.crt”],
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
"rootCertificateFileName": "test_cert_ca.crt" } }	

Certificate details for A10

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, PEM-.cer, DER-.der, DER-.cer, PKCS#7-.p7b, PKCS#7-.p7c, PKCS#7-.p12, and PKCS#7-.pfx
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the A10 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the A10 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pfxPassword	(Optional) Password for the **pfx** and **pkcs12** file type. It is **mandatory** only if the certificate file type is **.pfx** or **.pkcs12**. **Type**: Boolean **Constraints**: The password should be Base64 encoded.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the A10 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request payload for non pfx and p12 cert types

```
{ "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
        "selectedProfiles":[ "device_name:@serverssl-insecure-compatible:@Common" ],
        "certificateDetails":{ “certificateType”:”PEM-.crt”,
        "certificateFileName":"certificate_push.crt",
        "privateKeyFileName":"certificate_push.key", "pushRootAndIntermediateCertificates":
        true, "intermediateCertificateFileNames":[ "test_cert_ca.crt"] } }
```

Request payload for pfx and p12 cert types

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PKCS-.pfx”,
 "certificateFileName":"certificate_push.pfx",
 "pushRootAndIntermediateCertificates": true,
 "intermediateCertificateFileNames":[ "test_cert_ca.crt"],
 “pfxPassword”:”cGFzc3dvcmQ=”
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
} }	

Certificate details for AmazonELB

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateLocation	(Mandatory) Location of the certificate. Values are **ACM** or **IAM**. **Type**: String
certCAReferenceId	(Optional) Reference ID to input the certificate location. It is **mandatory** if certificateLocation is **ACM**. **Type**: String **Constraints**: The special characters allowed are ('=', '/', ',', '.', '@', '-').
certificateFileName	(Optional) A user defined file name for pushing the certificate into the AmazonELB device. It is **mandatory** if certificateLocation is **IAM**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the CA file name and intermediate certificate file name.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
Request payload if certificateLocation is ACM	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certCAReferenceId”: "arn:aws:iam::2313:amazonELB"
“certificateLocation”: "ACM"
“certificateType”: "PEM-.pem"
“pushRootAndIntermediateCertificates”: true
}
```

Request payload if certificateLocation is IAM

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateFileName: "sample.pem",
“certificateLocation”: "IAM",
“certificateType”: "PEM-.pem",
“pushRootAndIntermediateCertificates”: true
}
```

Certificate details for NginxPlus

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, and PEM-.cer
certificateLocation	(Mandatory) A user defined file name for pushing the certificate into the NginxPlus device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus (continued)

Name	Mandatory
	Type: String **Constraints**: The certificate file name should not begin and end with special characters except -, ., _. It should not be the same as CA file name and intermediate file name.
keyLocation	(Mandatory) A user defined file for pushing the key into the NginxPlus device. **Type**: String **Constraints**: The key file name should not begin and end with special characters except -, ., _. Key file name should be same as certificateFileName.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean

Request Payload

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateLocation":"/home/appviewx",
"keyLocation":"/home/appviewx",
"privateKeyInDevice": true
}
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the HAProxy device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean
privateKeyLocation	(Mandatory) A user defined file name for pushing the keys into the HAProxy device. It is **mandatory** if privateKeyInDevice is **true**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.

Request Payload

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateFileName":"/opt/haproxy/certificate_push.pem",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy (continued)

Name	Mandatory
"privateKeyLocation": true, "privateKeyLocation": "/opt/haproxy/test_cert.key" } }	

Response for Push and Bind SYNC API

Note: The response details/parameters are common for all vendor devices.

Parameters

Name	Description
response	Contains the parameters certificate, deviceProfiles, applicationConnectors, success and messages. **Type**: Object
certificate response	Details about the selected certificate which was used to push into the ADC devices **Type**: List <Object>
deviceProfiles response	Details about the device profiles to which the certificate is bound. **Type**: List <Object>
applicationConnectors response	Details about the application connectors where the push operation occurred. **Type**: List <Object>
success response	Determines whether the push operation succeeded. **Type**: Boolean
messages response	Details of the push operation. **Type**: List <String>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
message	Success or failure messages **Type**: String
appStatusCode	Application specific status code for the response. **Type**: String
tags	More info in case of failure response **Type**: Object
headers	Details of the response headers if any **Type**: Object

Sample Request/Response

Request Payload

```
{
 "applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```

Note: Please refer to the "Request Structure" to identify the changeable values.

Response Details

```
{
 "response": {
 "certificate": <Selected Certificate>,
 "deviceProfiles": <Selected Profiles>,
 "applicationConnectors": <Application connectors with its work order status>,
 "success": <Status of the operation>,
 "messages": <Response message for the push action performed>
 },
 "message": null,
 "appStatusCode": <Error Code>,
 "tags": {},
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```


Sample Response (common for all vendors)


```
{
"response": {
"certificate": {
"commonName": "appviewx_test",
"serialNumber": "C4:DA:38:94:6B:A7:08:92:FB:A5:31:89:60:C6:D3:E7",
"issuerCommonName": "AppViewX Intermediate CA",
"status": "Managed",
"avxStatus": null,
"associatedObjects": [
"device_name::serverssl-insecure-compatible:Common:server-ssl"
],
"discoverySources": [
"device_name"
],
"subjectOrganization": "",
"subjectOrganizationUnit": "",
"subjectLocality": "",
"subjectState": "",
"subjectCountry": "",
"issuerOrganization": "AppViewX Inc",
"issuerOrganizationUnit": "",
"issuerLocality": "Seattle",
"issuerState": "Washington",
"issuerCountry": "US",
"version": "3",
"validFrom": 1617025560000,
"validTo": 1648561560000,
"validFor": "364 day(s) 23 hr(s) 57 min(s)",
"keyAlgorithmAndSize": "RSA 1024",
"signatureAlgorithm": "SHA160withRSA",
"signatureHashAlgorithm": "SHA160",
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) ",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

"basicConstraints": "Subject Type=End entity, Path Length=none",

"group": "Default",

"subjectAlternativeNames": [

"DNS : appviewx_test"

],

"complianceStatus": "Compliant",

"applications": [],

"expiryStatus": "Valid",

"permission": null,

"category": "Server",

"uuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",

"id": "6061da0e92d28c50bd40336b",

"certificateAuthority": "AppViewX",

"authorityKeyIdentifier": "D0:D7:4B:D0:82:85:A4:98:70:6E:75:97:26:C6:A3:14:A5:C0:31:4D",

"subjectKeyIdentifier": "9D:1D:77:A0:CA:35:C5:5B:D4:3A:70:1A:AB:B0:2A:DD:CD:61:D9:80",

"issuerSerialNumber": "2C:F4:8E:5F:5F:D2:C2:F2:8A:DB:5A:D4:A1:06:A5:B2",

"authorityInfoAccess": [

"AuthorityInfoAccess : [accessMethod : 1.3.6.1.5.5.7.48.1, alterativeName : , url :

https://172.18.0.157:31443/avxapi/controller/avxocsp?issuerserialnumber=597558399065138247098035107238630291 70]"

],

"certificatePolicies": [],

"crlDistributionPoints": [

"CrlDistributionPoint : [name : , url : https://172.18.0.157:31443/avxapi/controller/avxcrl?crlFileName=597558399065138247098035107238630291 70.crl]"

],

"thumbprintAlgorithm": "SHA-1",

"thumbPrint": "64:E8:0C:89:5F:6A:F1:2D:09:47:8C:5B:D5:DC:1B:CE:42:78:06:E7",

"type": "Others",

"genericFields": {

"vs_ip_AppViewX": "",

"device_name_AppViewX": ""

},

"certAttributes": {

"test": "test"

},

"validFromDate": null,

"validToDate": null,

"discoveredFileNames": [],

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

"issuingTemplate": null,

"csrGenerationSource": "appviewx",

"certificateHSMDetails": null,

"deviceDetails": null,

"newConnectors": [],

"csrAvailable": true,

"enhancedSANTypes": null,

"autoRenewDate": "",

"missingParamsForAutoRenew": "CSR parameters are available for certificate renewal",

"base64ImageContent": null,

"caConnectorName": null,

"caSettingName": null,

"suspendedCertificate": false,

"comments": null,

"mailAddress": "",

"streetAddress": "",

"postalCode": "",

"publicKeyModulus": null,

"requestIds": [

"R145",

"R146"

],

"orderId": null,

"publicKey":

"30:81:89:02:81:81:00:8E:EA:40:EF:61:06:00:89:9F:99:70:61:03:C3:D2:28:C1:EF:12:B2:FB:1A:6E:65:1C:85:3D:E1:8D:BD:DF:68:C9:76:A4:23:0D:79:A2:E6:52:F0:68:FC:AD:87:D2:D7:70:7C:76:C5:3F:A5:96:7B:D3:74:8A:5A:98:70:48:95:37:51:E3:33:1B:A7:32:19:E5:39:54:38:8A:1A:5B:A0:9C:5D:B5:D6:A6:EC:D9:DB:8A:FB:B8:BD:66:A6:E2:F9:D8:BF:AB:4D:F1:D3:31:E1:CB:6E:84:CF:C3:6F:E8:1F:E3:AF:12:F4:22:11:13:5E:F3:56:B1:8B:4E:18:BC:4D:02:03:01:00:01",

"ellipticCurve": null,

"issuedByRootCertificate": false,

"cumulativeSanCount": 1,

"privatekeyAvaliable": true

},

"deviceProfiles": [

{

"profileId": "device_name:@serverssl-insecure-compatible:@Common",

"vendor": "F5",

"deviceName": "device_name",

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"vendorCategory": "ADC",
"profileIdentifierForView": "device_name::serverssl-insecure-compatible:Common:server-ssl",
"profileDisplayOrder": "Partition:@Profile Name:@SSL Type",
"connectorType": "PROFILE_CONNECTOR",
"applications": [],
"hollisticViewData": {
"Partition": "Common",
"Profile Name": "serverssl-insecure-compatible",
"SSL Type": "server-ssl"
},
"overviewData": {},
"inventoryData": {
"associatedObjects": "device_name::serverssl-insecure-compatible:Common:server-ssl"
},
"vendorProperties": {
"partition": "Common",
"sslType": "server-ssl",
"name": "serverssl-insecure-compatible",
"partitionNameWithoutPath": "Common",
"iAppProfile": false
}
}
],
"applicationConnectors": [
{
"appconnectorId": "device_name:@serverssl-insecure-compatible:@Common:@9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"profileInfo": {
"profileId": "device_name:@serverssl-insecure-compatible:@Common",
"vendor": "F5",
"deviceName": "device_name",
"vendorCategory": "ADC",
"profileIdentifierForView": "device_name::serverssl-insecure-compatible:Common:server-ssl",
"profileDisplayOrder": "Partition:@Profile Name:@SSL Type",
"connectorType": "PROFILE_CONNECTOR",
"applications": [],
"hollisticViewData": {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

"Partition": "Common",

"Profile Name": "serverssl-insecure-compatible",

"SSL Type": "server-ssl"

},

"overviewData": {},

"inventoryData": {

"associatedObjects": "device_name::serverssl-insecure-compatible:Common:server-ssl"

},

"vendorProperties": {

"partition": "Common",

"sslType": "server-ssl",

"certificateFileName": "certificate_push_202103291347.crt",

"rootCertificateFileName": "test_cert_ca.crt",

"certificatePartition": "Common",

"name": "serverssl-insecure-compatible",

"partitionNameWithoutPath": "Common",

"privateKeyPartition": "Common",

"keyType": "RSA",

"privateKeyFileName": "certificate_push_202103291347.key",

"iAppProfile": false

}

},

"backupInfo": {

"rollbackEligibility": false,

"backupDisplayMessage": null,

"backupCertUuid": null,

"backupCertCommonName": null,

"backupCertSerialNumber": null,

"unbindCertificate": false,

"backupProperties": null

},

"syncInfo": {

"syncMessage": {

"title": "Certificate Push",

"message": "Certificate pushed to the device successfully",

"utcTime": "2021-03-29T13:48:30.605",

"status": "SUCCESS",

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"batchId": null
},
"syncStatus": "SYNCRONIZED"
},
"userPreference": {
"autoPush": false,
"overwrite": true,
"securePush": false,
"userName": "admin",
"scheduledPushDate": null,
"modifiedData": true,
"modifiedTime": "2021-03-29T13:46:34.691",
"fileProperties": {
"pushRootAndIntermediateCertificates": false,
"certificateFileName": "certificate_push.crt",
"rootCertificateFileName": "test_cert_ca.crt",
"privateKeyFileName": "certificate_push.key"
},
"validationType": "DEFAULT",
"customApplications": null
},
"vendorScriptDetails": [],
"workflowDetails": {
"requestId": "146",
"workOrderId": "0",
"workflowStatus": "In Progress",
"workflowType": "VW",
"userName": "admin",
"actionType": "PUSHBIND",
"actionTypeDisplayName": "Push",
"taskId": "avxapi_5",
"taskName": "Post Push Script Execution",
"taskType": "others",
"taskStatus": "In Progress",
"currentAction": null,
"proceedProcess": null,
"breakdownProcess": null,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"reviewComponent": false,
"implemetationTime": 0,
"workOrderLogs": [
"Pre Push Script not available",
"Certificate push successful in device : device_name. Certificate/Key/CA file name already exists in device with different content. Certificate push has been completed successfully with names: [ Certificate File Name: certificate_push_202103291347.crt, Private Key File Name: certificate_push_202103291347.key, CA File Name: test_cert_ca.crt ]."
]
},
"loggerStatus": null,
"previousApplicationConnectorId": null
}
],
"success": true,
"messages": [
"Certificate push to the profiles completed successfully"
]
},
"message": null,
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Rollback to ADC profile

The API initiates the rollback of a certificate to an ADC profile.

Before you begin

Ensure the following before attempting to rollback certificate to a ADC device profile through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state

Request Structure

Endpoint:	/certificate/rollback

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Type:	POST
Sample URL:	
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
autoApproval	Indicates whether the auto-approval is needed for the action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload	Contains all the parameters to be sent in the request body for the post request.
Body	**Type**: Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector id. **Type**: List <String>

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the rollback request
requestId	Request Id for rollback action for the application connector. response **Type**: String
connectorId	Application connector Id. response **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission. **Remediation**: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LAST_RETRIEVAL	Unable to retrieve connector information.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	App connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
 "applicationConnectorIds": [ "device_name:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```

Response

```
{
 "response": "Success",
 "message": "App connector rollback action initiated for 1 connector(s).",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

Discover Certificates from Firewall

The API will discover certificates and it’s private keys from the firewall device.

Before you begin

Before attempting to discover certificates from a particular Firewall device through AppViewX, the user has to ensure the following:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Firewall devices should be added in AppViewX.
- The device should be in Managed state.

Request Structure

URL: */certificate/discovery/instance*

Type: `POST`

Parameters

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if `username` and `password` are not provided.
`username`	Header	AppViewX login username.	`String`	Required if `sessionId` is not provided.
`password`	Header	AppViewX login password.	`String`	Required if `sessionId` is not provided.
`Content-Type`	Header	Specifies the nature of the data in the payload.	`String`	Value of the param should be '**application/json**'
`gwkey`	Query	Tenant Key. This is needed only in case of multi tenant installations and can be ignored in other type of installations.	`String`	NA
`gwsource`	Query	Source from which the request is triggered (E.g. external).	`String`	NA
`Payload`	Body	Contains all the params to be sent in the request body for the post request.	`Payload`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Mandatory	Description	Field Type	Constraints
discoveryType	Yes	Type of the discovery.	String	Possible values: ONDEMAND, SCHEDULED
name	Yes	Name of the discovery instance to be created.	String	NA
description	No	Description of the discovery request.	String	NA
groupName	Yes	Specifies the group under which the discovered certificate needs to be tagged.	String	Not mandatory if the field rbacRuleProcessRequired is **true**.
source	Yes	Source of the certificates.	String	Value should be **FIREWALL**.
certStatus	Yes	Specifies the certificate status to be maintained in the inventory after discovering the certificates.	String	Possible values are Managed, Monitored, None. If None certificates will not be moved to certificate inventory.
targetList	Yes	Name of the devices where the certificates need to be discovered.	List of String	Device names which are added already need to be specified.
coolingPeriod	Yes	Whether the discovery is sequential or parallel.	Number	0 - sequential 1< - parallel
associatedRule	No	Name of the rule to be associated with the discovered certificates.	String	Rule name which is added already need to be specified.
rbacRuleProcessRequired	No	Whether Rbac rule process in required or not.	Boolean (true or false)	If true new certificates will be tagged under the group specified in the rule.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

202 Accepted returns string of type application/json with the following body params.

Parameters

Name	Description	Field Type
response	Contains the response attributes for the discovery request.	response
message	Success message of the action or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

response

Name	Description	Field Type
discoveryName	Name of the discovery request created.	String
message	Success message of the action or failure description in case of error.	String

Status Codes

Status Codes and Description

HTTP Status code	appStatusCode	Message	Possible remediation
202 Accepted	NA	Discovery history details added successfully with discovery id 5f5b25dd2ceb1150424ed850, and discovery operation has been triggered.	NA
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.	Ensure that valid username and password or valid sessionId

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes and Description (continued)

HTTP Status code	appStatusCode	Message	Possible remediation
			is provided as header param.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>.	Check and ensure that valid value is provided for <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found.	Check and ensure that valid value is provided for the `targetList` field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name.	Please provide different value for the field name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found.	Check and ensure that valid value is provided for the `groupName` section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1.	Please provide the correct value

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes and Description (continued)

HTTP Status code	appStatusCode	Message	Possible remediation
			in the field `coolingPeriod`.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED.	Please provide the correct value in the field `discoveryType`.
500 Internal Server Error	avx-common-011	Error while processing.	NA

Sample Request/Response

Sample Request

```
{
"discoveryType": "ONDEMAND",
"name": "ServerDiscovery",
"description": "Discovery from server devices",
"source": "SERVER",
"coolingPeriod": "5",
"associatedRule": "RevokedCertExclusion",
"certStatus": "MANAGED",
"rbacRuleProcessRequired": false,
"groupName": "Default",
"discoverAllCerts": false,
"templatesToFilter": [],
"targetList": [
"ApacheLinux"
]
}
```

Sample Response

```
{
"response": {
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

"discoveryName": "ServerDiscovery",

"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered."

},

"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered.",

"appStatusCode": null,

"tags": {},

"headers": null

}

Discover Certificates from Server

The API will discover certificates and it's private keys from the server device.

Before you begin

Before attempting to discover certificates from a particular Server device through AppViewX, the user has to ensure the following:

- Server devices should be added in AppViewX.
- The device should be in Managed state.

Request Structure

URL: */certificate/discovery/instance*

Type: POST

Parameters

Name	Type	Description	Field Type	Constraints
sessionId	Header	Session Id received after login	String	Required if username and password are not provided
username	Header	AppViewX login username	String	Required if sessionId is not provided
password	Header	AppViewX login password	String	Required if sessionId is not provided

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Type	Description	Field Type	Constraints
Content-Type	Header	Specifies the nature of the data in the payload.	String	The value of the param should be **'application/json'**
gwkey	Query	Tenant Key. This is needed only in case of multi tenant installations and can be ignored in other type of installations.	String	NA
gwsource	Query	Source from which the request is triggered (E.g. external).	String	NA
Payload	Body	Contains all the params to be sent in the request body for the post request	Payload	NA

Name	Mandatory	Description	Field Type	Constraints
discoveryType	Yes	Type of the discovery	String	**Possible values:** ONDEMAND, SCHEDULED
name	Yes	Name of the discovery instance to be created.	String	NA
description	No	Description of the discovery request	String	NA
groupName	Yes	Specifies the group under which the discovered certificate needs to be tagged.	String	Not mandatory if the field **rbacRuleProcessRequired** is true
source	Yes	Source of the certificates	String	The value should be **SERVER**
certStatus	Yes	Specifies the certificate status to be maintained in the inventory after discovering the certificates.	String	Possible values are Managed, Monitored, None. If None certificates will not be moved to certificate inventory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

(continued)

Name	Mandatory	Description	Field Type	Constraints
targetList	Yes	Name of the devices where the certificates need to be discovered	List of String	Device names that are added already need to be specified
coolingPeriod	Yes	Whether the discovery is sequential or parallel	Number	0 - sequential >1 - parallel
associatedRule	No	Name of the rule to be associated with the discovered certificates	String	Rule name which is added already need to be specified
rbacRuleProcessRequired	No	Whether Rbac rule process is required or not	Boolean (true or false)	If true new certificates will be tagged under the group specified in the rule

Response Structure

202 Accepted returns string of type application/json with the following body params

Parameters

Name	Description	Field Type
response	Contains the response attributes for the discovery request	response
message	Success message of the action or failure description in case of error	String
appStatusCode	Application-specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response	NA

response

Name	Description	Field Type
discoveryName	Name of the discovery request created	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

response (continued)

Name	Description	Field Type
message	Success message of the action or failure description in case of error	String

Status Codes

Status Codes and Description

HTTP Status code	appStatusCode	Message	Possible remediation
202 Accepted	NA	Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered.	NA
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials	Ensure that valid username and password or valid sessionId is provided as header param.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>	Check and ensure that valid value is provided for <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found	Check and ensure that a valid value is provided for the **targetList** field in the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes and Description (continued)

HTTP Status code	appStatusCode	Message	Possible remediation
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	The Discovery name already exists. Please specify a different Discovery name	Please provide a different value for the field **name**
404 Not Found	GROUP_NOT_FOUND	A specified certificate group is not found	Check and ensure that valid value is provided for the **groupName** section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	cooling period should be 0 or greater than 1	Please provide the correct value in the field **coolingPeriod**.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED	Please provide the correct value in the field **discoveryType**.
500 Internal Server Error	avx-common-011	Error while processing	NA

Sample Request/Response

Sample Request

```
{
"discoveryType": "ONDEMAND",
"name": "ServerDiscovery",
"description": "Discovery from server devices",
"source": "SERVER",
"coolingPeriod": "5",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"associatedRule": "RevokedCertExclusion",
"certStatus": "MANAGED",
"rbacRuleProcessRequired": false,
"groupName": "Default",
"discoverAllCerts": false,
"templatesToFilter": [],
"targetList": [
"ApacheLinux"
]
}
```


Sample Response


```
{
"response": {
"discoveryName": "ServerDiscovery",
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered."
},
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


HP iLO Vendor Integration via REST Interface

Overview

The HP iLO vendor integration via REST interface (iLO V4) encompasses the following actions:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 4: MultiCloud Configuration User Guide

Note: Logs for all cloud device-related activities can be viewed here.

AWS cloud instance has been integrated with AppViewX using SSM, which is an inbuilt agent supported by AWS. In this document, the pre-requisites required for integrating AWS EC2 instances with AppViewX and the basic functionality have been explained.

Supported Vendors

Server	
Linux (OS)	Web Service
Native	AWS
Apache	Y(19.4)
RapidSB	AWS
Generic Linux	Y(19.4)
JBoss	Y(20.1)
MQ Server	Y(20.1)
NGNIX	Y(20.1)
Rabbit MQ	Y(20.1)
My SQL	Y(20.1)
Windows (OS)	Web Service
RapidSB	AWS
Apache	Y(20.2)
Tomcat	Y(20.2)

Prerequisites

The following are the pre-requisites only for the EC2 services. For the other services, we do not have any pre-requisites.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- A dedicated/Shared S3 bucket with R/W and delete access is required.
- SSM should have command execution and document creation access.
- EC2 instances should have a working SSM agent with an EC2 Instance role associated with it for discovery.
- For adding a cloud account we need AWS API keys(Access key/Secret key).
- IAM policy configuration for EC2:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ssm:GetDocument",
        "ssm:CreateDocument"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::name_of_dedicated_bucket_created_for_appviewx"
      ]
    }
  ]
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
}
```

Note: For the other services, the IAM policy will be shared based on the ask.

Limitation

Only the processes on the Linux platform are supported.

- Prerequisites
- Viewing the Cloud Device Inventory
- Amazon Web Services (AWS)
- Azure
- Google Cloud Platform (GCP)
- Apache SSM integration specification
- Functional Specification
- Generic Linux SSM Integration Specification
- Instances Discovery Specification

Prerequisites

The following are the prerequisites only for the EC2 services. For the other services, AppViewX does not have any prerequisites.

- A dedicated/shared S3 bucket with R/W and delete access is required.
- SSM should have command execution and document creation access.
- EC2 instances should have a working SSM agent with an EC2 Instance role associated with it for discovery.
- For adding a cloud account, you need AWS API keys (access key/secret key).
- IAM policy configuration for EC2:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
{
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "ssm:SendCommand",
            "ec2:DescribeInstances",
            "ec2:DescribeRegions",
            "ssm:GetDocument",
            "ssm:CreateDocument"
        ],
        "Resource": "*"
    },
    {
        "Sid": "VisualEditor1",
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:ListBucket",
            "s3:DeleteObject"
        ],
        "Resource": [
            "arn:aws:s3:::name_of_dedicated_bucket_created_for_appviewx"
        ]
    }
  ]
}
```

Note: For the other services, the IAM policy will be shared based on the ask.

Limitation

Only the processes on the Linux platform are supported.

Viewing the Cloud Device Inventory

The cloud device inventory is displayed at two levels:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Outer inventory: Displays details of all cloud accounts added
- Inner inventory: Displays details of an individual cloud account

To access the outer cloud device inventory:

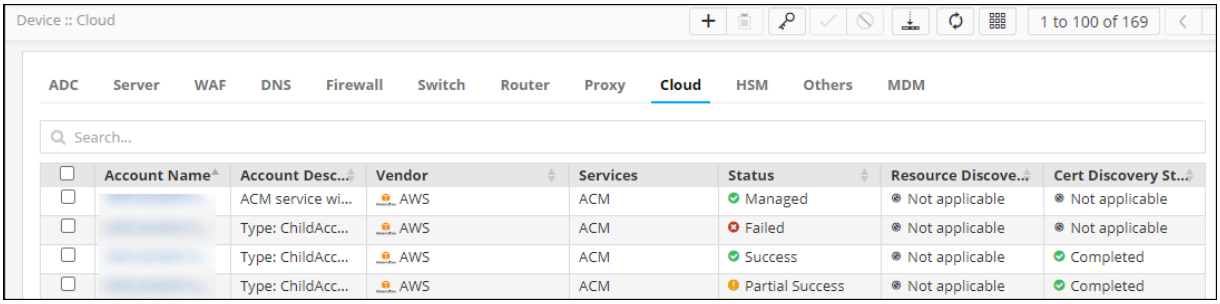
1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** screen is displayed.

   Alternate steps to access the cloud device inventory:

   a. Go to (**Menu**) > **Platform** > .**ASSET MANAGEMENT** > **Device Inventory**.

   The **Device :: ADC** page is displayed.

2. From the **Device :: ADC** screen, select **Cloud**.
   The **Device :: Cloud** outer cloud device inventory is displayed.



Understanding the cloud device inventory

Field	Description
Account Name	Name of the account to which the cloud device belongs
Account Description	Applicable only for a child account, this field displays the following details: • Account type (child) • Master account number • Discovery type: **ROLE_BASED** or **ORGANIZATION_BASED**
Vendor	Cloud device vendor name
Service	Service integrated for the cloud device
Status	Status of the discovered accounts.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>This field takes the following values:
• For the master account:
• Managed
• Failed
• For the child account:
• Success
• Partial Success
• Queued
• In Progress
• Failed</td></tr>
<tr><td>Resource Discovery Status</td><td>Note: Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to Not Applicable.

Note: The resource discovery status of accounts in this outer cloud inventory list depends on the corresponding status of all its reporting entities listed in the account level inventory here.

This field indicates the status of the resource discovery for the discovered accounts using the following values:
• Not started: Resource discovery for the account is yet to begin

Note: At this point, it is not mandatory for the associated account to be in the Managed (account credentials validated) state.

• In-Progress: Resource discovery for the entity by AppViewX in the customer’s AWS environment is currently in progress. The aggregated resource discovery status is In-Progress till the resource discovery status for all individual entities is Completed.

Note: This is possible only when the account is in the Managed state.

• Completed: Resource discovery by AppViewX in the customer’s AWS environment is complete.</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved**, • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. **Note:** The certificate discovery status of accounts in this outer cloud inventory list depends on the corresponding status of all their reporting entities listed in the account level inventory here. Indicates the status of the certificate discovery for the discovered accounts using the following values: • **Not started**: Certificate discovery for the account is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved**, • for EC2 when no EC2 instances are discovered, or • for all existing devices and child accounts as part of data migration. **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.

Amazon Web Services (AWS)

- Prerequisites for Migrating AWS Standalone Accounts from Older Versions
- Onboarding a Standalone Account in AWS
- Onboarding a Cross Account in AppViewX
- AWS Cross/Federated Account Onboarding

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important: AWS standalone device migration is supported only from the following versions of CERT+ SaaS: **v2020.1**, **v2020.2**, **v2020.3** - **v2020.3 FP7**. The following prerequisites are also applicable to only these versions.

Important: AWS device migration **is not** supported from the following versions of CERT+ SaaS: **v2012.x**, **v2019.x**, and **v2021.x**. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: For customers migrating from versions **20.1.x**, **20.2.x**, and **20.3.6**, AppViewX recommends that you delete the following before migration:

- All of their Amazon CA settings
- Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).

Note: For customers migrating from version **v2020.3.10** (mandatory):

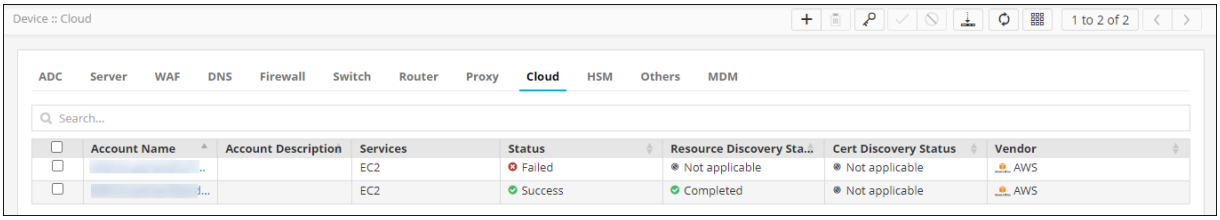
- Delete all of their Amazon CA settings before migration.
- Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the **standalone AWS cloud accounts** migrated from the above listed versions to version **v2022.1 FP1**:

- For standalone accounts where one of the associated services is not EC2
- For standalone accounts where one of the associated services is EC2

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
   The **Device :: Cloud** page is displayed.



3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.

4. From the top-right corner of the **Device :: Coud** page, click the  (**Fetch config**).
   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

• Before Migration
• After Migration

Before Migration

Merge permissions from all individual buckets into any one S3 bucket.

After Migration

1. Select a migrated standalone account from the **Device :: Cloud** page.
   The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
4. Click **Add**.
5. Click **Save**.

   Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Onboarding a Standalone Account in AWS

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

Note: The following steps cover only the bare minimum requirements for onboarding a standalone AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Note: If you already have a AWS account set up with the required roles and policies created and mapped, refer **Onboarding a Standalone Account in AppViewX**.

- Step 1: Creating a IAM User in AWS
- Step 2: Generating User Identity
- Step 3: Attaching Policies to the Created User
- Step 4: Creating a EC2 Role
- Step 5: Attaching Policies to a EC2 Role
- Step 6: Onboarding a Standalone Account in AppViewX
- Account Level/Inner Inventory

Step 1: Creating a IAM User in AWS

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Login to AWS and from the **Services** menu, go to **Identity & Access Management Service** (IAM).
2. From the left navigation panel, under **Access management**, click **Users**.
   The **IAM > Users** screen is displayed.
3. To add a new user, click **Add users**.
   The **Specify user details** screen is displayed.
4. On the **Specify user details** screen, enter the **User name** and click **Next**.

   Note: Console access is not required for this use case, hence the corresponding fields can be left blank.

   The **Set permissions** screen is displayed.
5. Click **Next**.

   Note: Instructions for setting permissions for this user are covered in **Step 3: Attaching Policies to the Created User**.

   The **Review and create** screen is displayed.
6. Click **Create user**.
   The **IAM > Users** screen is displayed. The user created is listed on this screen, under the **Users** list.

What to do next: Generate user identity to acquire the access key and secret key.

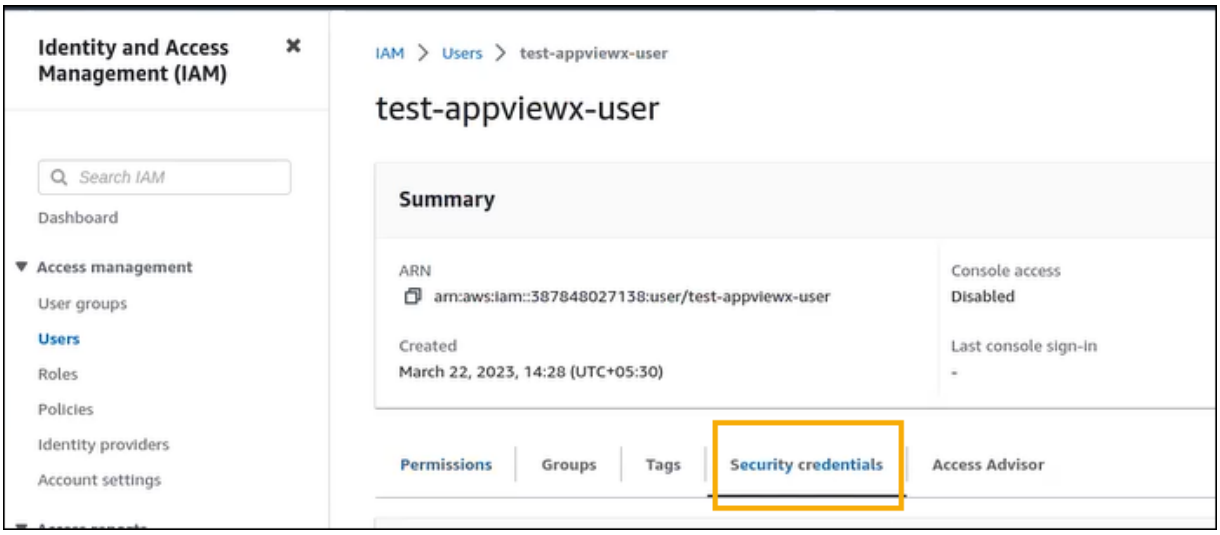
Step 2: Generating User Identity

In order to onboard a standalone account in AppViewX, you will require the account user's access key and secret key.

To retrieve the access key and the secret key:

1. From the **Users** list, click the **User name** of the user created in Step 1.
   The **IAM > Users > <selected user name>** screen is displayed.
2. Click **Security Credentials**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



3. From the **Access keys** section, click **Create access key**.
   You will be navigated **IAM > Users > <selected user name> > Create access key** screen.
4. Under **Access key best practices & alternatives**, select **Other** and click **Next**.
5. Click **Create access key**.
   The **Retrieve access keys** screen is displayed.
6. From the **Access key** section, copy the access key.
   To copy the **Secret access key**, click show and copy the secret access key.

> **Important:** On the **Retrieve access keys** page, the secret access key is displayed only once. Hence, it is recommended that you copy and paste the key to a secure location.

> **Tip:** Alternatively, you can click **Download .csv file** to download a file that contains your access key and secret access key.

7. Click **Done**.

What to do next: Attach policies to assign permissions to the created user.

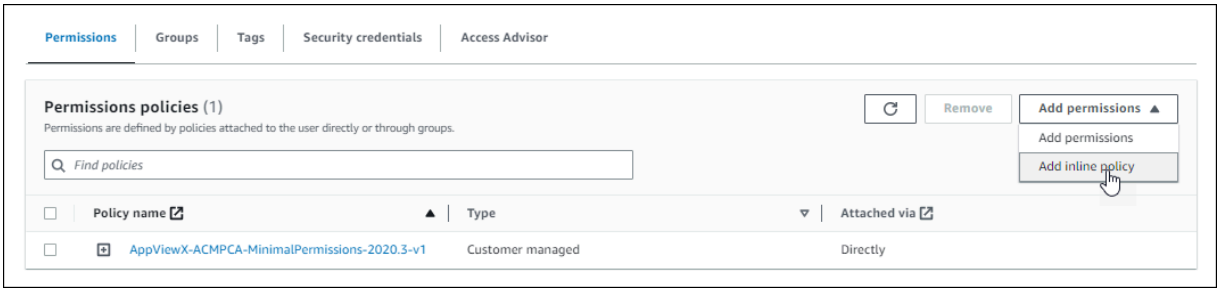
Step 3: Attaching Policies to the Created User

AWS supports two different policy types: **a customer inline policy**, which is a private set of permissions created for a specific user (recommended) and **a customer managed policy**, which is like a public policy that can be mapped to any new/existing users.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX recommends creating a dedicated policy for each service type.

1. From the user summary screen, under the **Permissions** tab, from the **Permissions policies** section, from the **Add permissions** dropdown menu, select **Add inline policy**.



   The **Create Policy** screen is displayed.
2. To create a policy by specifying the **JSON** structure:

   a. Clear the code in the **JSON** tab.

   b. For the required service, copy the JSON structure of the permissions and paste it in the **JSON** tab of the **Create policy** screen.
   For the full list of actions and the corresponding permissions, refer **AWS IAM Prerequisites for Standalone Account Onboarding**.

3. Click **Review policy**.
   The **Create policy** > **Review policy** page is displayed.
4. On this page, enter a policy **Name**.

> **Tip:** While the policy name is subjective and is left to the user's discretion, AppViewX recommends the following naming convention: **Appviewx-<service name>-policy**

5. Click **Create policy**.

What to do next: If you want to associate the EC2 service with the onboarded account, create a EC2 role. If not, proceed to onboarding the standalone account in AppViewX.

- AWS IAM Prerequisites for Standalone Account Onboarding

AWS IAM Prerequisites for Standalone Account Onboarding

- IAM Prerequisites for Discovering and Managing SSL Certificates in ACM
- IAM Prerequisites for Discovering and Managing SSL Certificates in CloudFront

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- IAM Prerequisites for Managing SSM Permissions for the EC2 Policy
- IAM Prerequisites for Managing SSM Permissions for EC2 Role
- IAM Prerequisites for Enabling S3 Bucket Access to AppViewX
- IAM Prerequisites for Discovering and Managing SSL Certificates in ELB
- IAM Prerequisites for Discovering and Managing Certificates in IAM
- IAM Prerequisites for Discovering and Managing Private CA Certificates

IAM Prerequisites for Discovering and Managing SSL Certificates in ACM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate"
         ],
         "Resource": "*"
      }
   ]
}
```

Note: Route53 IAM permissions are optional when automatic DNS record creation in Route53 is not required for Certificate Enrollment & Renewal requests.

```
{
   "Version": "2012-10-17",
   "Statement": [
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "route53:ListHostedZones",
            "route53:ChangeResourceRecordSets"
        ],
        "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing SSL Certificates in CloudFront

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "iam:GetServerCertificate",
            "acm:GetCertificate",
            "acm:ListCertificates",
            "iam:ListServerCertificates",
            "ec2:DescribeRegions",
            "cloudfront:ListDistributions",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "cloudfront:UpdateDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListTagsForResource",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate"
        ],
        "Resource": "*"
      }
  ]
}
```

IAM Prerequisites for Managing SSM Permissions for the EC2 Policy

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

IAM Prerequisites for Managing SSM Permissions for EC2 Role

```
{
   "Version": "2012-10-17",
   "Statement": [
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    {
        "Action": [
            "ssm:DescribeDocument",
            "ec2messages:GetEndpoint",
            "ec2messages:GetMessages",
            "ssmmessages:OpenControlChannel",
            "ec2messages:DeleteMessage",
            "ssm:UpdateInstanceInformation",
            "ec2messages:FailMessage",
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

IAM Prerequisites for Enabling S3 Bucket Access to AppViewX

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "s3:GetObject",
  "s3:ListBucket",
  "s3:DeleteObject",
  "s3:GetBucketLocation"
         ],
         "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
         ],
      }
   ]
}
```

IAM Prerequisites for Discovering and Managing SSL Certificates in ELB

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
            "elasticloadbalancing:ModifyListener",
            "ec2:DescribeInstances",
            "iam:ListServerCertificates",
            "elasticloadbalancing:DescribeTags",
            "ec2:DescribeRegions",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeListeners",
            "ec2:DescribeAvailabilityZones",
            "acm:GetCertificate",
            "elasticloadbalancing:DescribeTargetHealth",
            "acm:ListCertificates",
            "elasticloadbalancing:DescribeTargetGroups",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "elasticloadbalancing:AddListenerCertificates",
            "elasticloadbalancing:DescribeListenerCertificates"
        ],
        "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing Certificates in IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:UploadServerCertificate",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing Private CA Certificates

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "acm:RenewCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "acm-pca:CreateCertificateAuthorityAuditReport",
 "acm-pca:DescribeCertificateAuthorityAuditReport,
 "acm-pca:GetCertificate",
 "acm-pca:ListCertificateAuthorities",
 "acm-pca:IssueCertificate",
 "acm-pca:RevokeCertificate",
 "s3:GetBucketLocation",
 "s3:GetObject"
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
        ],
        "Resource": "*"
      }
    ]
}
```

Step 4: Creating a EC2 Role

Important: This step is required only if you choose to associate the EC2 service with the onboarded account.

1. From the left navigation panel, under **Access management**, click **Roles**.
   The **IAM > Roles** screen is displayed.
2. Click **Create role**.
   The **IAM > Roles > Create role** screen is displayed.
3. Under **Trusted entity type**, select **AWS service**.
4. Under **Use case**, select **EC2**.
5. Click **Next**.
6. On the **Add permissions** screen, click **Next**.
7. On the **Name, review, and create** screen, enter a role name, and review the rest of the role details.
8. Click **Create role**.

What to do next: Attach policies to the created EC2 role.

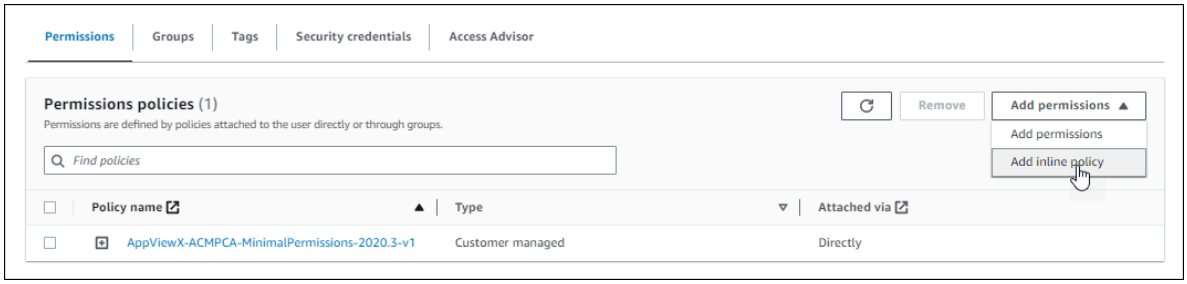
Step 5: Attaching Policies to a EC2 Role

1. On the **IAM > Roles** page, under **Roles**, select the EC2 role created in step 4.
2. From the role summary screen, under the **Permissions** tab, from the **Permissions policies** section, select the EC2 policy you want to attach to this role.
   OR

   To create a new EC2 policy:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. From the **Add permissions** dropdown menu, select **Add inline policy**.



The **Create Policy** screen is displayed.

b. Clear the code in the **JSON** tab.

c. For the EC2 service, copy the JSON structure of the permissions and paste it in the **JSON** tab of the **Create policy** screen.

Click here for the predefined JSON structure for:

- Managing SSM permissions for the EC2 policy
- Managing SSM permissions for the EC2 role

What to do next: Onboard the standalone account in AppViewX.

Step 6: Onboarding a Standalone Account in AppViewX

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.
Account name*	Enter the customer's unique AWS account name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Account number*	Enter the customer's AWS account number.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access key*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	According to the type of the new cloud device being added, select the corresponding Amazon Cloud Service for the device.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Service region*	Service regions are regions that are supported by the selected service. From the dropdown list, select the service regions that should be scanned for certificates. **Note:** To be able to fetch and select from the available regions, ensure that the credentials have been provided in the **Credentials** section.
CA Operation Mode*	**Note:** This field is displayed only when the **Amazon Private CA** service is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • **ACM** • **PCA**
S3 Bucket*	**Note:** This field is displayed only when the **PCA** CA operation mode is selected. Enter the S3 bucket name.
Discovery Certificate	**Note:** This field is displayed only when one/both of the CA operation modes are selected. To enable instance certificate discovery at the time of device addition, select this checkbox.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Account Level/Inner Inventory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

Onboarding a Cross Account in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

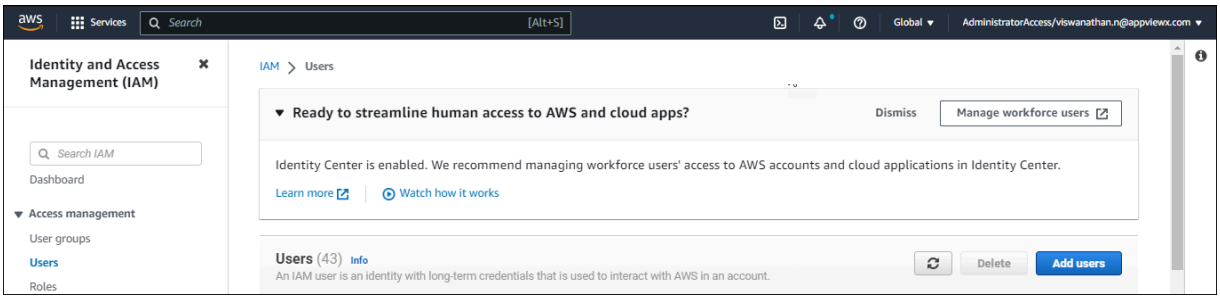
Note: If you already have a AWS account set up with the required roles and policies created and mapped, you can directly start with **Onboarding a Cross Account in AppViewX** .

- Step 1: Creating a IAM User in AWS
- Step 2: Generating User Identity
- Step 3: Attaching Policies to the Created User
- Step 4: Creating a Role in the Child Account in AWS
- Step 5: Attaching Policies to the Created Role
- Step 6: Creating a EC2 Role
- Step 7: Attaching Policies to a EC2 Role
- Step 8: Onboarding a Cross Account in AppViewX
- Account Level/Inner Inventory
- Configuring Organization Based Discovery
- Configuring IAM Policy Based Discovery
- Configuring Trigger Based Sync
- Configuring Schedule Based Sync

Step 1: Creating a IAM User in AWS

1. Login to AWS and from the **Services** menu, go to **Identity & Access Management Service** (IAM).
2. From the left navigation panel, under **Access management**, click **Users**.
   The **IAM > Users** screen is displayed.
3. To add a new user, click **Add users**.
   The **Specify user details** screen is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



4. On the **Specify user details** screen, enter the **User name** and click **Next**.

> **Note:** Console access is not required for this use case, hence the corresponding fields can be left blank.

   The **Set permissions** screen is displayed.
5. Click **Next**.

> **Note:** Instructions for setting permissions for this user are covered in **Step 3: Attaching Policies to the Created User**.

   The **Review and create** screen is displayed.
6. Click **Create user**.
   The **IAM > Users** screen is displayed. The user created is listed on this screen, under the **Users** list.

What to do next: Generate user identity to acquire the access key and secret key.

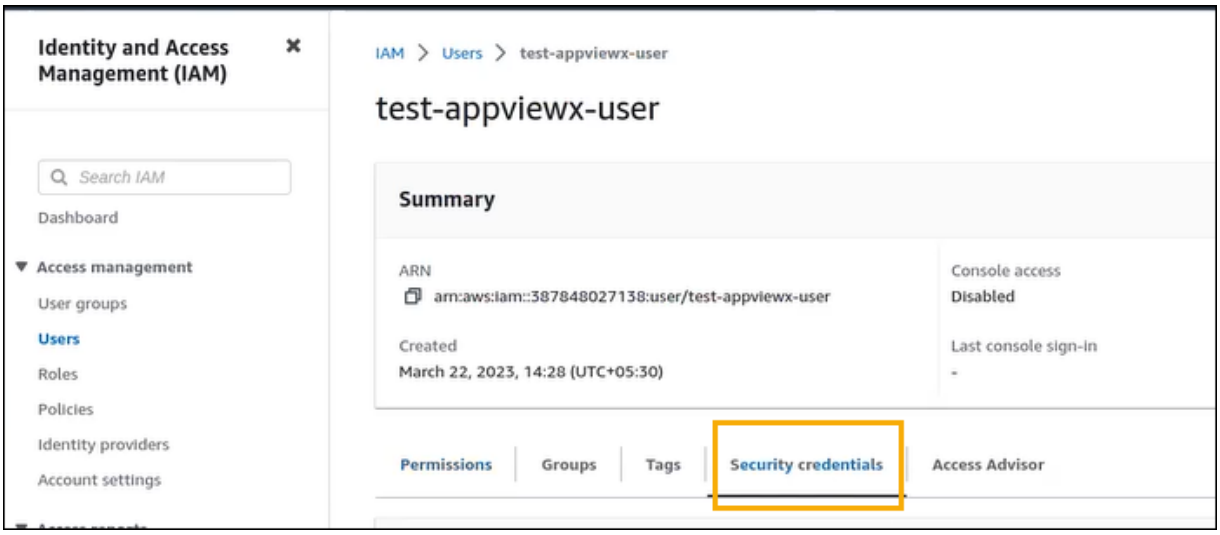
Step 2: Generating User Identity

In order to onboard a standalone account in AppViewX, you will require the account user's access key and secret key.

To retrieve the access key and the secret key:

1. From the **Users** list, click the **User name** of the user created in Step 1.
   The **IAM > Users > <selected user name>** screen is displayed.
2. Click **Security Credentials**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



3. From the **Access keys** section, click **Create access key**.
   You will be navigated **IAM > Users > <selected user name> > Create access key** screen.
4. Under **Access key best practices & alternatives**, select **Other** and click **Next**.
5. Click **Create access key**.
   The **Retrieve access keys** screen is displayed.
6. From the **Access key** section, copy the access key.
   To copy the **Secret access key**, click show and copy the secret access key.

> **Important:** On the **Retrieve access keys** page, the secret access key is displayed only once. Hence, it is recommended that you copy and paste the key to a secure location.

> **Tip:** Alternatively, you can click **Download .csv file** to download a file that contains your access key and secret access key.

7. Click **Done**.

What to do next: Attach policies to assign permissions to the created user.

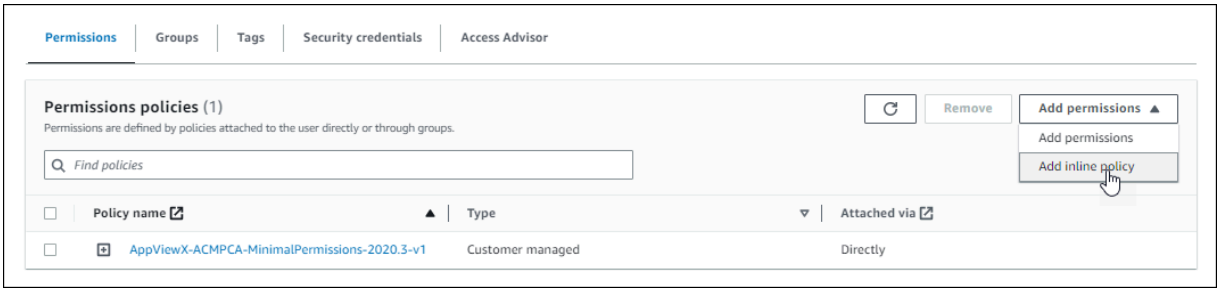
Step 3: Attaching Policies to the Created User

AWS supports two different policy types: **a customer inline policy**, which is a private set of permissions created for a specific user (recommended) and **a customer managed policy**, which is like a public policy that can be mapped to any new/existing users.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX recommends creating a dedicated policy for each service type.

1. From the user summary screen, under the **Permissions** tab, from the **Permissions policies** section, from the **Add permissions** dropdown menu, select **Add inline policy**.



   The **Create Policy** screen is displayed.
2. To create a policy by specifying the **JSON** structure:

   a. Clear the code in the **JSON** tab.

   b. For the required service, copy the JSON structure of the permissions and paste it in the **JSON** tab of the **Create policy** screen.
   For the full list of actions and the corresponding permissions, refer **AWS IAM Prerequisites for Master Account**.

3. Click **Review policy**.
   The **Create policy** > **Review policy** page is displayed.
4. On this page, enter a policy **Name**.

> **Tip:** While the policy name is subjective and is left to the user's discretion, AppViewX recommends the following naming convention: **Appviewx-<service name>-policy**

5. Click **Create policy**.

What to do next: Create a role in the child account in AWS.

- AWS IAM Prerequisites for Master Account

AWS IAM Prerequisites for Master Account

- IAM Prerequisites for Discovering Child Accounts using Policy-based Discovery
- IAM Prerequisites for Discovering Child Accounts using AWS Organization Services
- IAM Prerequisites for Enabling Assume Role Access to all AWS Accounts

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- IAM Prerequisites for Enabling Assume Role Access for a Specific Child Account
- IAM Prerequisites for Enabling S3 Bucket Access to the AppViewX Platform
- IAM Prerequisites for Accessing Organization Services to Discover AWS Accounts

IAM Prerequisites for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetPolicyVersion",
            "iam:GetPolicy",
            "iam:GetUserPolicy",
            "iam:ListGroupsForUser",
            "iam:ListGroupPolicies",
            "ec2:DescribeRegions",
            "iam:ListAttachedUserPolicies",
            "iam:ListAttachedGroupPolicies",
            "iam:ListUserPolicies",
 "iam:GetGroupPolicy",
 "iam:GetUser"
         ],
         "Resource": "arn:aws:iam::494906431772:role/AppViewX"
      }
   ]
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

IAM Prerequisites for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "organizations:Describe*",
            "organizations:List*"
         ],
         "Resource": "*"
      }
   ]
}
```

IAM Prerequisites for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
        "Resource": "*"
      }
    ]
}
```

IAM Prerequisites for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Resource": "arn:aws:iam::537094514474:role/AppViewX"
      }
   ]
}
```

IAM Prerequisites for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Resource": "arn:aws:iam::387848027138:role/AppViewX-S3-Bucket-Access"
      }
   ]
}
```

IAM Prerequisites for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

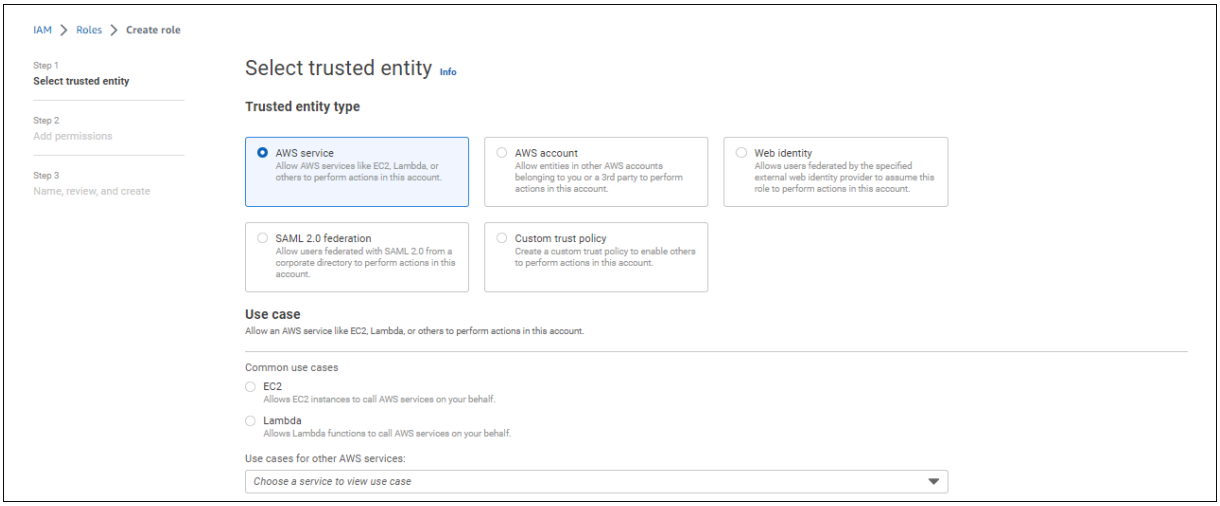
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
        "Resource": "arn:aws:iam::537094514474:role/AppViewX"
    }
  ]
}
```

Step 4: Creating a Role in the Child Account in AWS

1. Login to AWS and from the **Services** menu, navigate to **Identity & Access Management Service** (IAM).
2. From the left navigation panel, under **Access management**, click **Roles**.
   The **IAM > Roles** screen is displayed.
3. Click **Create Role**.
   The **IAM > Roles > Create role** page is displayed.



4. Under **Trusted entity type**, select **AWS account**.
5. Select **Another AWS account** and, in the **Account ID** field, enter the account ID of the master account.
6. Click **Next**.
7. On the **Add Permissions** screen, click **Next**.

> **Note:** Instructions for setting permissions for this role are covered in **Step 5: Attaching Policies to the Created Role**.

   The **Name, review, and create** screen is displayed.
8. Click **Create role**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The **IAM > Roles** screen is displayed. The role created is listed on this screen, under the **Roles** list.

> **Note:** The RoleARN of the roles created in the child account should match with the RoleARN defined in the master account user policy.

What to do next: Assign permissions to the role created in the child account using policies.

Step 5: Attaching Policies to the Created Role

1. From the **IAM > Roles** page, under the list of **Roles**, select the role created in step 4.
   For the selected role, the **IAM > Roles > <role name>** summary page is displayed.
2. Under the **Permissions** tab, from the **Permissions policies** section, from the **Add permissions** dropdown menu, select **Create inline policy**.
   The **Create Policy** page is displayed.
3. To create a policy by specifying the **JSON** structure:

   a. Clear the code in the **JSON** tab.

   b. For the required service, copy the JSON structure of the permissions and paste it in the **JSON** tab of the **Create policy** screen.
   For the full list of actions and the corresponding permissions, refer **AWS IAM Prerequisites for Child Account**.

4. Click **Review policy**.
   The **Create policy** > **Review policy** page is displayed.
5. On this page, enter a policy **Name**.

> **Tip:** While the policy name is subjective and is left to the user's discretion, AppViewX recommends the following naming convention: **Appviewx-<service name>-policy**

6. Click **Create policy**.

What to do next: If you want to associate the EC2 service with the onboarded account, create a EC2 role. If not, proceed to onboarding the cross account in AppViewX.

- AWS IAM Prerequisites for Child Account

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AWS IAM Prerequisites for Child Account

- IAM Prerequisites for Allowing an IAM User in the Master Account to Access Resources in the Child Account
- IAM Prerequisites for Discovering and Managing SSL Certificates in ACM
- IAM Prerequisites for Discovering and Managing SSL Certificates in CloudFront
- IAM Prerequisites for Managing SSM Permissions for the EC2 Policy
- IAM Prerequisites for Managing SSM Permissions for EC2 Role
- IAM Prerequisites for Discovering and Managing SSL Certificates in ELB
- IAM Prerequisites for Discovering and Managing Certificates in IAM
- IAM Prerequisites for Discovering and Managing Private CA Certificates

IAM Prerequisites for Allowing an IAM User in the Master Account to Access Resources in the Child Account

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Resource": "arn:aws:iam::387848027138:root"
      }
   ]
}
```

IAM Prerequisites for Discovering and Managing SSL Certificates in ACM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
        "Effect": "Allow",
        "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate"
        ],
        "Resource": "*"
    }
  ]
}
```

Note: Route53 IAM permissions are optional when automatic DNS record creation in Route53 is not required for Certificate Enrollment & Renewal requests.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "route53:ListHostedZones",
        "route53:ChangeResourceRecordSets"
      ],
      "Resource": "*"
    }
  ]
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

IAM Prerequisites for Discovering and Managing SSL Certificates in CloudFront

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
            "acm:GetCertificate",
            "acm:ListCertificates",
            "iam:ListServerCertificates",
            "ec2:DescribeRegions",
            "cloudfront:ListDistributions",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "cloudfront:UpdateDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListTagsForResource",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate"
         ],
         "Resource": "*"
      }
   ]
}
```

IAM Prerequisites for Managing SSM Permissions for the EC2 Policy

```
{
   "Version": "2012-10-17",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Managing SSM Permissions for EC2 Role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:DescribeDocument",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ssmmessages:OpenControlChannel",
        "ec2messages:DeleteMessage",
        "ssm:UpdateInstanceInformation",
        "ec2messages:FailMessage",
        "ssmmessages:OpenDataChannel",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing SSL Certificates in ELB

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "elasticloadbalancing:ModifyListener",
        "ec2:DescribeInstances",
        "iam:ListServerCertificates",
        "elasticloadbalancing:DescribeTags",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "ec2:DescribeRegions",
            "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeListeners",
            "ec2:DescribeAvailabilityZones",
            "acm:GetCertificate",
            "elasticloadbalancing:DescribeTargetHealth",
            "acm:ListCertificates",
            "elasticloadbalancing:DescribeTargetGroups",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "elasticloadbalancing:AddListenerCertificates",
            "elasticloadbalancing:DescribeListenerCertificates"
        ],
        "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing Certificates in IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    }
  ]
}
```

IAM Prerequisites for Discovering and Managing Private CA Certificates

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "acm:RenewCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "acm-pca:CreateCertificateAuthorityAuditReport",
 "acm-pca:DescribeCertificateAuthorityAuditReport,
 "acm-pca:GetCertificate",
 "acm-pca:ListCertificateAuthorities",
 "acm-pca:IssueCertificate",
 "acm-pca:RevokeCertificate",
 "s3:GetBucketLocation",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"s3:GetObject"
            ],
            "Resource": "*"
        }
    ]
}
```

Step 6: Creating a EC2 Role

Important: This step is required only if you choose to associate the EC2 service with the onboarded account.

1. From the left navigation panel, under **Access management**, click **Roles**.
   The **IAM > Roles** screen is displayed.
2. Click **Create role**.
   The **IAM > Roles > Create role** screen is displayed.
3. Under **Trusted entity type**, select **AWS service**.
4. Under **Use case**, select **EC2**.
5. Click **Next**.
6. On the **Add permissions** screen, click **Next**.
7. On the **Name, review, and create** screen, enter a role name, and review the rest of the role details.
8. Click **Create role**.

What to do next: Attach policies to the created EC2 role.

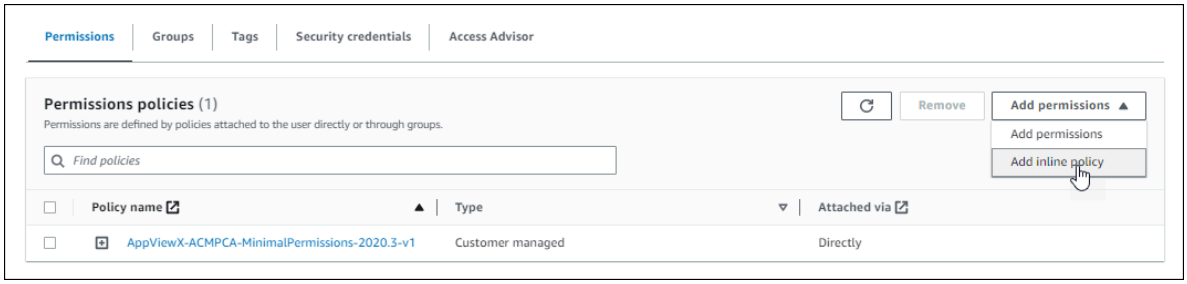
Step 7: Attaching Policies to a EC2 Role

1. On the **IAM > Roles** page, under **Roles**, select the EC2 role created in step 4.
2. From the role summary screen, under the **Permissions** tab, from the **Permissions policies** section, select the EC2 policy you want to attach to this role.
   OR

   To create a new EC2 policy:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. From the **Add permissions** dropdown menu, select **Add inline policy**.



The **Create Policy** screen is displayed.

b. Clear the code in the **JSON** tab.

c. For the EC2 service, copy the JSON structure of the permissions and paste it in the **JSON** tab of the **Create policy** screen.

Click here for the predefined JSON structure for:

- Managing SSM permissions for the EC2 policy
- Managing SSM permissions for the EC2 role

What to do next: Onboard the cross account in AppViewX.

Step 8: Onboarding a Cross Account in AppViewX

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, from the following options, select **Cross or Federated**.
Account name*	Enter the customer's unique AWS account name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Account number*	Enter the customer's AWS account number.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

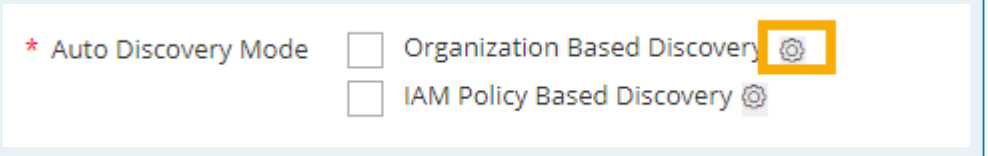
Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account)
Access key*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

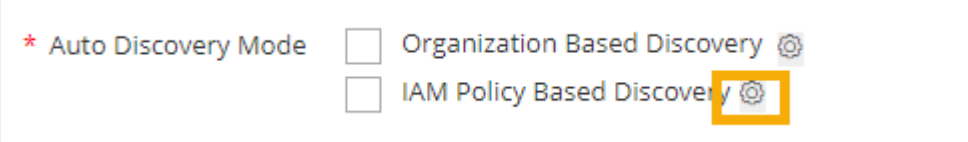
Field	Description
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	Select the auto discovery mode from the following options: • **Organization Based Discovery**: On selecting this option, the **Organization based discovery** popup window is displayed. For instructions on configuring organization based discovery, click here. **Tip:** An alternate way to access the **Organization based discovery** popup window is by clicking ⚙, located as shown in the image below: 

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM Policy**: On selecting this option, the **IAM Policy based discovery** popup window is displayed. For instructions on configuring IAM policy based discovery, click here. **Tip:** An alternate way to access the **IAM Policy based discovery** popup window is by clicking , located as shown in the image below:  **Note:** You can select one or both auto-discovery modes.
Service*	From the **Select the Service(s)** dropdown list, select the services required for the CLM operations. **Tip:** To select all services, select the **Select all** check box displayed at the beginning of the list of services. **Note:** • When **ACM (Certificate Authority)** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Certificate Authority Service**to configure the ACM services. These fields are explained in the table in Step 10. • When **Amazon Private CA** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Private CA**. These fields are explained in the table in Step 11. • When the **EC2(EC2 Instance)** service is selected, an additional set of fields is displayed to configure the EC2 services. These fields are explained in the **EC2 Services** table in Step 7.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **ACM Certificate Authority Service** section.

Note: This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for the ACM Certificate Authority Service

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected. From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.
**: Mandatory fields*	

9. Enter/Select the required details in the **ACM Private CA** section.

Note: This section is displayed only when the **ACM (Amazon Private CA)** service is selected for a **Cross or Federated** account.

Field description for the ACM Private CA section

Field	Description
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • ACM • PCA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>S3 Bucket*</td><td>
NOTE: This field is displayed only when the PCA operation mode is selected.

a. Enter the S3 bucket name.

b. Click  .

The ARN Advanced Settings action pane is displayed.

c. In the ARN Advanced Settings action pane, enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.
The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

10. Enter/Select the required details in the **EC2 Services** section.

Field description for the EC2 Services section

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>S3 Deployment Type*</td><td>From the dropdown list, select the deployment type for the S3 bucket.</td></tr>
<tr><td>S3 Bucket Name*</td><td>a. Click  .

The ARN Advanced Settings action pane is displayed.

b. In the ARN Advanced Settings action pane, enter the following details:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming.</td></tr>
<tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td></td><td>To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.</td></tr></table>
**: Mandatory fields*	

11. To add the new device to the cloud device inventory, click **Add**.

> **Tip:** To select multiple services for a device, after you click **Add**, go back to the **Services** dropdown list and select the next service you want to enable for the device. Enter/select the rest of the details and click **Add**. Repeat this process for as many services you want to enable for the new device. The table is populated with a separate entry for each service.

- Details of the child accounts for the added master account are displayed in the inner inventory table at the bottom of the page. The details captured in the inner inventory are explained here.
- Details of the master account are listed on the **CERT+** > **Administration** > **Certificate Authority** > **<Selected CA>** page.

> **Note:** For a public Certificate Authority, only the child account details are listed on the **CERT +** > **Administration** > **Certificate Authority** > **Amazon** > **ACM CA** page. There is no inner inventory for a public certificate authority.

12. After enabling all the services for the new device, click **Save**.
    - On saving the device, through SSM, AppViewX will communicate with EC2 instances through SSM.
    - AppViewX will discover the processes from these instances and manage them in the Server device inventory.

Once all the details are entered, you can add them to the Apache Linux server.

> **Note:** Apart from the Apache and Tomcat processes vendor, the rest of the processes will be managed in the server inventory only as "Generic Linux".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

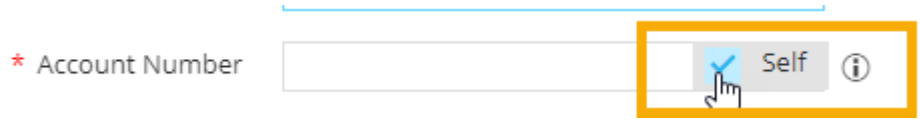
Field	Description
	This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.
   The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.
   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:
- If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**. 
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

AWS Cross/Federated Account Onboarding

The process of onboarding a cross or federated account access involves the following steps:

- Step 1: Creating an S3 bucket using the Cloudformation template
- Step 2: Creating a child account using the CloudFormation template
- Step 3: Creating a master account using the CloudFormation template

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Step 4: Mapping EC2 roles to a customer's EC2 instances
• Step 5: Testing Onboarding in the AppViewX Environment

Step 1: Creating an S3 bucket using the Cloudformation template

1. Login to the AWS account and go to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.
3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.
4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:
   a. For **Template source**, select **Upload a template file**.
   b. To **Upload a template file**, click **Choose file**.
   c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
   d. Select the **S3Bucket.yaml** file and click **Open**.
6. Click **Next**.

   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.
7. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemo-S3**.
8. In the **Parameters** section, enter the following details:

   a. **AccountId**: From the top-right corner of the screen, click your username and copy the account ID displayed.

   b. **BucketName**: Enter a name for the S3 bucket that will be created in the backend. Recommended format to name the S3 bucket: **avxdemo-<account ID>**.

   c. **OrganizationID**:
      i. From the top-right corner of the screen, click your username.
      ii. From the menu displayed, right click **Organization** to open it in a new tab.

      The **Dashboard** is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

iii. From the **Dashboard**, copy the organization ID and paste it into the **OrganizationID** field.

> **Note:** The organization ID is a mandatory entry for the CloudFormation template.

d. **RoleName**: Enter a name for the S3 bucket role. For the purpose of this guide, the S3 bucket role will be called **avxdemos3bucketrole**.

The details entered on the **Specify stack details** page will be used to create a bucket policy for the S3 bucket created for the AWS account. This bucket policy can be customized later based on customer preferences for how they want to secure their infrastructure.

9. Click **Next**.
   The **Configure stack options** page (step 3 of the stack creation process) is displayed.
10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
11. Click **Next**.
    The **Review <stack name>** page (step 4 of the stack creation process) is displayed
12. On the **Review <stack name>** page, scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
13. Click **Create stack**.

    The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    - **Stack info**
    - **Events**
    - **Resources**
    - **Outputs**
    - **Parameters**
    - **Templates**
    - **Change sets**

    When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**. This means that, in the backend, an S3 bucket as well as the roles required to provision the bucket have been created. The bucket policy for the S3 bucket has also been updated accordingly.

14. Go to the **Parameters** tab and note the bucket name to use it in the CloudFormation template for the master account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

What to do next: Create a child account using the CloudFormation template.

Step 2: Creating a child account using the CloudFormation template

1. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.

2. From the navigation pane on the left, click **Step 2 Specify stack details**.
   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.
3. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemoc1**.
4. In the **Parameters** section, enter the following details:
   a. **MasterAccountNumber**: From the top-right corner of the screen, click your username and copy the account ID displayed. Paste it in the **MasterAccountNumber** field.
   b. **S3BucketName**: Enter the S3 bucket name copied from the **Parameters** tab of the **avxdemo-S3** stack.
5. Click **Next**.

   The **Configure stack options** page (step 3 of the stack creation process) is displayed.

6. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
7. Click **Next**.

   The **Review <stack name>** page (step 4 of the stack creation process) is displayed.

8. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
9. Click **Create stack**.

   The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

   - **Stack info**
   - **Events**
   - **Resources**
   - **Outputs**
   - **Parameters**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Templates**
- **Change sets**

When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**.

10. Navigate to the **Resources** tab for the **avxdemoc1** stack.
    You will see that a policy called **AppViewXCLM** has been created. This policy will have all the permissions and prerequisites required for AppViewX to discover all the ACM, ELB, and EC2 instances.
11. Navigate to the **Outputs** tab for the **avxdemoc1** stack.
    Note down the **ChildRoleARN** to use it in the CloudFormation template for the master account.

What to do next: Create a master account using the CloudFormation template.

Step 3: Creating a master account using the CloudFormation template

1. Go to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.
3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.
4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:
   a. For **Template source**, select **Upload a template file**.
   b. To **Upload a template file**, click **Choose file**.
   c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
   d. Select the **master_account.yaml** file and click **Open**.
6. Click **Next**.

   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.
7. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemom1**.
8. In the **Parameters** section, enter the following details:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. For **ApplyAssumeRoleForAll**, from the dropdown list, select **False**.

b. From the **Outputs** tab of the **avxdemoc1** CloudFormation template for the child account, copy the **ChildRoleARN** and paste it in the following fields:
   - **ChildRoleARN**
   - **OrganizationRoleARN**

c. From the **Outputs** tab of the **avxdemo-S3** CloudFormation template, copy the **S3BucketAssumeRole** and paste it in the following fields:
   - **S3BucketRoleARN**
   - **SQSRoleARN**

d. In the **UserName** field, enter a username for the IAM account. For the purpose of this guide, the username will be set to **avxdemo-user**.

9. Click **Next**.
   The **Configure stack options** page (step 3 of the stack creation process) is displayed.
10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
11. Click **Next**.
    The **Review <stack name>** page (step 4 of the stack creation process) is displayed
12. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
13. Click **Create stack**.

    The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    - **Stack info**
    - **Events**
    - **Resources**
    - **Outputs**
    - **Parameters**
    - **Templates**
    - **Change sets**
14. From the **Outputs** tab of the stack, note the access key and the secret key information to use in AppViewX.

What to do next: Map the EC2 roles to the customer's EC2 instances.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Step 4: Mapping EC2 roles to a customer's EC2 instances

The EC2 role created using the CloudFormation template with the naming convention **<Stack_Name>-Ec2RoleForSSM** must be mapped to the EC2 instances. This mapping is required for enabling SSM communication between the instances and AppViewX and for enabling access to the S3 buckets to store the SSM run command response.

What to do next: Test device onboarding the AppViewX environment.

Step 5: Testing Onboarding in the AppViewX Environment

1. Login to AppViewX.
2. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
3. From the **Device :: ADC** page, select **Cloud**.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **AWS**.
5. Enter/select the **Basic information**.

Field description for the Basic information section

Field	Description
Account type*	From the dropdown list, select **Cross or Federated**.
Account name*	Enter the account name, **avxdemo**.
Account number*	Enter the AWS account number.
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for the communication, select this checkbox.
Default Region*	From the dropdown list, select a default region for the API communication.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter the **Credentials**-related details:

Field descriptions for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: To manually enter the access and secret key for the customer's AWS account) • **Credential List - CyberArk**: To automatically retrieve the customer's AWS key details from CyberArk)
Access key*	Copy the **AccessKey** from the **Outputs** tab of the **avxdemom1** template.
Secret key*	Copy the **Secret Access Key** from the **Outputs** tab of the **avxdemom1** template.
**: Mandatory fields*	

7. Enter the details required to **Discover resources**.

Field descriptions for the Discover resources section

Field	Description
Auto Discover Resources*	By default, the **Auto Discover Resources** toggle key is set to **ON** and is non-editable. Enabling this feature allows discovering all the cross or federated/child accounts for the provided master account details.
Advanced Settings*	By default, the **Advanced Settings** toggle key is set to **ON** and is non-editable. This feature allows customizing the auto discovery process.
AutoSync	To enable automatic synchronization, enable this toggle.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	Select the **IAM Policy**.
Services*	Select the ACM, ELB, and EC2 services (and their subservices, as required).
Service region*	For the purpose of this solution guide, click **Fetch Region** and select the regions US East (N. Virginia) and US West (N. California).
Route53 Zone Auto Approval*	To support DNS validation as an automatic process, turn on the **Route53 Zone Auto Approval** toggle.
Cert sync	Select one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • Minimum: 900 seconds (15 minutes) • Maximum: 129,600 seconds (36 hours) • Default: 3600 seconds (1 hour)
Role Session name*	**Role Session name** is an identifier for the assumed role session. Use the **Role Session name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons. By default, the **Role Session name** is set to **appviewx**.
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account. For the purpose of this guide, external ID is undefined.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Source Identity	The source identity is specified by the principle that is calling the **AssumeRole** operation. For the purpose of this guide, source identity is undefined.
Session Tags	Enter the key-value attribute pairs required when assuming an IAM role or federating a user in the AWS STS.
**: Mandatory fields*	

8. In the **EC2 Services** section, copy the **S3Bucket Name** from the **Resources** tab of the **avxdemo-S3** template.
9. In the **S3 Bucket Name** field, click .
   The **ARN Advanced Settings** pop-up window is displayed.
10. Copy the **Role ARN** from the **Outputs** tab of the **avxdemo-S3** template and paste it in the **Role ARN** field.
11. Click **Apply**.
12. Click **Save**.

The discovered account will be displayed in the grid on the **Device :: Cloud** page.

Note: The discovered account will be added one more time as a child account since the use case uses federated access. This behaviour will be altered in the future releases to avoid dual listing of discovered AWS accounts.

Azure

Important: After migrating to AppViewX v2022.1.0 and beyond, from any of the previous versions, ensure that you have entered the data centre details for each existing Azure account. For instructions to do this, follow steps 1-5 listed here.
This step is not required for migration to v2022.1.0 to any of the later versions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Important: At the time of migrating to AppViewX v2023.1.0 FP2 and beyond, manually trigger a config fetch for all the Azure accounts already created. Delete all on-demand and scheduled discovery instances created for Azure and, post a successful config fetch, create a new discovery instance.

This will ensure that all functionality enhancements are applied correctly.

This documentation focuses on the benefits and implementation of integrating the following Azure services with AppViewX, for a holistic certificate lifecycle management for the Azure services:

- Azure Key Vault
- Azure Application Gateway
- Azure Virtual Machines

- Azure Services Supported by AppViewX
- Permissions Required for Onboarding Azure
- Onboarding Azure Settings in AppViewX

Azure Services Supported by AppViewX

AppViewX supports the following Azure services:

- **Key Vault**

  The Azure Key Vault is a key management solution from Microsoft that offers the following features:

  - Secrets Management: The key vault can be used for securely storing and managing access to tokens, passwords, API keys, and other secrets.
  - Key Management: The key vault simplifies the creation and management of encryption keys used for data encryption.
  - Certificate Management: Azure key vault simplifies the certificate lifecycle management of TLS/SSL certificates

- **Application Gateway**

  The Azure Application Gateway is a web traffic load balancer that helps to optimize and secure web applications traffic. The application gateway operates at the application layer of the OSI model and makes routing decisions based on attributes of an HTTP request, for example the URI path or the host headers.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Virtual Machines**

  Azure Virtual Machines (VMs) are scalable and flexible computing resources provided by Microsoft Azure. They enable users to run virtualized Windows or Linux servers in the cloud. Azure VMs allow you to quickly deploy and manage virtualized infrastructure to support various applications, workloads, and services.

Permissions Required for Onboarding Azure

- Key Vault
- Application Gateway
- Virtual Machine

Key Vault


```
{
 "properties": {
  "roleName": "AppViewX_KeyVault_Role",
  "description": "",
  "assignableScopes": [
   "/subscriptions/f2689969-42f6-4fb5-b3be-e3a02e33751c"
  ],
  "permissions": [
   {
    "actions": [
     "Microsoft.KeyVault/vaults/read"
    ],
    "notActions": [],
    "dataActions": [
     "Microsoft.KeyVault/vaults/certificates/import/action",
     "Microsoft.KeyVault/vaults/certificates/create/action",
     "Microsoft.KeyVault/vaults/certificates/update/action",
     "Microsoft.KeyVault/vaults/certificates/read"
    ],
    "notDataActions": []
   }
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  ]
 }
}
```

Application Gateway

```
{
   "properties": {
      "roleName": "AppViewX_AppGW_Permission",
      "description": "",
      "assignableScopes": [
         "/subscriptions/f2689969-42f6-4fb5-b3be-e3a02e33751c"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.Network/applicationGateways/write",
               "Microsoft.Network/applicationGateways/read",
               "Microsoft.Network/applicationGatewayAvailableSslOptions/predefinedPolicies/read",
               "Microsoft.Network/applicationGatewayAvailableSslOptions/read",
               "Microsoft.Network/virtualNetworks/subnets/join/action"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
         }
      ]
   }
}
```

Virtual Machine

```
{
  "properties": {
    "roleName": "AppViewX_VirtualMachine_Role",
    "description": "",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  "assignableScopes": [
    "/subscriptions/f2689969-42f6-4fb5-b3be-e3a02e33751c"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.Compute/virtualMachines/read"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ]
 }
}
```


Onboarding Azure Settings in AppViewX

1. Go to  (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click  (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox.
**: Mandatory fields*	

6. Enter/Select the **Key information**.

Field description for the Key information section

Field	Description
***Subscription ID**	Enter the customer's Azure subscription ID.
***Tenant ID**	Enter the customer's Azure tenant ID.
***Client ID**	Enter the customer's Azure client ID.
***Client secret**	Enter the customer's Azure client secret key.
***Services**	From the dropdown list, select the service(s) that will be mapped to this setting.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastru On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the  icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule.

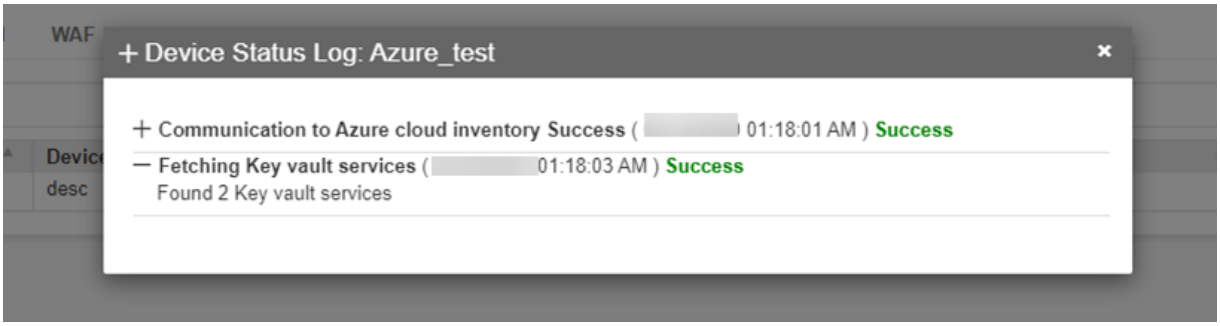
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Field descriptions for the General Information section **Field** | *Frequency of Sync | Set the s frequenc i. From ii. From **Advance Settings** | To set th i. Enab The A (in the ii. To se The F iii. Enter The s
*: Mandatory fields	

7. From **Additional attributes**, for the required services, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
8. Click **Save**.
9. Return to the **Device :: Cloud** page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.



11. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Google Cloud Platform (GCP)

Google Cloud Platform (GCP) is a suite of computing services provided by Google, that can be integrated with an organization's multicloud setup to meet specific business requirements.

Using GCP in a multicloud setup offers the following advantages:

- Diversity of services (especially in the areas of big data, machine learning, and data analytics) to enhance the overall capabilities of your organization's infrastructure
- Access to advanced analytics and process automation tools
- Support for data analytics and big data capabilities
- Global network infrastructure known for its speed and reliability
- Security expertise
- Data storage and management capabilities

- GCP Services Supported by AppViewX
- Onboarding GCP Projects in AppViewX
- Limitations

GCP Services Supported by AppViewX

AppViewX supports the following GCP services:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Certificate Manager**

  Certificate Manager is a managed GCP service that automates the process of obtaining, issuing, and renewing certificates, and then seamlessly integrating to provision your certificates for the load balancer.

- **Load Balancer**

  GCP comes with a set of load balancers that distribute incoming network traffic evenly across multiple instances or services. Load balancers ensure that your multicloud setup conforms to the requirements of high availability, fault tolerance, and scalability.

  Types of load balancers in GCP:
  - Google Cloud Load Balancer
  - Network Load Balancer
  - SSL Proxy Load Balancer
  - TCP Proxy Load Balancer
  - UDP Load Balancer
  - Internal TCP/UDP Load Balancer
- **Classic Certificates**

  Classic certificates is a GCP service that lets you create and manage Google-managed SSL certificates.

Onboarding GCP Projects in AppViewX

- Onboarding a Single GCP Project
- Onboarding GCP Projects within an Organization

Onboarding a Single GCP Project

- Prerequisites for Onboarding a Single GCP Project
- Onboarding a Single GCP Project in AppViewX

Prerequisites for Onboarding a Single GCP Project

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To onboard a single GCP project in AppViewX, you are first required to create and associate roles with the project to be onboarded.

1. To create a custom role, create a **.yml** file with the permissions to be assigned to that role.
   A sample **.yml** is given below:

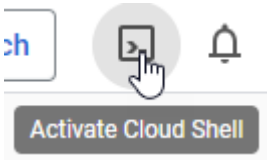
```
title: test_gcp_project_role
description: Test GCP PROJECT
stage: GA
includedPermissions:
- certificatemanager.certmapentries.create
- certificatemanager.certmapentries.delete
- certificatemanager.certmapentries.get
- certificatemanager.certmapentries.list
- certificatemanager.certmapentries.update
- certificatemanager.certmaps.create
- certificatemanager.certmaps.delete
- certificatemanager.certmaps.get
- certificatemanager.certmaps.list
- certificatemanager.certmaps.update
- certificatemanager.certmaps.use
- certificatemanager.certs.create
- certificatemanager.certs.delete
- certificatemanager.certs.get
- certificatemanager.certs.list
- certificatemanager.certs.update
- certificatemanager.certs.use
- compute.globalOperations.get
- compute.regionOperations.get
- compute.regionSslCertificates.create
- compute.regionSslCertificates.delete
- compute.regionSslCertificates.get
- compute.regionSslCertificates.list
- compute.regionTargetHttpsProxies.get
- compute.regionTargetHttpsProxies.list
- compute.regionTargetHttpsProxies.setSslCertificates
- compute.regionTargetHttpsProxies.update
- compute.regionTargetHttpsProxies.use
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
- compute.regions.get
- compute.regions.list
- compute.sslCertificates.create
- compute.sslCertificates.delete
- compute.sslCertificates.get
- compute.sslCertificates.list
- compute.targetHttpsProxies.get
- compute.targetHttpsProxies.list
- compute.targetHttpsProxies.setCertificateMap
- compute.targetHttpsProxies.setSslCertificates
- compute.targetHttpsProxies.update
- compute.targetHttpsProxies.use
- compute.targetSslProxies.get
- compute.targetSslProxies.list
- compute.targetSslProxies.setCertificateMap
- compute.targetSslProxies.setSslCertificates
- compute.targetSslProxies.update
- compute.targetSslProxies.use
- resourcemanager.projects.get
```

2. From the Google Cloud Console, from the dropdown menu (

), select the project you want to onboard.

3. Click 

(**Activate Cloud Shell**) to activate the cloud shell for the selected project and execute the following command:

```
gcloud iam roles create ROLE_ID --project=PROJECT_ID --file=YAML_FILE_PATH
```

4. From the Google Cloud Console, in the project you want to onboard, create a service account. To do this:

   a. Go to ☰ (**Menu**) > **IAM & Admin** > **Service Accounts**.

   b. Click **+CREATE SERVICE ACCOUNT**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

c. Under **Service Account Details**, enter a **Service account name**.
The **Service account ID** is automatically generated.

d. [Optional] Enter a **Service account description**.

e. Click **CREATE AND CONTINUE**.

f. Under **Grant this service account access to project**, from the **Select a role** dropdown list, select the custom role created in steps 1 and 2.

g. Click **CONTINUE**.

h. Under **Grant users access to this service account**, click **DONE**.

> **Note:** This is an optional section and for the purpose of this document, can remain unspecified.

You will be navigated to the **Service accounts** page.

i. From the **Email** account, select the service account just created and go to the **KEYS** tab.

j. Click **ADD KEY**.

k. From the **Create private key for "<service account name>"** dialog box, select the format in which you want to download the key details.
Your options include: **JSON** (Recommended) or **P12**

l. Click **CREATE**.
The key details, in the selected format, are downloaded to your local system.

5. Login to the AppViewX UI to onboard the GCP project.

Onboarding a Single GCP Project in AppViewX

1. In the AppViewX UI, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
The **Device** :: **ADC** page is displayed.
2. On the **Device** :: **Cloud** page, click (**Add**).
The **Device :: Cloud > Add** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Under **Device details**, from the list of **Vendors**, select **GCP**.
4. Enter/Select the **Basic Information** for onboarding a single GCP project.

Field description for the basic information

Field	Description
***Onboarding Method**	From the dropdown list, select **Onboard a Single GCP Project**.
***Account Name**	Enter your unique GCP account name. **Note:** • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and the period (**.**) characters.
Account Description	Enter a description of the GCP account to be added.
Proxy Required	To use a proxy server for this communication, select this checkbox.
***Data Center**	From the dropdown list, select the data center through which communication with the certificate authority will be established.

5. Enter/Select the **Project & Credential Details**.

Field descriptions for the project and credential details

Field	Description
Service Account Key	To access the GCP services using AppViewX, the credentials are supplied either in a JSON or in the form of a certificate file. After you have created the GCP service account, you can download the JSON file or the certificate file with the credential details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Depending on the artifact download, from the **Service Account Key** field, select the **JSON File** or the **Certificate Upload** option.
***Upload JSON**	**Note:** This field is displayed only when **Service Account Key** = **JSON File**. Click **Upload** and navigate to the location of the JSON file.
***Certificate and Key**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Click **Upload** and navigate to the location of the certificate file.
***Email**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your email ID registered with GCP.
***Project Id**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your GCP project ID.
Validate Credential	To validate the credentials uploaded using JSON/ certificate file, click validate credential.

6. Enter/Select the details required to **Discover Resources**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: The fields in this section are enabled only after the credentials entered in the **Project & Credential Details** section have been validated.

Field descriptions for discovering resources

Field	Description
***Service Type**	From the dropdown list, select the services required for CLM operations.
Cert Sync	Select from one of the following options: • **Managed**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with your GCP account but certificate discovery will be disabled.
Auto Sync	To enable (default)/disable automatic synchronization, use the **Auto Sync** key. Currently the GCP implementation in AppViewX only supports schedule-based synchronization.
Schedule Based Discovery	**Note:** This field is displayed when **Auto Sync** is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	To schedule a discovery, set the frequency using the two dropdown lists for this field. For example, to set the frequency to 10 days: a. From the first dropdown list, select **10**. b. From the second dropdown list, select **Days**.

7. Click **Save**.
   Details of the added GCP account are displayed in the outer inventory (explained here).

Onboarding GCP Projects within an Organization

- Prererequisites for Onboarding GCP Projects within an Organization
- Onboarding GCP Projects within an Organization in AppViewX

Prererequisites for Onboarding GCP Projects within an Organization

To onboard GCP projects within an organization in AppViewX, at the organizational level, you are first required to create and associate roles with the projects to be onboarded.

1. To create a custom role, create a **.yml** file with the permissions to be assigned to that role.
   A sample **.yml** is given below:

```
title: test_gcp_org_role
description: Test GCP ORG
stage: GA
includedPermissions:
- certificatemanager.certmapentries.create
- certificatemanager.certmapentries.delete
- certificatemanager.certmapentries.get
- certificatemanager.certmapentries.list
- certificatemanager.certmapentries.update
- certificatemanager.certmaps.create
- certificatemanager.certmaps.delete
- certificatemanager.certmaps.get
- certificatemanager.certmaps.list
```

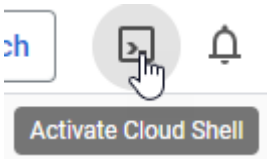
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- certificatemanager.certmaps.update
- certificatemanager.certmaps.use
- certificatemanager.certs.create
- certificatemanager.certs.delete
- certificatemanager.certs.get
- certificatemanager.certs.list
- certificatemanager.certs.update
- certificatemanager.certs.use
- compute.globalOperations.get
- compute.regionOperations.get
- compute.regionSslCertificates.create
- compute.regionSslCertificates.delete
- compute.regionSslCertificates.get
- compute.regionSslCertificates.list
- compute.regionTargetHttpsProxies.get
- compute.regionTargetHttpsProxies.list
- compute.regionTargetHttpsProxies.setSslCertificates
- compute.regionTargetHttpsProxies.update
- compute.regionTargetHttpsProxies.use
- compute.regions.get
- compute.regions.list
- compute.sslCertificates.create
- compute.sslCertificates.delete
- compute.sslCertificates.get
- compute.sslCertificates.list
- compute.targetHttpsProxies.get
- compute.targetHttpsProxies.list
- compute.targetHttpsProxies.setCertificateMap
- compute.targetHttpsProxies.setSslCertificates
- compute.targetHttpsProxies.update
- compute.targetHttpsProxies.use
- compute.targetSslProxies.get
- compute.targetSslProxies.list
- compute.targetSslProxies.setCertificateMap
- compute.targetSslProxies.setSslCertificates
- compute.targetSslProxies.update
- compute.targetSslProxies.use

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
- resourcemanager.folders.get
- resourcemanager.folders.list
- resourcemanager.projects.get
- resourcemanager.projects.list
```

2. From the Google Cloud Console, from the dropdown menu (

), select the organization the projects of which you want to onboard.
3. Each organization has multiple projects. Select one project belonging to the organization you selected in step 2.
4. Click 

(**Activate Cloud Shell**) to activate the cloud shell for the selected project and execute the following command:

```
gcloud iam roles create ROLE_ID --organization=ORG_ID --file=YAML_FILE_PATH
```

5. From the Google Cloud Console, in the project you want to onboard, create a service account. To do this:

   a. Go to (**Menu**) > **IAM & Admin** > **Service Accounts**.

   b. Click **+CREATE SERVICE ACCOUNT**.

   c. Under **Service Account Details**, enter a **Service account name**. The **Service account ID** is automatically generated.

   d. [Optional] Enter a **Service account description**.

   e. Click **CREATE AND CONTINUE**.

   f. Under **Grant this service account access to project**, from the **Select a role** dropdown list, select the custom role created in steps 1 and 2.

   g. Click **CONTINUE**.

   h. Under **Grant users access to this service account**, click **DONE**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

> **Note:** This is an optional section and for the purpose of this document, can remain unspecified.

You will be navigated to the **Service accounts** page.

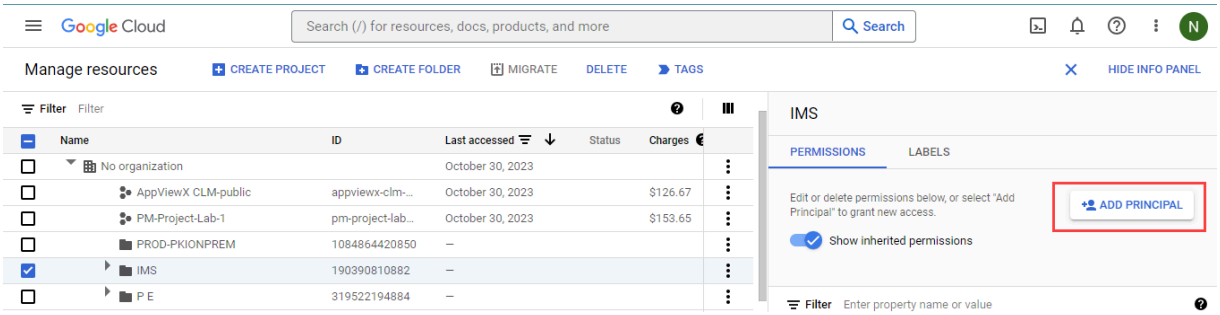
i. From the **Email** account, select the service account just created and go to the **KEYS** tab.

j. Click **ADD KEY**.

k. From the **Create private key for "<service account name>"** dialog box, select the format in which you want to download the key details.
Your options include: **JSON** (Recommended) or **P12**

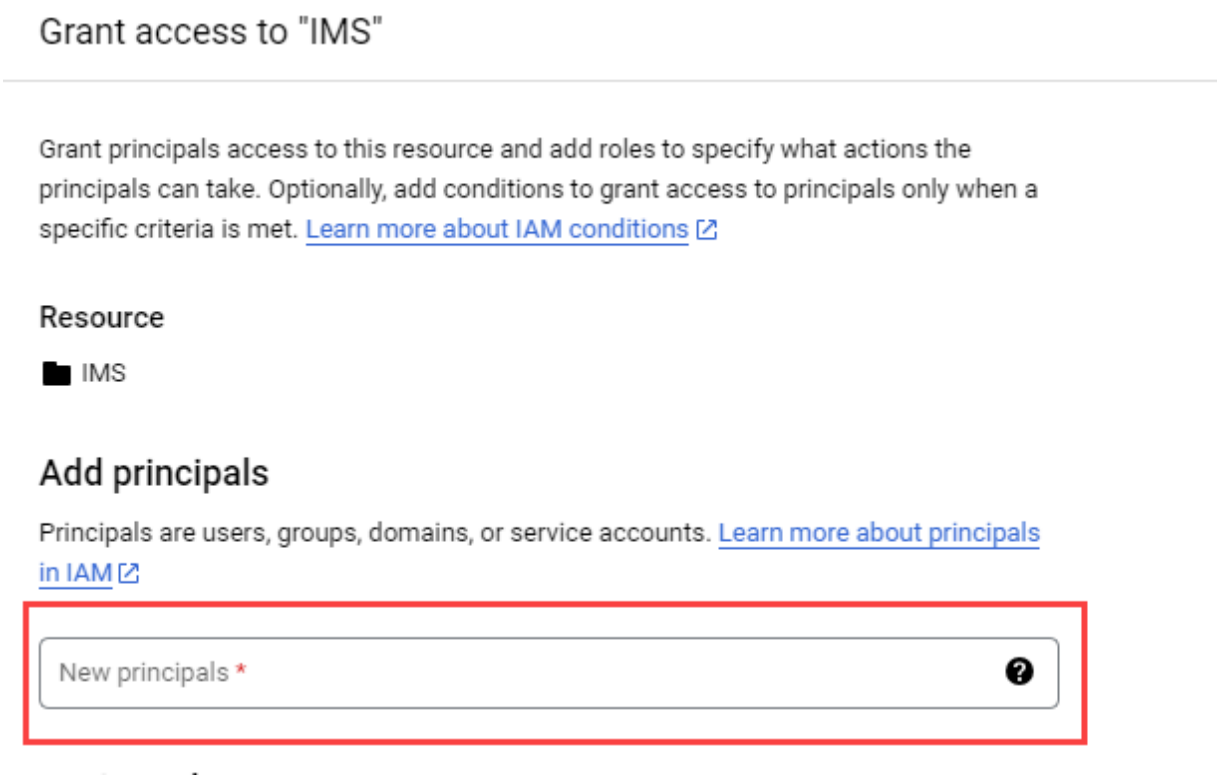
l. Click **CREATE**.
The key details, in the selected format, are downloaded to your local system.

6. On the Google Cloud Console, go to **Menu** > **IAM & Admin** > **Manage Resources**.
The **Manage Resources** screen is displayed.
7. Select the organization that you want to onboard and click **Add Principal**.



8. In the **Grant access to "<organization name>"** section, in the **New principals** field, paste the email address of the service account created in step 5.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



9. From the **Select a role** dropdown list, select the custom role created in step 1 of the prerequisites.
10. Click **SAVE**.
11. Login to the AppViewX UI to onboard the GCP project.

Onboarding GCP Projects within an Organization in AppViewX

1. In the AppViewX UI, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device** :: **ADC** page is displayed.
2. On the **Device** :: **Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
3. Under **Device details**, from the list of **Vendors**, select **GCP**.
4. Enter/Select the **Basic Information** for onboarding a single GCP project.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for the basic information

Field	Description
***Onboarding Method**	From the dropdown list, select **Onboard GCP Projects within Organization**.
***Account Name**	Enter your unique GCP account name. **Note:** • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and the period (**.**) characters.
Account Description	Enter a description of the GCP account to be added.
Proxy Required	To use a proxy server for this communication, select this checkbox.
***Data Center**	From the dropdown list, select the data center through which communication with the certificate authority will be established.

5. Enter/Select the **Project & Credential Details**.

Field descriptions for the project and credential details

Field	Description
***Organization ID**	To discover and onboard the GCP projects within the organization, enter your unique GCP organization resource ID.
Service Account Key	To access the GCP services using AppViewX, the credentials are supplied either in a JSON or in the form of a certificate file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	After you have created the GCP service account, you can download the JSON file or the certificate file with the credential details. Depending on the artifact download, from the **Service Account Key** field, select the **JSON File** or the **Certificate Upload** option.
***Upload JSON**	**Note:** This field is displayed only when **Service Account Key** = **JSON File**. Click **Upload** and navigate to the location of the JSON file.
***Certificate and Key**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Click **Upload** and navigate to the location of the certificate file.
***Email**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your email ID registered with GCP.
***Project Id**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your GCP project ID.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Validate Credential	To validate the credentials uploaded using JSON/ certificate file, click validate credential.

6. Enter/Select the details required to **Discover Resources**.

> **Note:** The fields in this section are enabled only after the credentials entered in the **Project & Credential Details** section have been validated.

Field descriptions for discovering resources

Field	Description
***Project Onboarding State**	From the following values, select the state for onboarding the projects discovered from the GCP organization: • **Managed**: Enables project onboarding and allows instant GCP cloud resource and certificate discovery • **Unmanaged**: Disables project onboarding, preventing resource and certificate discovery for these projects.
***Service Type**	From the dropdown list, select the services required for CLM operations.
Cert Sync	Select from one of the following options: • **Managed**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with your GCP account but certificate discovery will be disabled.
Auto Sync	To enable (default)/disable automatic synchronization, use the **Auto Sync** key. Currently the GCP implementation in AppViewX only supports schedule-based synchronization.
Schedule Based Discovery	**Note:** This field is displayed when **Auto Sync** is enabled. To schedule a discovery, set the frequency using the two dropdown lists for this field. For example, to set the frequency to 10 days: a. From the first dropdown list, select **10**. b. From the second dropdown list, select **Days**.

7. Click **Save**.
   Details of the added GCP account are displayed in the outer inventory (explained here).

Limitations

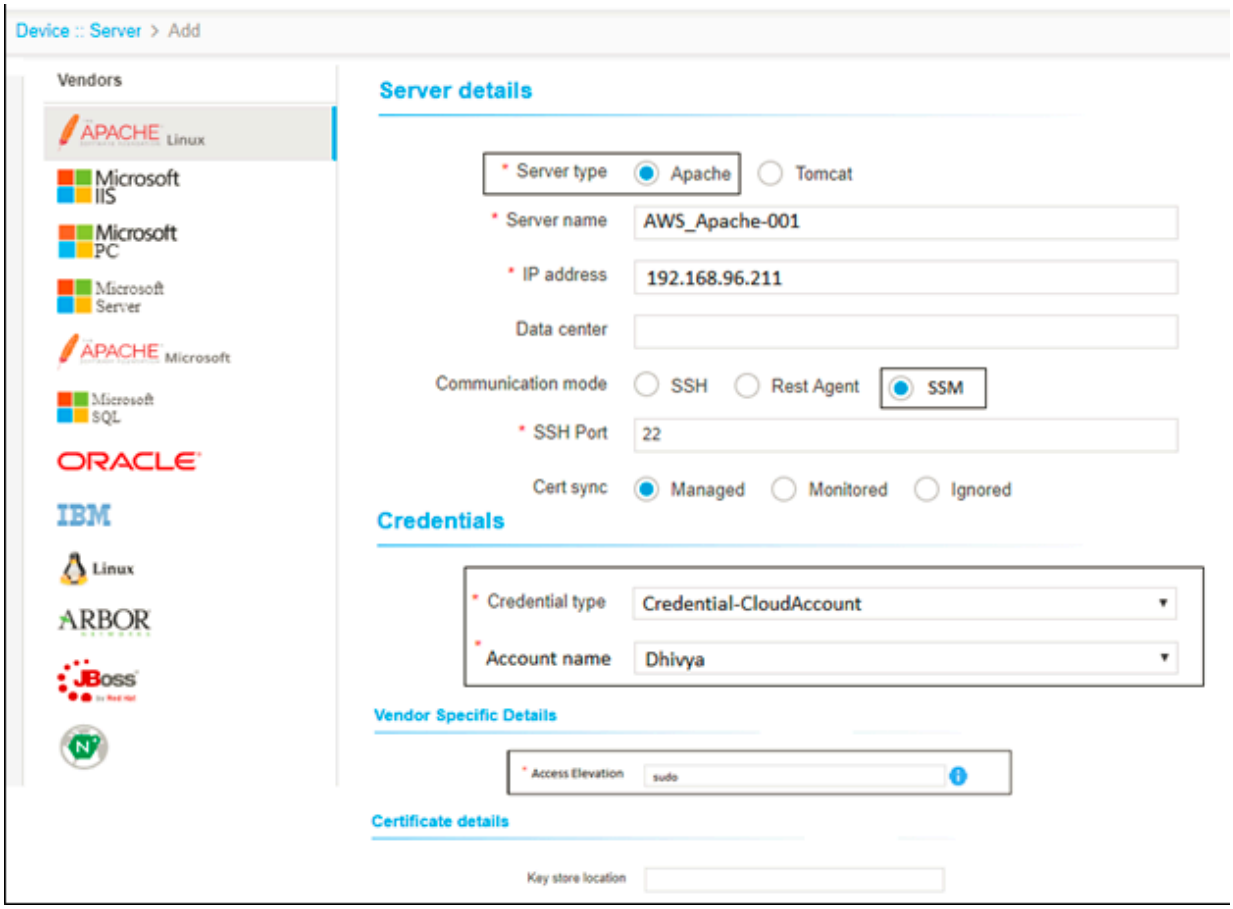
- Pushing certificates to the Certificate Manager and binding to the Classic Loadbalancers in the standard tier is currently not supported.

Apache SSM integration specification

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Device Addition

- **Apache (Linux)** serversdiscovered from Amazon EC2 instances should be added under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill in the Apache (Linux) device addition page.
- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.
- By default, access elevation should be selected as **Sudo.**



Credential management

- Credential Type is a mandatory field.
- When a device is added from a could account, **Credential-Cloud Account must** be displayed corresponding to the credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- While modifying the mandatory details in the Apache form, the user should be able to select a different cloud account credential that is added to the cloud inventory.
- Similarly, while modifying the mandatory details in the Apache form, the user should be able to provide credentials manually in the Apache device addition form.

> **Note:** Once the Apache instance is identified and successfully added, the user should be able to perform all the actions (device level as well as certificate level).

Functional Specification

Basic information specifications

- Users should be able to provide basic information such as Account name, Device description, and Account number.
- The account name should be maintained as a unique factor; the user should not be allowed to add the same account name more than once.
- When the user tries to submit the same Account name, a pop-up error message displays as **Account name already available in the inventory**.

Account name

- The account name is a mandatory field. Users should provide a valid name in this column.
- The account name field should be an alphanumeric field. Users should be able to provide alphabets and numbers.
- Users should not be able to provide any special characters in this field, except period (.)
- Users should not be able to provide [space] in this field.
- The account name field should support only 25 characters. Block users to enter more than 25 characters.
- Add an information icon next to the account name text box and displays a message as **Account name should be unique**. The account name already in the cloud inventory cannot be added again. Only alphanumeric and period (.) can be entered in this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Description

- Users can provide the description in this paragraph box.
- Allow a maximum of 250 characters in the description field.
- Allow numbers, alphabets, all the special characters, and [space] in the description field.

Account number

- The account number is an optional field. Users should provide a valid account number in this column.
- Users should be able to enter only numbers in the account number.
- Users should not be able to provide any special characters or empty spaces in this field.
- Users should be able to provide a maximum of 25 numbers. Users should not be able to provide more than 25 entries.

Proxy required

- Proxy required is an optional field, when the user selects this checkbox, AppViewX will try to communicate via Proxy in case of network failure/absence.
- If the user does not select this checkbox, then AppViewX will connect/communicate only via the internet/network, if there is network failure/absence, AppViewX will not try to communicate via provided Proxy.

Credentials Specifications

- Only when the master credential is selected in the above section, the **Credential** section will be displayed in this form. When the user lands on this page to add a new cloud device, by default, the master credential will be selected, hence the **Credential** section will be displayed as well.
- Users should be able to provide the credentials in this section; if the master credential is selected against the credential type. It should be used to access all the services that are selected in the services section.

Credential input type

- The credential input type is a mandatory field. It is a single select dropdown. By default, **Manual Entry** will be displayed.
- Credential input type should list three options, they are
  - Manual entry
  - Credential list – CyberArk
  - Credential list – AppViewX

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- When **Manual Entry** is selected, **Access Key** and **Secret key fields** should bedisplayed below Credential input type fields.
  - The access key and secret key are mandatory fields and Password encrypted fields.
  - Users should provide both access key and secret key corresponding to the account added.
  - These keys will be used to access all the services that are selected in the services section.
- When **Credential List – CyberArk** is selected, the **Credential list dropdown** should be displayed below the **Credential type** field.
  - Users should be able to select a credential that is saved in CyberArk. This credential will be used to access all the services that are selected in the services section.
- When the **Credential list – AppViewX** is selected, the **Credential list dropdown** should be displayed below the **Credential type** field.
  - Users should be able to select a credential that is saved in AppViewX vault. This credential will be used to access all the services that are selected in the services section.

Access key

- When the user lands on this page to add a new cloud device, by default, Manual Entry will be displayed under the Credential input type. Hence, the Access Key field will be displayed as well.
- The access key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to enter empty spaces in this field.
- The minimum and maximum length of the access key is 16 and 128 characters respectively.

Secret key

- When the user lands on this page to add a new cloud device, the manual entry will be displayed under the credential input type. Hence, the secret key field will be displayed as well.
- The secret key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to enter empty spaces in this field.
- The maximum length of the secret key is 256 characters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Key information specifications

- Users should be able to provide the key information such as the **datacenter**, **region**, **credential type**, and **account number**.
- Users have to provide a data center, region, and service. If any of these fields are empty, while submitting the form, the X mark will be displayed against the field that is not filled. A message will be displayed when the user mouse over the X mark, “Value is missing in <*fieldName*> field”.

Data Center

- **Data center** is a mandatory field, the **Select a data center** message must be displayed as a play holder when the user lands on this page to add a new cloud device.



- Users can select a data center for the dropdown (single select dropdown).



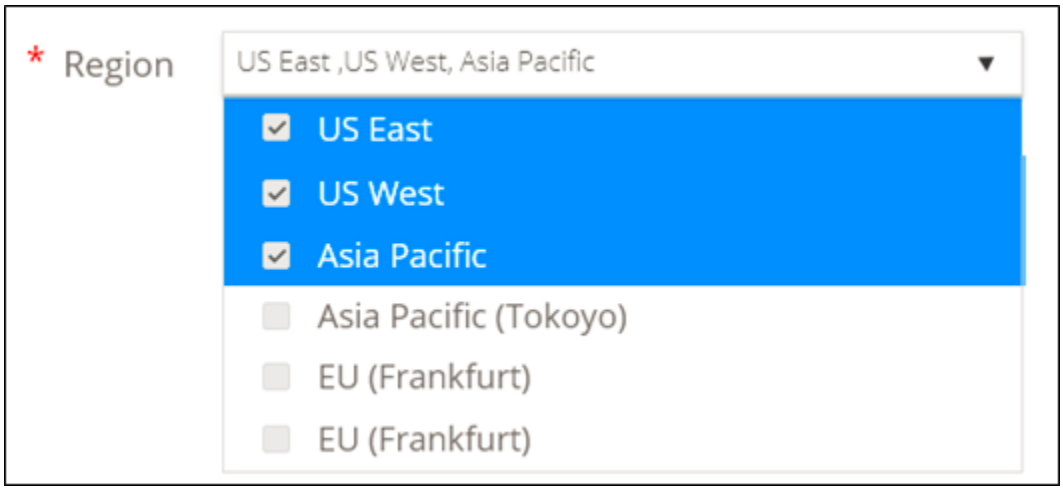
- Based on the data center selected, the region corresponding to the selected data center will be listed below the field region field.
- Users should be restricted to submit this form, without filling a data center. If the user does not select a data center, while submitting the form, X mark will be displayed against the data center field. A message will be displayed when the user mouse over X mark, “Value is missing in datacenter field”.

Region

- Region is a mandatory field.
- Fetch region(s) button will be enabled only when the credentials are given. The user should provide the credentials to enable the fetch region(s)
- Once credentials are provided, the fetch region(s) will be enabled. Users should be able to click the fetch region(s) button.
- Once the user click fetch region(s) by providing valid credentials, a list of all the regions corresponding to the credential provided will be displayed in the drop-down,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- If provided credentials do not have any region (or) if the provided credential is invalid, then None will be displayed in the dropdown.



- The **Select the region(s)** message must be displayed as a play holder when the user lands on this page to add a new cloud device.
- Users can select single or multiple regions from this dropdown (multi-select dropdown).
- Users should be able to select all / unselect all the regions from this field.
- Users should be able to free-text search the region in the dropdown.
- Users should be restricted to submit this form, without selecting at least one region. If the user does not select a region, while submitting the form, the X mark will be displayed against the region field. A message will be displayed when the user mouse over X mark, **Value is missing in region field**.

Service

1. Service is a mandatory field. It is a multi-select text box. By default, **ACM** and **IAM** will be selected.



2. Users can select single or multiple service(s) from this dropdown (multi-select text box).
3. ACM, IAM, ELB, and EC2 are the services that should be listed in the dropdown.
4. AppViewX should support four Amazon AWS services, they are, ACM, IAM, ELB, and EC2 instances. Users should be able to select any one of these services from this field.
5. Based on the selected service, the user should provide additional details in the below section.
6. Users should be able to select all / unselect all the services from this field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Users should be able to free-text search the service from this field.
8. Users should be restricted to submit this form, without selecting at least one service. If the user does not select a service, while submitting the form, X mark will be displayed against the service field. A message will be displayed when the user mouse over X mark, **Value is missing in-service field**.

Additional Attributes Specifications

Service Input Status

- The services that are selected in the services section will be displayed as a tab in this section.
- Each tab will have a different set of fields that are required for accessing each service.
- There are a few mandatory fields corresponding to each service.
- When the user lands on this page to add a new cloud device, by default, **ACM** and **IAM** tabs will be displayed.
- Once mandatory fields are filled, each tab will be indicated with a GREEN tick mark. Only when all the selected services are marked with a GREEN tick, the user will be able to submit the form.
- If the user tries to save without filling in the required detail, an **X** mark should be displayed against each tab that is not completed.
- When the user mouse over **X**mark below message should be displayed, “Mandatory fields are not filled in this tab”

Cert sync

- Cert sync is a mandatory field. When the user lands on this page to add a new cloud device, by default, Managed will be selected.
- Cert sync should be available in all the tab.
- Cert sync have three options,
  - **Managed**: Certificates within the cloud (corresponding to the service selected), & its objects will be discovered and moved to inventory with managed status. Users can perform different AppViewX actions on the certificates that are in managed status. For example, cert sync in the ACM tab is selected as **Managed**, then all the certificates in ACM will be discovered and moved to the inventory with managed status.
  - **Monitored**: Certificates within the cloud (corresponding to the service selected), and their objects will be discovered and moved to inventory with monitored status. Users can only monitor the certificates that are in monitored status, user cannot perform any AppViewX actions on these certificates. For

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

example, cert sync in the ACM tab is selected as **Monitored**, then all the certificates in ACM will be discovered and moved to the inventory with monitored status.

- **Ignored**: The cloud account will be added and managed in AppViewX. Certificates within the cloud (corresponding to the service selected), & its objects will **not** be discovered; only the profiles will be created.

Collection type

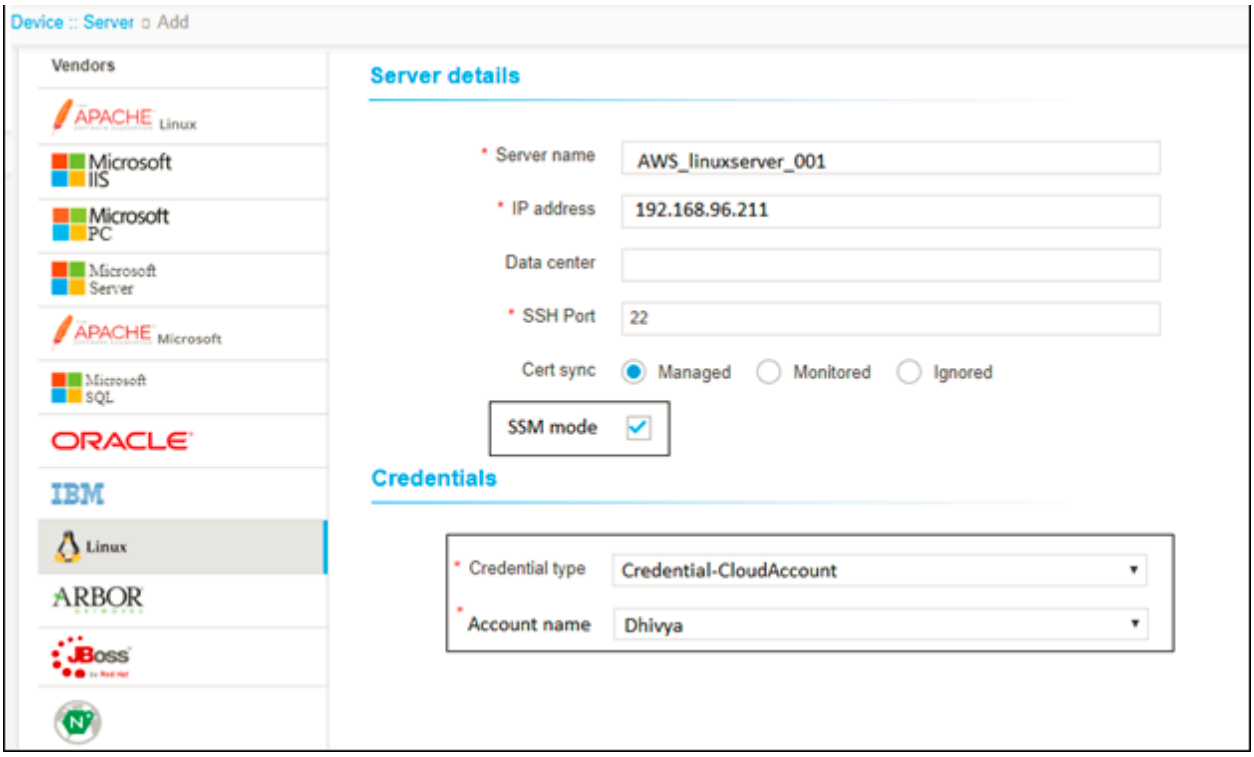
1. The collection type field will be displayed only when the EC2 option is selected under the service section.
2. Collection type is an optional field.
3. All the regions selected by the user should be listed in the collection type section.
4. Users should be able to select a single S3 bucket for all the regions, also users should be able to select an individual S3 bucket for each region.
5. Data stored in S3 must be removed instantly.

Generic Linux SSM Integration Specification

Device Addition

- ApartfromApache, all other instances identifiedfrom Amazon EC2 should be added under Generic Linux under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill on the Generic Linux device addition page.
- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.

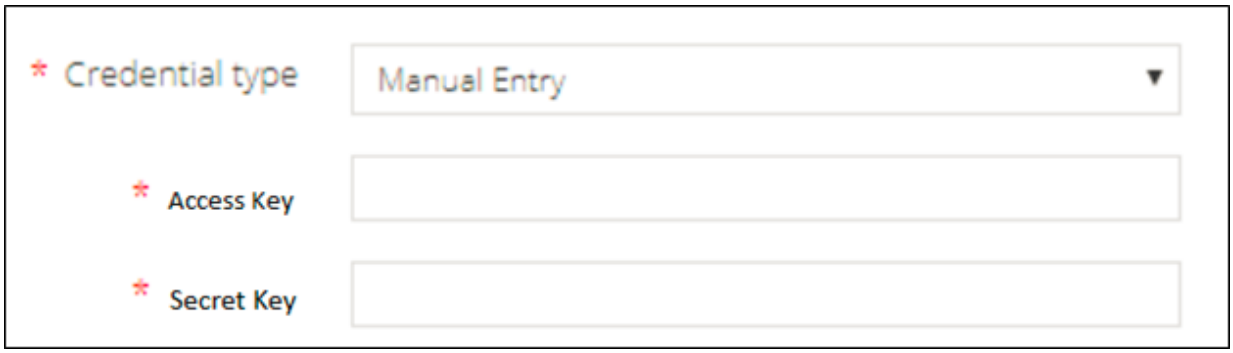
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Credential management

- Credential Type is a mandatory field.
- When a device is added from a Could account, **Credential-CloudAccount must** be displayed corresponding to a credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.
- While modifying the mandatory details in the Generic Linux form, the user should be able to select a different cloud account credential that is added to the cloud inventory.
- Similarly, while modifying the mandatory details in the Generic Linux form, the user should be able to provide credentials manually in the Generic Linux device addition form.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- Only when the mode of communication is SSM, Access key, and Secret key fields will be displayed under Credential type.

Instances Discovery Specification

Specifications

- It is mandatory for the user to provide credentials and S3 bucket details to identify instances within the Amazon EC2 service.
- With details provided, AppViewX should be able to identify Apache (Linux) server within the Amazon EC2 service and all other instances within the EC2 service will be mapped to Generic Linux in the server tab.
- AppViewX uses the SSM mode of communication to discover certificates within these instances.
- If multiple Apaches run in the same EC2 instance, then only one account will be added under the Apache server tab; if multiple apache running in different EC2 instances; then each instance (apache) will be added as a different account under the Apache server tab.
- All the certificates within these instances should be discovered by AppViewX, when the **Cert sync** field is selected as **Managed**/ **Monitored**.
- Should not support push certificates including private key via SSM. CSR must be generated in the device itself only a signed public key should be pushed to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 5: MultiCloud API Guide

This guide explains the APIs used for all cloud device-related activities.

• Push Certificates to ACM
• Push Certificates to IAM
• Push Certificates to ELB via ACM
• Push Certificates to ELB via IAM
• Push Certificates to Cloudfront via ACM
• Push Certificates to Cloudfront via IAM

Push Certificates to ACM

This API will push certificates and their corresponding private keys to AWS devices with the AWS Certificate Manager (ACM) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ACM service through AppViewX, ensure the following:

• AWS devices with the ACM service should be added in AppViewX
• The devices should be in **Managed** state.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId	(Mandatory) Session ID received after login. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwkey *Query*	Tenant key This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ACM
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::acm",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"ACM",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"ACM",
  "certificateTags":{
  },
  "intermediateCertificateFileName":[
  ]
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ACM"],
 "validationSettings":{
 }
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```


Push Certificates to IAM

This API will push certificates and their corresponding private keys to AWS devices with the Identity Access and Management (IAM) service.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before You Begin

Before attempting to push a certificate to an AWS device with the IAM service through AppViewX, ensure the following:

- AWS devices with the IAM service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwkey	(Mandatory) Tenant key

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Query	This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: IAM
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation":{
    "category":"cloud",
    "vendor":"AWS",
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  "profileFilterSelection":"::iam",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"IAM",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"IAM",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@IAM"],
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    "tags": {

    },

    "headers": null

}
```


Push Certificates to ELB via ACM

This API will push certificates and their corresponding private keys to AWS devices with the Elastic Load Balancer (ELB) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ELB service through AppViewX, ensure the following:

- AWS devices with the ELB service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
	Constraints: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwkey *Query*	(Mandatory) Tenant key This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible values: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible values: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::elb",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"ELB",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"ELB",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ELB"],
}
```


Sample Response


```
{
  "response": [
    {
      "requestId": "51",
      "connectorId": "1715213308394"
    }
  ],
  "message": "1 connector(s) saved and push opertaion has been triggered.",
  "appStatusCode": null,
  "tags": {
  },
  "headers": null
}
```


Push Certificates to ELB via IAM

This API will push certificates and their corresponding private keys to AWS devices with the Elastic Load Balancer (ELB) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ELB service through AppViewX, ensure the following:

- AWS devices with the ELB service should be added in AppViewX
- The devices should be in **Managed** state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwkey *Query*	(Mandatory) Tenant key This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource	(Mandatory) Source from which the request is triggered. (E.g. external)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation":{
    "category":"cloud",
    "vendor":"AWS",
    "profileFilterSelection":"::elb",
    "name":"AWS connector",
    "description":""
  },
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 "certificateDetails":{
   "certificateType":"PEM-.pem",
   "locationType":"ELB",
   "certificateFileName":"",
   "certCAReferenceId":"",
   "pushRootAndIntermediateCertificates":true,
   "defaultCertificate":false,
   "profileFilterSelection":"ELB",
   "certificateTags":{
   }
  },
 "certificateTags":{
 },
 "pushDetails":{
   "scriptLocation":"appviewx",
   "preValidationScriptPath":"",
   "postValidationScriptPath":"",
   "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
   "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ELB"],
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Push Certificates to Cloudfront via ACM

This API will push certificates and their corresponding private keys to AWS devices with the CloudFront service.

Before You Begin

Before attempting to push a certificate to an AWS device with the CloudFront service through AppViewX, ensure the following:

- AWS devices with the CloudFront service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
	Constraints: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwkey *Query*	(Mandatory) Tenant key This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible values: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::cloudfront",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"CloudFront",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"CloudFront",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@CloudFront"],
}
```


Sample Response


```
{
  "response": [
    {
      "requestId": "51",
      "connectorId": "1715213308394"
    }
  ],
  "message": "1 connector(s) saved and push opertaion has been triggered.",
  "appStatusCode": null,
  "tags": {
  },
  "headers": null
}
```


Push Certificates to Cloudfront via IAM

This API will push certificates and their corresponding private keys to AWS devices with the CloudFront service.

Before You Begin

Before attempting to push a certificate to an AWS device with the CloudFront service through AppViewX, ensure the following:

- AWS devices with the CloudFront service should be added in AppViewX
- The devices should be in **Managed** state.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Structure

Request structure values

Parameter	Value
URL	/certificate/pushToDevice
Type	POST

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwkey *Query*	(Mandatory) Tenant key This is needed only in case of multi tenant installations and can be ignored in other type of installations. **Type**: String
gwsource	(Mandatory) Source from which the request is triggered. (E.g. external)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certfiicate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation":{
    "category":"cloud",
    "vendor":"AWS",
    "profileFilterSelection":"::cloudfront",
    "name":"AWS connector",
    "description":""
  },
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 "certificateDetails":{
   "certificateType":"PEM-.pem",
   "locationType":"CloudFront",
   "certificateFileName":"",
   "certCAReferenceId":"",
   "pushRootAndIntermediateCertificates":true,
   "defaultCertificate":false,
   "profileFilterSelection":"CloudFront",
   "certificateTags":{
   }
  },
 "certificateTags":{
 },
 "pushDetails":{
   "scriptLocation":"appviewx",
   "preValidationScriptPath":"",
   "postValidationScriptPath":"",
   "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
   "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@CloudFront"],
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 6: CERT+ Troubleshooting Guide

This guide helps you troubleshoot some common problems that can occur while executing CLM actions.

- Troubleshooting for CAs
- Troubleshooting General
- Troubleshooting Protocols
- Troubleshooting AWS, CLOUD
- Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

Troubleshooting for CAs

- Troubleshooting for Amazon CA
- Troubleshooting Custom CA
- Troubleshooting DigiCert CA
- Troubleshooting EJBCA CA
- Troubleshooting Entrust MPKI
- Troubleshooting GlobalSign CA
- Troubleshooting GoDaddy CA
- Troubleshooting Google Private CA
- Troubleshooting InCommon CA
- Troubleshooting LetsEncrypt CA
- Troubleshooting Microsoft Enterprise CA
- Troubleshooting Microsoft Standalone CA
- Troubleshooting Sectigo CA
- Troubleshooting Symantec CA
- Troubleshooting Trustwave CA
- Windows Agent Setup

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting for Amazon CA

Overview

This section will guide you in troubleshooting the common problems that you might encounter when using Amazon CA functionalities like setting addition, enrollment, renewal, regeneration, and revocation.

Supported Web Browsers

Below table lists the supported web browsers for troubleshooting issues on Amazon CA.

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Below table lists the supported devices for troubleshooting issues on Amazon CA.

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Amazon CA
- Issues in Enrolling an Amazon CA Certificate
- Issues in Renewing an Amazon Certificate
- Issues in Regenerating an Amazon CACertificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Revoking an Amazon CA Certificate
• Issues in Amazon CA

Issues in Configuring Amazon CA

Configuring Amazon CA

For instructions on configuring Amazon CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Amazon already exists in inventory.	Check the CA setting name; it should be unique.
Please provide information as required.	Some of the mandatory fields might be missing or might be invalid.	Add valid information in the mandatory section.
Connection failed due to incorrect CA settings details : The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method.	Secret access key or access key is incorrect.	Please check the provided access key and secret key is valid.
Unable to establish connection with CA.	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Enrolling an Amazon CA Certificate

Enrolling an Amazon CA Certificate

For instructions on enrolling an Amazon CA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	• Domain validation failed in amazon CA. • Exceeded the limit for new certificates.	• Validate the provided domain is as per standard. • Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon side.	Retry the action after some time.
Unable to establish connection with CA	• The configured CA details may be incorrect. • Proxy details may not be configured. • AppViewX may not be able to reach CA.	• Check the CA details configured on the CA settings page. • Check whether proxy details are configured in proxy settings. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity.	• Internet connectivity may be unavailable. • Invalid URL provided in CA Settings.	• Please check Internet connectivity to reach CA. • Please Check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Renewing an Amazon Certificate

Renewing an Amazon CA Certificate

For instructions on renewing an Amazon CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Look for an email from ACM, and then follow the link in that email to validate your domain	Domain validation required	Check for email triggered from ACM to validate the domain.
One or more domain names were not validated before the certificate expired, and ACM did not renew the certificate. You can request a new certificate.	Issue in domain name validation.	Check whether the provided domain is valid.
ACM hasn't started the managed renewal process for this certificate.	ACM has not started the renewal request for the provided certificate.	Retry the request after some time.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due	Please refer to the user privileges in the Amazon server for creating

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	to insufficient privileges, disabled features, etc.	certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Regenerating an Amazon CACertificate

Regenerating an Amazon CA Certificate

For instructions on regenerating an Amazon CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	Domain validation failed in amazon CA.	Validate the provided domain is as per standard.
	Exceeded limit for a new certificate.	Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon site.	Retry the action after some time.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support
Too many create certificate requests	Too many create certificate requests for Amazon	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Revoking an Amazon CA Certificate

Revoking an Amazon CA Certificate

For instructions on revoking an Amazon CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
AWS Premium Support Subscription is required to use this service. This certificate can be revoked by submitting a ticket with AWS support.	Amazon does not support certificate revoke.	Check with Amazon premium support for getting revoke service.

Issues in Amazon CA

Troubleshooting Custom CA

Overview

This section will help you troubleshoot the common problems that you might encounter when using Custom CA functionalities like setting addition, enrollment, fetching, renewal, regeneration, and revocation.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Below table lists the supported web browsers for troubleshooting issues on Custom CA.

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Below table lists the supported devices for troubleshooting issues on Custom CA.

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Custom CA and Custom CA Fetch CA Names
- Issues in Enrolling a Custom CA certificate
- Issues in Fetching a Custom CA Certificate
- Issues in Renewing a Custom CA certificate
- Issues in Regenerating a Custom CA certificate
- Issues in Revoking a Custom CA certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Configuring Custom CA and Custom CA Fetch CA Names

Issues in Custom CA Setting Addition

For instructions on configuring Custom CA using the AppViewX user interface, click here.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. On the **Certificate Authority** page that opens, click **CUSTOM**.
3. Click **Configure Now**.
4. In the **General Information** section, enter the details as required.
5. Click **Save**.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Failed to add custom CA details as name already exists	A CA setting with the same name for Custom CA already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Upload a valid CA certificate in .pfx format	Upload certificate not in .pfx or .p12 format	Upload the certificate in either of pfx or p12 format
Uploaded CA certificate already exist	Uploaded certificate already exists.	Uploaded a new certificate
Issuer serial number is mandatory on request.	Issuer serial number is missing.	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing.	Please provide ca certificate details

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a Custom CA certificate

Enrolling a Custom CA Certificate

For instructions on enrolling a Custom CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Fetching a Custom CA Certificate

Error Message	Possible Cause	Possible Solution
Entered order id is invalid.	Order ID is invalid.	Provide valid order ID.

Issues in Renewing a Custom CA certificate

Renewing a Custom CA Certificate

For instructions on renewing a Custom CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide CA certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the mandatory field.
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Regenerating a Custom CA certificate

Regenerating a Custom CA Certificate

For instructions on regenerating a Custom CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Revoking a Custom CA certificate

Revoking a Custom CA Certificate

For instructions on revoking a Custom CA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Serial number or revocation request is null or empty.	Invalid request or invalid serial number specified.	Provide the valid request.
The certificate cannot be revoked as it does not have CRL distribution point.	Certificate does not have a CRL distribution point.	Invalid serial number provided.
The certificate is already revoked.	Certificate is already revoked.	Already revoked, so I need to revoke again.
Entered revocation reason is invalid.	Invalid reason specified	Specify valid reason to revoke the certificate

Troubleshooting DigiCert CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using Digicert CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring DigiCert CA
- Issues in Enrolling a DigiCert certificate
- Issues in Renewing a DigiCert certificate
- Issues in Regenerating a DigiCert CA Certificate
- Issues in Revoking a DigiCert certificate
- Issues in Discovering DigiCert CA Certificates

Issues in Configuring DigiCert CA

Configuring DigiCert CA

For instructions on configuring DigiCert CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Digicert already exists in inventory.	Check the CA Setting name, it should be unique.
Fetch certificate types action has failed Connection failed due to incorrect CA settings details	Please check the Service URL or API Access key.	Verify the service URL configured: Sample URL: https://www.digicert.com/services/v2/.
Fetch certificate types action has failed Access denied due to missing permission.	Access Key may be wrong or may not have enough authorization.	Verify the Access key and check its API authorization, it should be set as none.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details might have not been configured.	Configure valid proxy details.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Issues in Enrolling a DigiCert certificate

Enrolling a DigiCert CA Certificate

For instructions on enrolling a DigiCert CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Renewing a DigiCert certificate

Renewing a DigiCert CA Certificate

For instructions on renewing a DigiCert CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Please provide a valid order Id of the certificate.	OrderId may be incorrect to perform CLM action in Digicert	Verify the orderid of the certificate from the Digicert CA account.
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Regenerating a DigiCert CA Certificate

Regenerating a DigiCert CA Certificate

For instructions on regenerating a DigiCert CA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Revoking a DigiCert certificate

Revoking a DigiCert Certificate

For instructions on revoking a DigiCert CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while revoking certificate-The specified order was not found.	The order id provided in the connector might be wrong.	Check the orderId for the certificate in Digicert CA Portal.
Error while revoking certificate-Order Id not provided to get corresponding certificate Id.	orderid is not provided for the action	Provide a valid order id to proceed with the action.
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering DigiCert CA Certificates

Discovering DigiCert CA Certificates

For discovering DigiCert CA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Service unavailable, please limit request volume	DigiCert throws a service unavailable error, please limit request volume when: • 1000+ continuous requests fired, So with buffer to enroll certificates, 900 certificate requests • only be fired in a batch	AppViewX CERT+ discovery automatically handles it by introducing a delay of 50 minutes between each 900 requests.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting EJBCA CA

This section helps you troubleshoot the common problems that you might encounter when using EJBCA CA functionalities like EJBCA CA setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring EJBCA CA and Fetching EEPs
- Issues in Enrolling an EJBCA certificate
- Issues in Renewing an EJBCA certificate
- Issues in Regenerating an EJBCA Certificate
- Issues in Revoking an EJBCA certificate
- Issues in Suspending an EJBCA certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Reinstating EJBCA certificate
• Issues in Discovering EJBCA certificates

Issues in Configuring EJBCA CA and Fetching EEPs

Configuring EJBCA CA

For instructions on configuring EJBCA CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for EJBCA already exists in the inventory.	Check the CA Setting name. It should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials - Certificate and key, URL	Uploaded client certificate is incorrect or does not have the required permissions.	Please check the uploaded certificate and its permissions. Ensure that the required permissions are assigned.
At least one end entity profile should be added.	CA Setting does not have at least one End entity profile selected and added.	CA Settings should have at least one End entity profile selected and added.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Issues in Enrolling an EJBCA certificate

Enrolling an EJBCA certificate

For instructions on enrolling an EJBCA CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName>must exist.	FieldName may be set as mandatory in the selected End entity profile in EJBCA portal.	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field is Organization, Organization unit, Locality, Country, State). If the field is not listed on the enrollment page, add the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		field in the End entity profile, then pass the value via the enrollment page.
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact no of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal to match the sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles.	Certificate profiles may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile.
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/ EJBCA server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in EJBCA server for creating certificates or contact the AppViewX Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters/ JSON body in the request.	Please validate the input parameters/payload provided or contact the AppViewX Support Team.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or contact the AppViewX Support Team.

Issues in Renewing an EJBCA certificate

Renewing an EJBCA certificate

For instructions on renewing an EJBCA CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while renewing certificate. - Subject DN field <FieldName> must exist.	FieldName may set as mandatory in the selected End entity profile in EJBCA portal	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (if the field is Organization, Organization unit, Locality, Country, State)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.
Error while renewing certificate. - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact number of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Error while renewing certificate. - Couldn't find certificate profile (<ProfileId>), among available certificate profiles	Certificate profile selected may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile.
Error while renewing certificate. - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/EJBCA server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or contact AppViewX Support.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew action.

Issues in Regenerating an EJBCA Certificate

Regenerating an EJBCA Certificate

For instructions on regenerating an EJBCA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName> must exist.	FieldName may set as mandatory in the selected end entity profile in EJBCA portal.	1. Set the FieldName as optional in the selected end entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		is Organization, Organization unit, Locality, Country, State). If the field is not listed on the enrollment page, add the field in the end entity profile, then pass the value via the enrollment page.
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No of values sent and number of values configured for the field do not match.	1. Send the exact number of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles	Certificate profiles may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	he configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters/JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for EJBCA	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Revoking an EJBCA certificate

Revoking an EJBCA Certificate

For instructions on revoking an EJBCA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while revoking certificate-Could not find end entity certificate.	The issuer name in the connector may be wrong	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide the issuer details.
Unable to establish connection with CA	he configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach the CA.	Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Suspending an EJBCA certificate

Suspending an EJBCA Certificate

1. Go to (**Menu**) > **CERT+** > **Certificate Inventory** > **Server Certificate/Client Certificate/Code Signing Certificate**.
2. From the server/client/code signing certificate inventory, select a EJBCA certificate.

   A holistic view of the selected certificate, along with the certificate number, is displayed.
3. From the dropdown menu next to the **Certificate**, click **Suspend**.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while suspending certificate- Could not find end entity certificate.	The issuer name in the connector may be incorrect.	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide issuer details.
Unable to establish connection with CA.	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Reinstating EJBCA certificate

Reinstating an EJBCA Certificate

For instructions on reinstating an EJBCA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Error while reinstating certificate- Could not find end entity certificate.	The issuer name in the connector may be wrong.	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide issuer details.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering EJBCA certificates

Discovering EJBCA Certificates

For discovering EJBCA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Expiry days need to be configured to discover certificates.	Expiry days not configured in the selected EJBCA CA Settings.	Set the expiry days in the selected CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Entrust MPKI

Overview

This section helps you troubleshoot the common problems that you might encounter when using Entrust MPKI functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Entrust MPKI CA
- Issues in Enrolling an Entrust MPKI Certificate
- Issues in Renewing a Entrust MPKI Certificate
- Issues in Regenerating a Entrust MPKI Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Revoking a Entrust MPKI Certificate
• Issues in Discovering Entrust MPKI certificates

Issues in Configuring Entrust MPKI CA

Configuring Entrust MPKI CA

For instructions on configuring Entrust MPKI CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings. CA Settings name already exists.	A CA setting with the same name for Entrust MPKI already exists in inventory.	Check the CA setting name, it should be unique.
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details have not been configured correctly.	Configure valid proxy details.
Unable to establish connection with the CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling an Entrust MPKI Certificate

Enrolling an Entrust MPKI Certificate

For instructions on enrolling an Entrust MPKI certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Renewing a Entrust MPKI Certificate

Renewing an Entrust MPKI Certificate

For instructions on renewing an Entrust MPKI certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Regenerating a Entrust MPKI Certificate

Regenerating a Entrust MPKI Certificate

For instructions on regenerating a Entrust MPKI certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Revoking a Entrust MPKI Certificate

Revoking a Entrust MPKI Certificate

For instructions on revoking a Entrust MPKI certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering Entrust MPKI certificates

Discovering Entrust MPKI Certificates

For discovering Entrust MPKI certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Troubleshooting GlobalSign CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using GlobalSign CA functionalities like setting addition, connectivity, certificate enrollment, renewal, reissue, revocation, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring GlobalSign CA
- Issues in Enrolling a GlobalSign CA Certificate
- Issues in Renewing a GlobalSign CA Certificate
- Issues in Revoking a GlobalSign CA Certificate
- Issues in Discovering GlobalSign CA Certificates
- Issues in Validating GlobalSign CA Connectivity
- Issues in Reissuing a GlobalSign CA Certificate

Issues in Configuring GlobalSign CA

Configuring GlobalSign CA

For instructions on configuring GlobalSign MSSL CA using the AppViewX user interface, click here.

For instructions on configuring GlobalSign Atlas CA using the AppViewX user interface, click here.

For instructions on configuring GlobalSign SSL CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
This field should not be null or empty	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		
CA Settings - [<Fields>] mandatory fields cannot be empty.		
CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.
Invalid URL	vendorSpecificSettings.url is not valid.	Provide valid input for vendorSpecificSettings.url.
Login should not be blank	vendorSpecificSettings.login is not valid.	Provide valid input for vendorSpecificSettings.login.
Password should not be blank	vendorSpecificSettings.password is not valid.	Provide valid input for vendorSpecificSettings.password.

Issues in Enrolling a GlobalSign CA Certificate

Enrolling a GlobalSign CA Certificate

For instructions on enrolling a GlobalSign CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.	Invalid credentials.	Check the credentials provided.
	Invalid Global Sign URL.	Check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Make sure your public IP is whitelisted by GlobalSign.
	Invalid CSR parameters.	Validate the CSR parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.
Invalid Common Name, Please provide valid commonname.	Common name provided in CSR is invalid.	Provide a valid common name in CSR parameters.
Empty response received from the portal, Check with Proxy/CA Setting configurations.	Error in provided CA details.	Check the given CA details.
	Check if the CA portal is accessible from AppViewX.	Check for internet/proxy settings.
Invalid Validity Period	Validity period provided is invalid.	Check with CA for the supported validity period and update accordingly.

Issues in Renewing a GlobalSign CA Certificate

Renewing a GlobalSign CA Certificate

For instructions on renewing a GlobalSign CA certificate, click renewing a certificate.

Issues in Revoking a GlobalSign CA Certificate

Revoking a GlobalSign CA Certificate

For instructions on revoking a GlobalSign CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Order ID not provided to get corresponding certificate Id.	Order id is empty in the revoke request.	Check and provide a valid order id.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Issues in Discovering GlobalSign CA Certificates

Issues in Discovering GlobalSign CA Certificates

For discovering GlobalSign CA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.	Invalid credentials.	Check the credentials provided.
	Invalid Global Sign URL.	Check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Make sure your public IP is whitelisted by GlobalSign.
	Invalid CSR parameters.	Validate the CSR parameters.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Issues in Validating GlobalSign CA Connectivity

Validating GlobalSign CA Connectivity

For instructions on validating the GlobalSign MSSL CA connectivity, click here.

For instructions on validating the GlobalSign Atlas CA connectivity, click here.

For instructions on validating the GlobalSign SSL CA connectivity, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid Global Sign Credentials.	Proxy details provided might be incorrect.	Provide valid proxy details.
	Invalid credentials	Please check the credentials provided.
	Invalid GlobalSign URL.	Please check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Please make sure your public IP is whitelisted by GlobalSign.
Connection failed due to incorrect CA settings details | Access denied due to invalid permissions.	Invalid credentials	Please check the credentials provided.

Issues in Reissuing a GlobalSign CA Certificate

Reissuing a GlobalSign CA Certificate

For instructions on reissuing a GlobalSign CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting GoDaddy CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using GoDaddy CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring GoDaddy CA
- Issues in Enrolling a GoDaddy CA Certificate
- Issues in Renewing a GoDaddy CA Certificate
- Issues in Regenerating a GoDaddy CA Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Revoking a GoDaddy CA Certificate
• Issues in Discovering GoDaddy Certificates

Issues in Configuring GoDaddy CA

Configuring GoDaddy CA

For instructions on configuring GoDaddy CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GoDaddy already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials – URL	URL entered might be wrong and not in proper URL format	Please check the URL entered
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Issues in Enrolling a GoDaddy CA Certificate

Enrolling a GoDaddy CA Certificate

For instructions on enrolling a GoDaddy CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may not be available for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact AppViewX Support.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy.	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Renewing a GoDaddy CA Certificate

Renewing a GoDaddy CA Certificate

For instructions on renewing a GoDaddy CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may not be available for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to submit the CSR request to certificate authority - No orderId available	There might not be any order id i.e certificate id available for the certificate in ca connector information.	• Update the order id manually by copying it from the GoDaddy portal. • Or do the following: 1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to renew the certificate	There might not be an available product to renew the certificate.	Purchase the product type separately for renewing the certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure	Invalid proxy details.	Please check the proxy details provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy/Internet connectivity/ GoDaddy Server.	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or contact AppViewX Support.

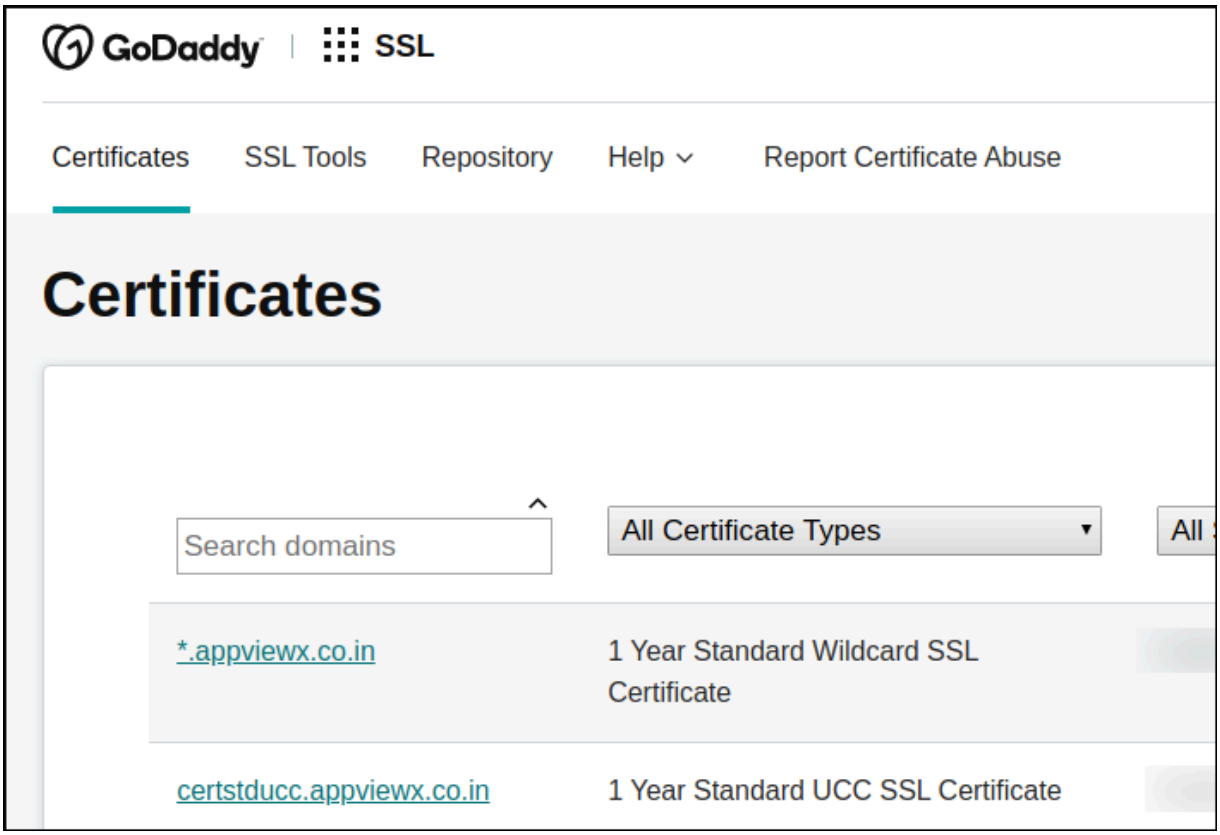
Retrieving the certificate ID (order ID) from the Go Daddy Portal

To retrieve the order ID (or) certificate ID for a particular certificate from the GoDaddy URL:

1. Login to your GoDaddy account.
2. Navigate to My Account -> SSL Certificates.

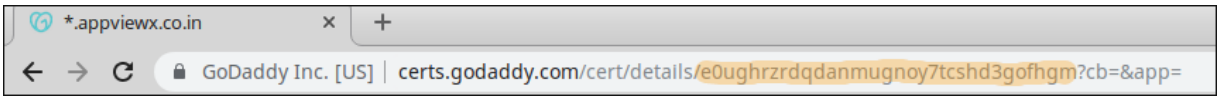
   Here you can see the list of certificates created via this GoDaddy account.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



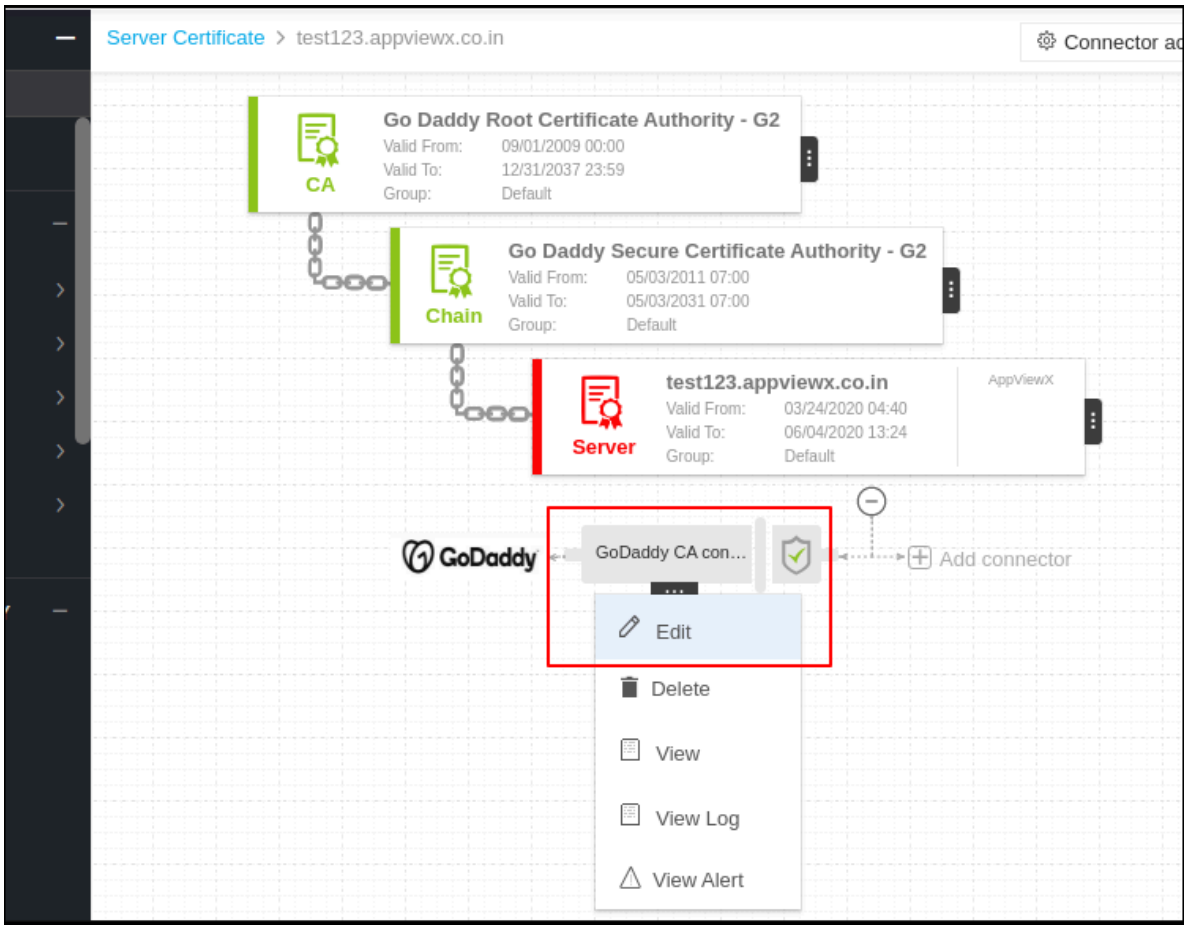
3. Click on the certificate for which you require the order ID.

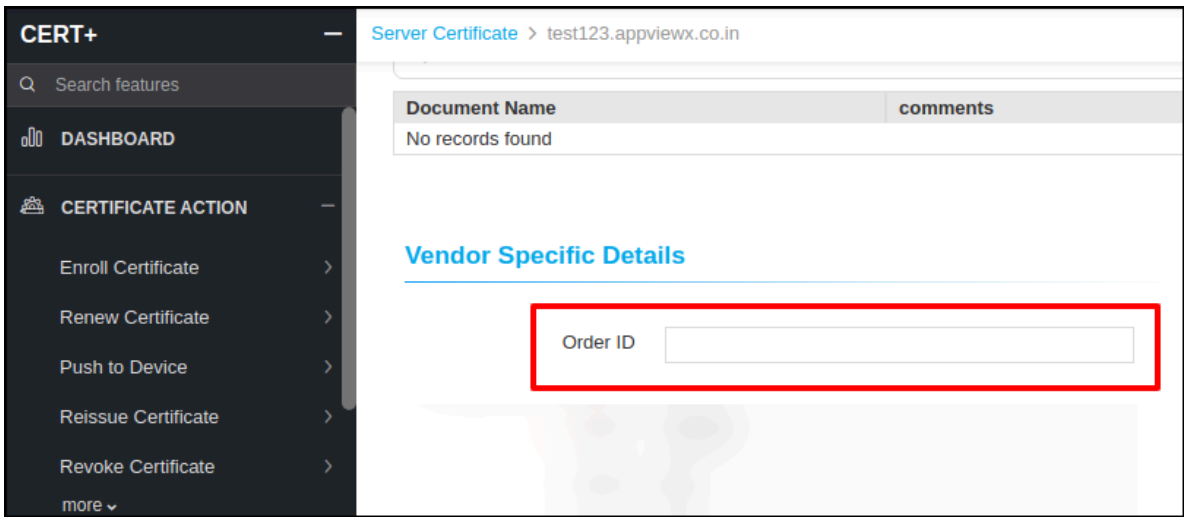
   In the URL framed you can see the order ID.



4. Use this order ID in our AppViewX CA connector as shown below:
   a. Click on edit in CA connector options.
   b. Find for Order Id in vendor specific fields.
   c. Input the order id obtained from CA portal and update the connector.
   d. Resubmit the failed request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating a GoDaddy CA Certificate

Regenerating a GoDaddy CA Certificate

For instructions on regenerating a GoDaddy CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	There might not be available units for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Revoking a GoDaddy CA Certificate

Revoking a GoDaddy CA Certificate

For instructions on revoking a GoDaddy CA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No orderId available	There might not be an order id i.e certificate id available for the certificate in ca connector information.	• Update the order ID manually. For instructions, refer the **Retrieving the certificate ID (order ID) from the Go Daddy Portal** here. • Or do the following: 1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering GoDaddy Certificates

Discovering GoDaddy Certificates

For discovering GoDaddy CA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates, or contact AppViewX Support.

Troubleshooting Google Private CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using Google private CA functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, suspension, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Google Private CA and Google Fetch CA Names
- Issues in Enrolling a Google Private CA Certificate
- Issues in Renewing a Google Private CA Certificate
- Issues in Regenerating a Google Private CA Certificate
- Issues in Revoking a Google Private CA Certificate
- Issues in Suspending a Google Private CA Certificate
- Issues in Reinstating a Google Private CA Certificate
- Issues in Discovering Google Private CA Certificates

Issues in Configuring Google Private CA and Google Fetch CA Names

Configuring Google Private CA

For instructions on configuring Google Private CA using the AppViewX user interface, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Google private already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a Google Private CA Certificate

Enrolling a Google Private CA Certificate

For instructions on enrolling a Google Private CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Renewing a Google Private CA Certificate

Renewing a Google Private CA Certificate

For instructions on renewing a Google Private CA certificate, click renewing a certificate.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported key type or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com	Please check this URL https://www.googleapis.com can be

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	may not be reachable.	accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and perform renew.

Issues in Regenerating a Google Private CA Certificate

Regenerating a Google Private CA Certificate

For instructions on regenerating a Google Private CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Revoking a Google Private CA Certificate

Revoking a Google Private CA Certificate

For instructions on revoking a Google Private CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reason may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Suspending a Google Private CA Certificate

Suspending a Google Private CA Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.

   The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server/Client/Code Signing Certificate**.

   The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Google certificate**.

   A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Reinstating a Google Private CA Certificate

Reinstating a Google Private CA Certificate

For instructions on reinstating a Google Private CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Discovering Google Private CA Certificates

Discovering Google Private CA Certificates

For discovering Googe Private CA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Troubleshooting InCommon CA

Overview

This section helps you troubleshoot the common problems that you might encounter while using functionalities like configuration, setting addition, CLM actions and discovery associated with InCommon Certificate Authority.

- Issues in Configuring InCommon CA
- Issues in Validating InCommon CA Connectivity
- Issues in Enrolling an InCommon CA Certificate
- Issues in Regenerating an InCommon Certificate
- Issues in Renewing an InCommon Certificate
- Issues in Reissuing an InCommon Certificate
- Issues in Revoking an InCommon Certificate
- Issues in Discovering InCommon Certificates

Issues in Configuring InCommon CA

Configuring InCommon CA

For instructions on configuring InCommon CA using the AppViewX user interface, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

The Certificate types available for the CA account will be fetched from the Certificate Authority.

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be incorrect.	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid.	Check and correct the URI. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong URL specified or the URL is not reachable	Base URL may be invalid.	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong.	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings of the general

Issues in Validating InCommon CA Connectivity

Issues in the InCommon CA

For instructions on validating the InCommon CA connectivity, click here.

Error Messages and Resolutions

CA settings will be validated and the connection status will be set to either **Success** or **Failure**.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid auth data	URI may be invalid	Check and correct the URI. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Connection failed due to incorrect CA settings details : Wrong URL specified or the URL is not reachable	Base URL may be invalid	Validate and correct the base URL.
Connection failed due to incorrect CA settings details : Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Enrolling an InCommon CA Certificate

Enrolling an InCommon Certificate

For instructions on enrolling an InCommon CA certificate, click here.

Error Messages ad Resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Regenerating an InCommon Certificate

Regenerating an InCommon Certificate

For instructions on regenerating an InCommon CA certificate, click here.

Error Messages and Resolutions

If a request has failed, then the failure status shall be displayed in the holistic view. Click on the link above the failure message to know the reason for the workflow failure. Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Renewing an InCommon Certificate

Renewing an InCommon Certificate

For instructions on renewing an InCommon CA certificate, click here.

Error Messages and Resolutions

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Reissuing an InCommon Certificate

Reissuing an InCommon Certificate

For instructions on reissuing an InCommon CA certificate, click here.

Error Messages and Resolutions

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Revoking an InCommon Certificate

Revoking an InCommon Certificate

For instructions on revoking an InCommon CA certificate, click here.

Error Messages and Resolutions

If the request has failed, then the failure status will be shown in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering InCommon Certificates

Discovering InCommon Certificates

For discovering InCommon CA certificates, you will need to run a certificate authority discovery scan. For instructions, click here.

Error Messages and Resolutions

If the discovery status is Failed, the reason for failure will be available in the Discovery Batch Summary pop, which can be launched by clicking the icon next to the discovery status.

Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Troubleshooting LetsEncrypt CA

Overview

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, connectivity, certificate enrollment, renewal, revocation, and other actions associated with LetsEncrypt.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Let's Encrypt CA
- Issues in Enrolling a Let's Encrypt CA Certificate
- Issues in Renewing a Let's Encrypt CA Certificate
- Issues in Revoking a Let's Encrypt CA Certificate
- Issues in Validating Let's Encrypt CA Connectivity
- Issues in Sending REST Requests to Let's Encrypt CA

Issues in Configuring Let's Encrypt CA

Configuring Let's Encrypt CA

For instructions on configuring LetsEncrypt CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings. CA settings name already exists.	A CA setting with the same name for LetsEncrypt already exists in inventory.	Check the CA Setting name, it should be unique.
Please validate given information	Invalid URL given.	Please check the URL.
	LetsEncrypt portal might be down.	Please check any problem in the LetsEncrypt portal.
	Proxy might be required.	Please check the proxy required for this environment. Proxy details may not be configured in proxy settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
This field should not be null or empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		
CA Settings - [<Fields>] mandatory fields cannot be empty.		
Invalid Email Id	Email ID given while account creation is invalid.	Provide valid email ID.

Issues in Enrolling a Let's Encrypt CA Certificate

Enrolling a Let's Encrypt CA Certificate

For instructions on enrolling an Let's Encrypt CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.
Invalid Authorization	Authorization failed while fetching the challenge.	Provide valid CSR details in the request to receive valid order details in the CA response.
Challenge Not Found	Challenge not received from CA.	Provide valid CSR details in the request to receive valid order details in the CA response.
Error during calculating thumbprint	Invalid public key or publicjsonweb key.	Provide valid details while adding the LetsEncrypt account.
Timeout while Validating Challenge	Challenge verification was not completed within the time limit.	Verify the challenge within the time limit or generate a new challenge and verify.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Challenge Verification Failed	Challenge verification returned status as Invalid from CA.	Check if the internet or proxy is enabled. Check if the TXT record has been added correctly.

Issues in Renewing a Let's Encrypt CA Certificate

Renewing a Let's Encrypt CA Certificate

For instructions on renewing a Let's Encrypt CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.

Issues in Revoking a Let's Encrypt CA Certificate

Revoking a Let's Encrypt CA Certificate

For instructions on revoking a Let's Encrypt CA certificate, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is valid.	Provide valid proxy details.
Content Extraction Failed	Unable to get encoded X509 certificate using its content.	Provide valid certificate content for the certificate to be revoked.

Issues in Validating Let's Encrypt CA Connectivity

Validating Let's Encrypt CA Connectivity

For instructions on validating the Let's Encrypt CA connectivity, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Communication with CA failed.	Proxy details provided may be incorrect.	Provide valid proxy details.
	Invalid LetsEncrypt Account Id.	Provide valid credentials associated with a valid account.

Issues in Sending REST Requests to Let's Encrypt CA

Error Message	Possible Cause	Possible Solution
In getKeyStore(), While getting instance for the keystore and loading the store file	Unable to read keystore file “avx_client_cert_keystore” from security path, i.e. $(JAVA_HOME}/lib/security/	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While traversing to java security folder	Java security directory is missing or is corrupted.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While getting the instance for the keystore	Unable to get Keystore instance.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While loading the key store	Unable to load keystore.	Internal error. Possibly a deployment issue. Contact support team.

Troubleshooting Microsoft Enterprise CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Enterprise.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Microsoft Enterprise CA and Fetch CAs
- Issues in the Certificate Lifecycle Management of a Microsoft Enterprise CA Certificate
- Issues in Revoking Microsoft Enterprise certificate
- Issues in Suspending Microsoft Enterprise certificate
- Issues in Reinstating Microsoft Enterprise certificate
- Issues in Discovering Microsoft Enterprise certificates

Issues in Configuring Microsoft Enterprise CA and Fetch CAs

Configuring Microsoft Enterprise CA

For instructions on configuring Microsoft Enterprise CA using the AppViewX user interface, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target.	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn –s http/machinename domain\username. • Please note this will work in environments where Kerberos Authentication is set up and there is an AD Domain Setup • If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) **OR** **Error Code 0x80070005 - Access is denied**	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "`Enable-PSRemoting -force`". 4. Execute "`netsh winhttp show proxy`" and if a proxy is configured then

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		• Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests. 5. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. 6. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	The Remote Procedure Call Service	Navigate to the target machine and start RPC service if it has stopped.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	is not responding.	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig". • Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached.	• Windows Gateway is not reachable from AppViewX. • Windows Gateway service is down.
Html response : Access is denied	Access is denied.	• In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. • Client certificate used in AppViewX is not imported in Target machine's Local computer store.
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution

	script executions.	100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		.

Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request.
This user is allowed a maximum number of 4 concurrent shells, which has been exceeded.
Close existing shells or raise the quota for this user.
	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator
		1. Check existing config winrm get winrm/config.
		2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Client Certificate gives Permission Denied 403 error. **This can happen in certain environment and its intermittent**	CA Store mismatch or invalid client certificate used.	Check if the Client certificate is installed correctly by checking the chain in the Personal Store. • Root of the client certificate should be available in the Trusted Root Certification Store of the Server. • Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. • If all the above looks good then go to the agent server and do the following steps 1. MMC. 2. Add “Add/Remove SnapIn. 3. select certificates. 4. select “LocalMachine”. 5. Navigate to the Personal Store and click on the client certificate. 6. Navigate to Chain. 7. Export the Root certificate and save it as Root.cer in a location. 8. Import the “Root.cer” into trusted Root back again. 9. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. 10. Click on the “Trusted Root” store and check if there are

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		certificates that have different IssuedTo and IssuedBy. 11. Take a backup of such certificates and move it to respective stores. 12. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
The permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or	The user name or password is incorrect.	Check if the credentials are valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.		
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
• **There is not enough space on the disk** • **The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic.** • **Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy**	There is not enough space on the disk.	Ensure that your hard disk has enough free space.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fail within the expected range.		
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Issues in the Certificate Lifecycle Management of a Microsoft Enterprise CA Certificate

Managing Microsoft Enterprise CA Certificates

For instructions on enrolling a Microsoft Enterprise CA certificate, click here.

For instructions on renewing a Microsoft Enterprise CA certificate, click here.

For instructions on regenerating a Microsoft Enterprise CA certificate, click here.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	may not be configured. 3. AppViewX may not be able to reach CA.	
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn’t have access to the template.	Please give access to the user.
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it and select properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		else install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add “Add/Remove SnapIn. c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected	Supply valid CSR values accepted by template or CA policy.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	template/CA's Policy.	
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Revoking Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Suspending Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate.**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Enterprise certificates

Issues in the Microsoft Enterprise Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Certificate Authority Scan**. The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Microsoft Enterprise**.
6. Click **Discover** at the bottom of the page.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting Microsoft Standalone CA

- Introduction
- Issues in Microsoft Standalone CA setting addition and fetch CAs
- Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Standalone certificate
- Issues in Revoking Microsoft Standalone certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Suspending Microsoft Standalone certificate
• Issues in Reinstating Microsoft Standalone certificate
• Issues in Discovering Microsoft Standalone certificates

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Standalone.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Microsoft Standalone CA setting addition and fetch CAs

Issues in the Microsoft Standalone CA Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**. The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Microsoft**.
5. Click **Standalone**.
6. Click **Add.**

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
3) CA Settings - [<Fields>] mandatory fields cannot be empty.		
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for	Kerberos configuration is not configured for target machine	The issue occurs with “Powershell Remoting” since it uses Kerberos Authentication 1. In Agent Machine start command prompt as Administrator and execute the following command. 2. `setspn –s http/machinename domain \username.` 3. Please note this will work in environments where Kerberos

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic		Authentication is setup and there is an AD Domain Setup. 4. If no kerberos authentication is set up then we need to communicate via WMI.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain" 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of administrator group
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	Remote Procedure Call Service	Navigate to the target machine and start RPC service if it has stopped.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	is not responding	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		3. Navigate to local Users and Groups and access "Administrators". 4. Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached	1. Windows Gateway is not reachable from AppViewX. 2. Windows Gateway service is down.
Html response : Access is denied	Access is denied	1. In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. 2. Client certificates used in AppViewX are not imported in Target machine's Local computer store.
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator. 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	CA Store mismatch or invalid client certificate used	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		4. If all the above looks good then go to agent server and do following steps a. MMC. b. Add “Add/Remove SnapIn. c. select certificates. d. select “LocalMachine” e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on “Trusted Root” store and check if there are any certificates which have different IssuedTo and IssuedBy. k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec) 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect	The username or password is incorrect.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network,	Powershell remoting is not configured	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
1. There is not enough space on the disk 2. The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. 3. Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed	There is not enough space on the disk	Ensure that your hard disk has enough free space.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
with the following error Value does not fail within the expected range.		
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling, Fetching, Renewing, Regenerating Microsoft Standalone certificate

Issues in the Microsoft Standalone Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Standalone certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	3. AppViewX may not be able to reach CA	
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
DATA is invalid log message	Invalid header for CSR	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if DLL is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1) `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec) 2) `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec)
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
destination to analyze and configure the WinRM service: "winrm quickconfig"		
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to agent server and do following steps: a. MMC . b. Add “Add/Remove SnapIn c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		j. Click on “Trusted Root” store and check if there are any certificates which have different IssuedTo and IssuedBy. k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers"
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM	Powershell remoting is not configured	1. C:\Windows\system32>WinRM quickconfig. 2. WinRM service is already running on this machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Issues in Revoking Microsoft Standalone certificate

Issues in the Microsoft Standalone Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Standalone certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Suspending Microsoft Standalone certificate

Issues in the Microsoft Standalone Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Standalone certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Standalone certificate

Issues in the Microsoft Standalone Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Standalone certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Standalone certificates

Issues in the Microsoft Standalone Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Certificate Authority Scan**. The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Microsoft Standalone**.
6. Click **Discover** at the bottom of the page.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid

Troubleshooting Sectigo CA

- Introduction
- Issues in Sectigo CA Configuration
- Issues in Sectigo CA setting validation
- Issues in Enrolling Sectigo Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Regenerating Sectigo Certificate
• Issues in Renewing Sectigo Certificate
• Issues in Reissuing Sectigo Certificate
• Issues in Revoking Sectigo Certificate
• Issues in Discovering Sectigo Certificates

Introduction

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, certificate enrollment, renewal, revocation, discovery, and other actions associated with Sectigo Certificate Authority.

Issues in Sectigo CA Configuration

Issues in the Sectigo CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**. The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Sectigo**. The **Sectigo** page is displayed.
5. Click **Add** or **Configure Now**.
6. Configure the **General Information** and **CA Configuration** details.
7. Click **Fetch Certificate Types**. The Certificate types available for the CA account will be fetched from the **Certificate Authority**.

Error Messages

Following errors may occur in this step -

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be invalid	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid	Check and correct the URI. For example: https://cert-manager.com/customer/

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Sectigo CA setting validation

Issues in the Sectigo CA

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**. The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Sectigo**. The **Sectigo** Page is displayed.
5. To validate the **CA setting**, click **Check** in **Connection Status**. **CA settings** will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Error Messages

Possible error scenarios could be as follows:

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be in valid	Check and correct the username and password.
Invalid auth data	URI may be invalid	Check and correct the URI.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Connection failed due to incorrect CA settings details : Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Connection failed due to incorrect CA settings details : Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Enrolling Sectigo Certificate

Issues in the Enrolling Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client** Tab. The **Enroll Certificate** page is displayed.
5. Select **Certificate Authority** as **Sectigo** and proceed with **Certificate Enrollment**.

Error Messages

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Regenerating Sectigo Certificate

Issues in the Regenerating Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab. The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate**.

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Renewing Sectigo Certificate

Issues in the Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab. The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Renew**.

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		the CA connector and resubmit the request.

Issues in Reissuing Sectigo Certificate

Issues in the Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab. The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page., click **List.**
6. Click any **Sectigo certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Reissue**.

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the link above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Revoking Sectigo Certificate

Issues in the Sectigo Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client** Tab. The **Server Certificate/Client Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Sectigo certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke.**

Error Messages

If the request has failed, then the failure status will be shown in the holistic view. Click on the **link** above the failure message to know the reason for the workflow failure.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and resubmit the request.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering Sectigo Certificates

Issues in the Sectigo Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Certificate Authority Scan**. The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Sectigo** and provide the necessary information.
6. Click **Discover** at the bottom of the page.

Error Messages

If the discovery status is Failed, the reason for failure will be available in the Discovery Batch Summary pop, which can be launched by clicking the icon next to the discovery status.

Common reasons for the failure are mentioned in the table below. Please follow the respective remediation steps and rerun the discovery.

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Troubleshooting Symantec CA

- Introduction
- Issues in Symantec CA setting addition and fetch custom attributes
- Issues in Enrolling Symantec certificate
- Issues in Fetching Symantec certificate
- Issues in Renewing Symantec certificate
- Issues in Regenerating Symantec certificate
- Issues in Revoking Symantec certificate
- Issues in Reissuing Symantec certificate

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Symantec CA.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Symantec CA setting addition and fetch custom attributes

Issues in the Symantec CA Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**. The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Symantec**.
5. Click **Add**.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Symantec already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.		
<Field> should not be blank	Mandatory field <Field> may be missing	Please add the field <Field> and proceed
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid	Use the valid certificate

Issues in Enrolling Symantec certificate

Issues in the Symantec Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab. The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Symantec**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Fetching Symantec certificate

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Renewing Symantec certificate

Issues in the Symantec Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Symantec certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating Symantec certificate

Issues in the Symantec Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. Click **List** From the menu bar at the top of the page.
6. Click any **Symantec certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate,** click **Regenerate**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Revoking Symantec certificate

Issues in the Symantec Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server**. The **Server Certificate** page is displayed.
5. From the menu bar at the top of the page , click **List**.
6. Click any **Symantec certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Reissuing Symantec certificate

Issues in the Symantec certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and and select **Reissue Certificate** submenu.
4. Click **Server**. The **Server Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Symantec certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Reissue**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Troubleshooting Trustwave CA

• Introduction
• Issues in Trustwave CA setting addition

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Enrolling Trustwave certificate
• Issues in Fetching Trustwave certificate
• Issues in Renewing Trustwave certificate
• Issues in Regenerating Trustwave certificate
• Issues in Revoking Trustwave certificate
• Issues in Reissuing Trustwave certificate

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Trustwave CA.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Trustwave CA setting addition

Issues in the Trustwave CA Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Certificate Authority**. The **Certificate Authority** page is displayed.
4. On the **Certificate Authority** page, click **Trustwave**.
5. Click **Add**.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Trustwave already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
<Field> should not be blank	Mandatory field <Field> may be missing.	Please add the field <Field> and proceed.
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Authentication failed for user <user>	Username or password may be wrong	Please provide the valid username and password
Authorization failed	Incorrect reseller id provided	Please provide valid reseller id.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
You don't have permission to access <url> on this server.	Invalid URL specified.	Please provide a valid URL.

Issues in Enrolling Trustwave certificate

Issues in the Trustwave certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server/Client/Code Signing** Tab. The **Enroll Server Certificate** page is displayed.
5. Select **Certificate Authority** as **Trustwave**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Specified common name is invalid , it should end with a domain name.	Please provide a valid common name.

Issues in Fetching Trustwave certificate

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Certificate is not issued	Certificate polling may be in progress.	Certificate polling will happen and retrieve once the certificate is issued.

Issues in Renewing Trustwave certificate

Issues in the Trustwave Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Renew Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Select any **Trustwave certificate**.
7. From the dropdown **Actions** in the toolbar at the top of the page, select **Renew Certificate**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and re- perform renew.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating Trustwave certificate

Issues in the Trustwave Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**.
4. Click **Server/Client/Code Signing Certificate** Tab. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Regenerate.**

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Invalid common name specified, it should end with a domain name.	Please provide a valid common name.

Issues in Revoking Trustwave certificate

Issues in the Trustwave Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate,** click **Revoke**.

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.

Issues in Reissuing Trustwave certificate

Issues in the Trustwave Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Reissue Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate** Tab. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Trustwave certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Reissue.**

Error Messages

Error Message	Possible Cause	Possible Solution
Proxy details are not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR content is empty	CSR may not be available for the certificate to reissue.	Either CSR or private key should be available in the certificate.

Windows Agent Setup

Overview

This section helps you troubleshoot the common problems that you might encounter when using Windows Agent Setup. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on Windows Agent Setup. It helps you understand the importance of installing a validator and the method to do so.

• Overview
• Installing a Validator
• Windows Gateway Errors and Solutions

Overview

This section helps you troubleshoot the common problems that you might encounter when using Windows Agent Setup. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on Windows Agent Setup. It helps you understand the importance of installing a validator and the method to do so.

Installing a Validator

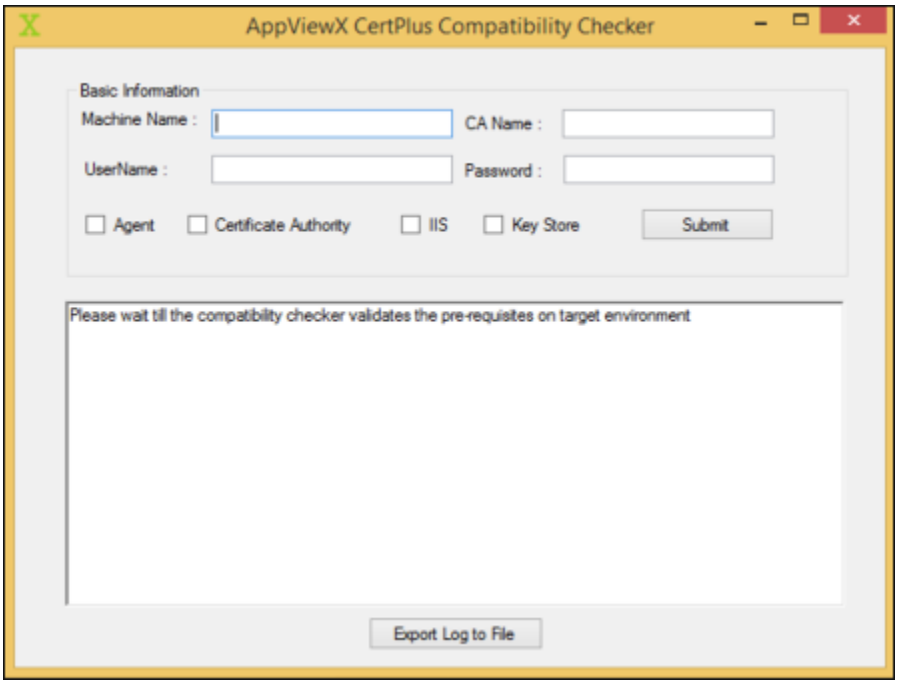
Validator analyzes an Agent and validates all the prerequisites before installing an agent. It is also used to troubleshoot any issue that occurs in the managed machines that run on a network. Before installing AppViewX gateway and the certificates, make sure you have downloaded the validator to either the Downloads folder or to the Desktop in your local environment.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Click the AppViewX.CertPlus.Validator.exe file to open the application for validation.
2. In the AppViewX CertPlus Validator screen that opens enter all the mandatory fields in the Basic Information section to proceed.
3. Select the Agent, Certificate Authority, IIS, and Non-IIS checkbox depending on what you want to validate and manage in the target machine.

• Based on the checkboxes you selected, the fields that are mandatory will be highlighted in Red color.
• The CA Name is required only if the Certificate Authority check box is selected.

Click Submit and the results are displayed as shown in the following image:



• AppViewX CertPlus Compatibility Checker is used for troubleshooting or validating the prerequisites as part of Windows Agent Installation. It comprises the following fields:

Name	Description	Condition
Machine Name	The name of the target machine must be validated. It is a hostname.	Mandatory field
CA Name	The name of the CA in the CA config.	Mandatory only when a CA is selected
User Name	User Name to be used for validating the target machine. It is in the format "username@domainname".	Mandatory field

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Condition
Password	The password corresponding to the provided user name.	Mandatory field

Options

- User can select single or multiple options based on the installation/ troubleshooting criteria:
- Agent: Select this option if we need to install an agent in the target machine which is configured in the "Machine Name". It will validate the prerequisites which are required for Agent Installation
- Certificate Authority: Select this option if we need to validate the Certificate Authority related functionality. The CA Name is mandatory only in this case. Use the certutil -dump command to get the CA Name. In the output of certutil command use-value in the "Server" as the Machine Name and use "Name" as the CA Name.
  - Based on the example below the machine Name is win3.avxdevlab.net and CA Name is avxdevlab-WIN3-CA-no-space.
  - IIS: Select this option if we need to validate the IIS sites related functionality.

Validations

Validate	Agent	CA	IIS	Keystore
User	Yes	Yes	Yes	Yes
.Net framework	Yes	Yes	Yes	Yes
Powershell	Yes	Yes	Yes	Yes
CertUtil	Yes	Yes	No	No
Certadm.dll	Yes	Yes	No	No
netsh	Yes	No	No	No
RPC	Yes	Yes	Yes	Yes
WinRM	Yes	Yes	Yes	Yes
WMI	Yes	Yes	Yes	Yes
IIS	No	No	Yes	No

- **KeyStore**: Select this option if you need to add to validate only the Microsoft Certificate Store related functionality

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

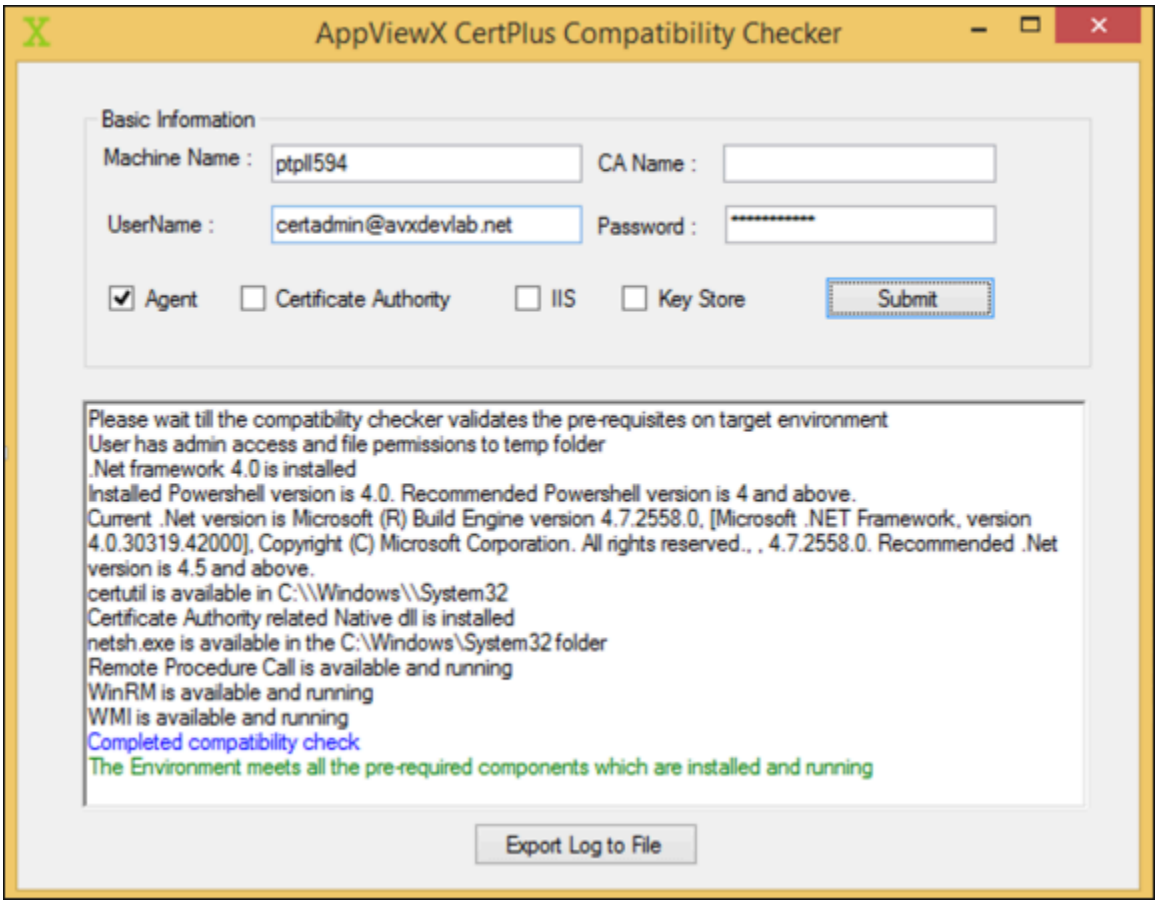


1. User Access: It will validate by connecting to the target machine with the specified username and password and check if it has admin access.
2. .Net Framework: It will check if .Net framework 4.5+ is installed and will display the current .Net framework version.
3. Powershell version: It will check if Powershell is installed and will display the current Powershell version
4. CertUtil: It will check if certutil component is available. This is used to get the CA name and the corresponding templates.
5. CertAdm.dll: This is the native component used to access the CA and will check if this component is available in the C:WindowsSystem32 folder. Sometimes, while trying to access this component during the verification it will return an error and hence, a manual check must be performed.
6. netsh.exe: This is used to bind the certificate to the installed agent port (8999).
7. RPC service: The remote procedure call service must be running to perform all the remote operations and it will validate if the service is installed and running on the target machine.
8. WinRM service: Windows Remote Management service is required for the Powershell execution and it will validate if the service is installed and running on the target machine.
9. WMI service: Windows Management Instrumentation service is required for WMI and Powershell execution and it will validate if the service is installed and running on the target machine.
10. IIS: It will check if the IIS server is installed and identify the current IIS version.

Color Codes during the Execution

- **Black**: Success information and output
- **Red**: An error or warning, must take corrective action based on the prerequisite document in case of any issues
- **Blue**: Completion of the validation process
- **Green**: Complete process is successful

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Export Log to File: This is used for exporting the validation summary into a log file.

Steps to test gateway installation:

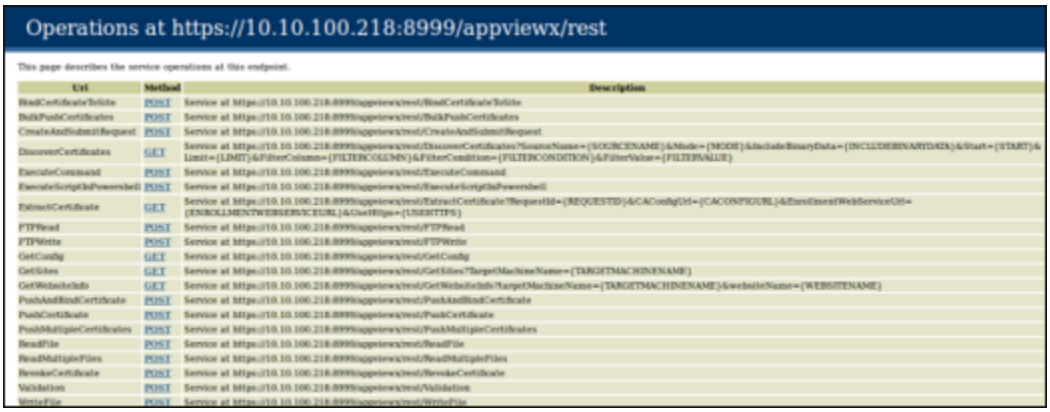
To test the installation, go to the following URL:

https://localhost:8999/appviewx/

`https://<IP/Hostname>:<Port>/appviewx/rest/help` (Needs the certificate to be on the store/ browser)

For example, https://xx.xx.xx.xx:8999/appviewx/rest/help

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



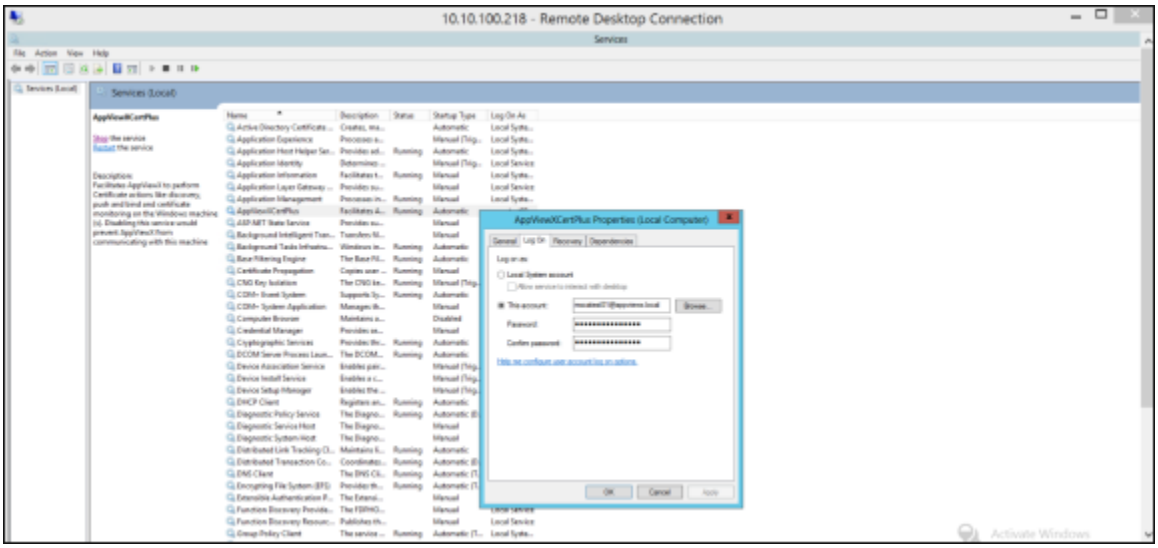
- The above page confirms the accessibility and installation of the service.
- In case, a different client authentication certificate is being used, ensure that the CRL mentioned in the certificate is reachable from the AppViewX Windows gateway hosting server.
- Go to **AppViewX>> Settings>> Certificate** to register the gateway with AppViewX.
- Register the gateway with the URL format as follows: `https://<IP/Hostname>:<Port>/appviewx`

For example, https://xx.xx.xx.xx:8999/appviewx

Modify Agent services with the service Account The Windows gateway agent can be installed using a service account or an admin account.

- If the customer has a policy that states that the service account cannot be part of the administrator group or that the service account is only a part of the user group, then:
  - The gateway agent service is installed using an admin account.
  - The installed agent service is updated with the service account details in services.msc. Add the account in the properties of the AppViewXCert Plus service.
  - Services.msc -> AppViewXCert Plus -> Right click (Properties) -> LogOn .> Update the user account in the format of username@domainname.
  - Refer to the following image.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- In this case, the following command has to be executed from the PowerShell:

Netsh http add urlacl url=https://+:8999/appviewx/user=appviewx.localmscatest01

- In the above command, the value for user = <domainserviceaccount> and the URL must be changed respectively.
- Once this is done, stop and start the AppViewXCertPlus Service in services.msc.

Windows Gateway Errors and Solutions

Error	Solution
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <machine name> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <name> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command `setspn -s http/machinename domainusername`. • This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<machine name> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic.	
Retrieving the COM class factory for remote component with CLSID	• The component used for accessing CA (certadm.dll) is not installed or has permission issues. • Check if the DLL is available in `C:WindowsSystem32` folder or else, install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. For example, for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot process the request. The following error with error code 0x80090322 occurred while using Negotiate authentication: An unknown security error occurred.	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command `setspn -s http/machinename domainusername`. • This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the	• Check if the WinRM service is running. • Go to the Powershell on the target machine and run the command `WinRM QuickConfig`.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic	• Execute the command `Enable-PSRemoting -force`. • Execute the command `netsh winhttp show proxy` and if a proxy is configured, it must be reset using the command `netsh winhttp reset proxy`.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <machine name> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	• Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable.	Go to the target machine and start the RPC service if it is stopped.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
0x800706ba (WIN32: 1722 RPC_S_SERVER_ UNAVAILABLE)	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path '\\<machine name>\C$\ \\Windows\\Temp\\qgwwkqi3.fff' is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.

More than 5 connections are not allowed	• Run Powershell as an administrator.
	• Check existing config `winrm get winrm/config`.
	• Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring.
	  • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
	  • `winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
	  • `winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`

Connecting to remote server failed with the following error message: The WS-Management service cannot process the	• Run Powershell as an administrator. • Check existing config `winrm get winrm/config`.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	• Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring. • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'` • `winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'` • `winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
Client Certificate gives Permission Denied 403 errors. This can happen in a certain environment and it's intermittent	• Check if the client certificate is installed correctly by validating the chain in the Personal Store. • The root of the client certificate must be available in the Trusted Root Certification Store of the server. • The intermediate of the client certificate must be available in the Intermediate Certification authorities of the server. • If all of the above are fine, go to the agent server and complete the following steps: 1. MMC 2. Add/Remove SnapIn 3. Select certificate 4. Select LocalMachine 5. Go to Personal Store and click on client certificate 6. Go to chain 7. Export the root certificate and save as Root.cer in a location 8. Import the Root.cer into trusted root back again 9. If this does not solve the issue, then check if the trusted root contains and non- root certificates 10. Click on "Trusted Root" store and check if there any certificate which has IssuedTo and IssuedBy different 11. Take a backup of such certificates and move it to respective stores 12. If it does not solve the issue, then add the root certificate to the "Client Certificate Issuers"
The permission on the certificate template do not allow the current user to enroll for this type of certificate	1. Go to the CA server. 2. Open Certificate Authority and select the CA Server. 3. Right-click on properties and select the Security tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
	4. Check if the user used in Agent has the necessary permissions to read, issue, manage, and request certificate(s). 5. If the user is a part of a group, then ensure that the group has the required permissions. 6. Click on the Certificate Templates and right-click to manage the template. 7. Right-click on the template which has the issue and navigates to security. 8. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib. IenumCERTVIEWROW.Next().	In the CA server, navigate to the registry through the regedit command and set the following: 1. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBSessionCount to 64 hex (100 Dec) 2. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.rn	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the	The user name or password is incorrect.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic.	

Connecting to remote server <machine name> failed with the following error message: WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits accesses to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	• WinRM service is already running on the following location of the machine: C:Windowssystem32>WinRM quickconfig
	• If WinRM is not set up to allow remote access to this machine for management, the following changes must be made:
	  • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
	  • Make these changes [y/n]? y

There is not enough space on the disk	Ensure that your hard disk has enough free space.
Management Connect to remote machine <machine name> as user failed with the following error User credentials cannot be used for local connections	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group. • Configure the credentials in AppViewX.CertPlus.Service Logon option.
Denied by Policy Module 0x80094800, The request was	Use template name instead of the template display name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error	Solution
for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	
Device Communication failed while using Native option to connect to CA remotely	1. Go to the agent machine. 2. Open `services.msc` using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
Certificate Request (CSR) is using a different account to request a certificate from CA as compared to account configured in AppViewX	1. Go to the agent machine. 2. Open `services.msc` using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.

Troubleshooting General

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Overview
• Troubleshooting Certificate Group
• Troubleshooting Certificate Policy
• Troubleshooting Certificate Reports Configuration
• Troubleshooting Configuration of Workflow

Overview

This section of the guide will help you address the general issues faced during various processes related to Certificates like Group, Policy, Reports, and workflow. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

Troubleshooting Certificate Group

• Overview
• Issues in Group create/update
• Issues in group delete
• Issues in assign/unassign certificate to a group

Overview

This section guides you in troubleshooting problems that you might encounter while dealing with Certificate Group like creating or updating, deleting, assigning/ unassigning certificates to a group.

Issues in Group create/update

Error Message	Possible Cause	Possible Solution
Given parent group is not present in AppViewX.	The parent group provided by the user does not exist in AppViewX.	Check if the group exists in the given parent group name.
Group already exists with the given name	Another group with the same name already exists.	Group name should be unique.
Missing user information.	User information is not available in the request.	Provide valid user information in the request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Permission restricted to this group to edit/delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Parent name and group name should not be same. Kindly change the parent name.	Parent group name and group name are the same in the given request.	Change the group name in the request.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
Failed to update certificate group.	AppViewX is not able to update the group details.	DB may not be accessible during that time.
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in group delete

Error Message	Possible Cause	Possible Solution
Default group cannot be deleted.	The user is trying to delete the default group provided by AppViewX.	AppViewX allows users to delete only user-defined groups.
Permission restricted to this group to edit/ delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Given parent group is not present in AppViewX.	The parent group provided by the user is not available in AppViewX.	Check if the group is available in the given parent group name.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Given child group is not present in AppViewX.	The child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Failed to delete certificate groups since it is not available. Those groups are <GroupNames>	Given groups are not available in AppViewX.	Check and provide a valid group name to delete.

Issues in assign/unassign certificate to a group

Error Message	Possible Cause	Possible Solution
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
The operation cannot be completed as <count> selected certificate(s) are in Read-Only access groups	Some of the selected certificates are in groups that have “read-only” permission for the user.	Remove the certificates that have “read-only” permission or Change the group permissions to “RW”.
Group name cannot be empty.	Group is given as empty in the request.	Groupname should not be empty. Give a valid group name.
Certificate uuid either empty/ invalid.	Certificate UUID is not given in the request.	Provide a valid certificate UUIDs to perform the action.

Troubleshooting Certificate Policy

- Overview
- Issues in policy create/update
- Issues in policy delete

Overview

This section of the guide will help you troubleshoot the common problems that you might encounter while dealing with Certificate Policy actions like creating or updating or deleting.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in policy create/update

Error Message	Possible Cause	Possible Solution
[group] Groups are already assigned to another policy or doesn't exist	The group may be associated with some other policy. Group may not be available in AppViewX.	Check if the group is associated with some other policy. Check if the group is available in AppViewX.
At least one ECDSA curve should be selected for each EC bitlength	ECDSA curve details are not provided in the request.	It is mandatory to give at least one ECDSA curve for each EC bit length.
Failed to fetch the policy.	AppViewX is not able to fetch policy details from DB.	DB may not be accessible during that time. Please retry the operation.
Policy already exists with the given name.	Policy name already exists in the inventory.	Policy names should be unique.
Failed to update certificate policy information.	AppViewX is not able to update policy details from DB.	DB may not be accessible during that time. Please retry the operation.
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in policy delete

Error Message	Possible Cause	Possible Solution
Default policy cannot be deleted.	The user is trying to delete the default policy provided by AppViewX.	AppViewX allows users to delete only user-defined policies.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Mandatory field is missing or invalid - policyNames	The field policyNames is not provided with any values in the request.	Check if the policyNames field is available and has values in the request.
Failed to delete certificate policy information.	AppViewX is not able to delete the policy.	DB may not be accessible during that time. Please retry the operation.

Troubleshooting Certificate Reports Configuration

- Overview
- Issues in Configuring Reports

Overview

This section of the guide helps you troubleshoot the common problems that you might encounter while configuring various certificate reports like validation status reports, summary reports, count by issuer reports.

Issues in Configuring Reports

Issues in configuring Validation Status Report

Error Message	Possible Cause	Possible Solution
FQDN cannot be null or empty.	The FQDN value provided is either null or empty.	Provide a valid FQDN value.
Certificate network discovery plugin may not be enabled. Contact AppViewX support team.	The plugin avx_vendor_cert_network_discovery is not enabled.	Enable avx_vendor_cert_network_discovery plugin.
Certificate network discovery plugin may be in not running state.	The plugin avx_vendor_cert_network_discovery may be in the “Not Running” state.	Start avx_vendor_cert_network_discovery plugin and try again.
IP <ipPort> is invalid	Given IP port is not valid.	Check and provide a valid IP port.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid FQDN.	AppViewX is not able to access the given FQDN.	Check if the FQDN is valid and whether AppViewX has access to the FQDN.
Missing user information.	User information is not available in the request.	Provide a valid session-id or username and password in the request.

Issues in configuring Certificate Summary Report

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/ update the scheduler job in crontab.	1. Provide valid cron settings. 2. DB may not be reachable, try after some time.

Issues in configuring Count by Issuer Report

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/ update the scheduler job in crontab.	1. Provide a valid cron setting. 2. DB may not be reachable, try after some time.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Configuration of Workflow

- Overview
- Issues in configuring workflow

Overview

This section of the guide helps you troubleshoot the problems encountered while configuring workflow.

Issues in configuring workflow

Error Message	Possible Cause	Possible Solution
Csr submission failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.
Certificate <action>failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.

Troubleshooting Protocols

- Overview
- Troubleshooting Auto-Enrolment ACME
- Troubleshooting Auto-Enrolment EST
- Troubleshooting Auto-enrolment of MsIntune SCEP
- Troubleshooting Auto-enrolment of SCEP

Overview

This section of the guide helps you to troubleshoot the various issues encountered by you while using different protocol functionalities. The different protocols covered are ACME, EST, MsIntune SCEP, and SCEP. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Auto-Enrolment ACME

- Introduction
- Issues in ACME setting addition and check the settings
- Issues in Auto Enrolling Certificate via ACME

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using ACME functionalities like setting addition, checking communication, enrollment, and revocation.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported ACME Client

- Certbot
- Cert manager

Issues in ACME setting addition and check the settings

Issues in ACME Setting Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **ACME**. The **Auto Enrollment ACME** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An ACME setting with the same name already exists in ACME Page.	Check the ACME Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
ACME setting is invalid - Agent ip is not reachable	The ACME agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
ACME setting is invalid - Policy is not associated to the provided group	The policy selected might be associated with some other group that is not selected.	Please check whether the selected policy and group are associated with one another.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Auto Enrolling Certificate via ACME

Note: From the client machine hit the auto-enroll call using AppViewX ACME server URL which is displayed on the ACME setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR)	The provided agent IP or agent name is not found in the ACME settings.	Check for the agent IP and agent name in the client machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Agent settings is not found		
Unable to perform ACME account creation/updation operation	ACME is already present or the account is not proper in the client machine.	1. Check whether the account is proper in the client machine. 2. Delete the acme accounts in the client machine and retry.
Unable to perform ACME challenge creation operation	Challenge verification failed before enrolling the certificate.	1. Check for the option selected in the ACME setting if it's HTTP or DNS. 2. Check for the reachability of URL for HTTP challenge verification.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid	1. Check for passwords in BASIC authentication. 2. Check for the nonce and other parameters in DIGACME parameters.
Unable to perform ACME order finalize operation	This phase is used to obtain the CSR and submit it.	1. Check for the input CSR in the request. 2. Check whether the CSR submission is successful in AppViewX.
Unable to obtain the enrolled certificate	The certificate might not be present for the provided transaction id.	Check if the certificate is enrolled or not in AppViewX inventory.
Unable to establish connection with ACME server.	There might be an issue with reaching the AppViewX ACME agent IP from the client.	Check whether the ACME agent IP is reachable from the client machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Check whether the ACME agent IP is open and can be accessible.
Group policy does not have the given hash function	The requACMEed hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the ACME setting. 3. In the hash function field include the “requACMEed” and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in work order log - “**Denied due to policy module**”	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as below: `"db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})"`  **Note:** This would allow multiple CSR’s with the same parameters in the certificate inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Auto-Enrolment EST

- Introduction
- Issues in EST setting addition and check the settings
- Issues in auto-enrolling certificate via EST
- Issues in obtaining CA certificate via EST
- Issues in auto re-enrolling certificate via EST

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using EST functionalities of CA like setting addition, enrollment, obtaining, and re-enrollment.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported EST Client

- Cisco Routers
- Libest client

Issues in EST setting addition and check the settings

Issues in EST setting Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **EST**. The **Auto Enrollment EST** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An EST setting with the same name already exists on EST Page.	Check the EST Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
EST setting is invalid - Agent ip is not reachable	The EST agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
EST setting is invalid - Certificate does not belong to the selected CA.	The issuer certificate provided does not belong to the CA which is selected.	Please check whether the selected issuer certificate belongs to the CA which was selected earlier.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in auto-enrolling certificate via EST

Note: From the client machine hit the auto-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the enroll request from the client machine	1. Check whether the client certificate and key are set in the enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the enrollment request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - “Denied due to policy module”.	Check for the bit length in the CSR parameters, if it is lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as given below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR’s with the same parameters in the certificate inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in obtaining CA certificate via EST

Note: From the client machine hit the get ca certificate call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the get ca request from the client machine.	1. Check whether the client certificate and key are set in the “get ca certificate request”. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the “get ca cert request”.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been	Check for the issuer certificate and its issuer certificate available in the inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	deleted or the server certificate has been deleted.	
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.

Issues in auto re-enrolling certificate via EST

Note: Note: From the client machine hit the auto re-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the re-enroll request from the client machine	1. Check whether the client certificate and key is set in the re-enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the re-enroll request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in logs and in failed Work order for the reason why submission got failed.
Unable to submit the CSR request to	There might be an error in the work order log - “**Denied due to policy module**”.	Check for the bit length in the CSR parameters, if its lesser than or equal to 1024 then increase that in the CSR.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
certificate authority - For MSCA		
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as mentioned below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR's with the same parameters in the certificate inventory.
Enrolled Certificate is not found	While renewing the enrolled certificate, the enrolled certificate might not be present in certificate inventory.	1. Check if the enrolled cert is present in certificate inventory. 2. Check if the enrolled certificate provided in "renew request" is a valid one and is enrolled already in AppViewX. 3. If the enrolled certificate is not present in inventory, check if the authentication cert is in cert inventory.

Troubleshooting Auto-enrolment of MsIntune SCEP

- Overview
- Issues in MSIntune SCEP setting addition and validating the settings
- Issues in auto enrolling certificate via MS Intune SCEP

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

This section helps you troubleshoot the common problems that you might encounter when using MSIntune SCEP functionalities like setting addition and certificate enrollment.

Issues in MSIntune SCEP setting addition and validating the settings

Issues in the MSIntune SCEP Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **MsIntune**. The **Auto Enrollment MsIntune** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent ip is not reachable	The MS Intune SCEP agent IP and specified port may not be reachable from the AppViewX node.	Validate and ensure that the agent IP/Port is reachable.
Certificate does not belong to the selected CA.	The server certificate provided in the agent setting does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.
CA setting connection is in Failed status	The connection status of the chosen CA setting chosen in the agent setting failed.	Check the specified CA setting and make necessary changes to make it valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in auto enrolling certificate via MS Intune SCEP

Note:

1. From the client machine, enroll for the certificate using Company Portal application.
2. Newly enrolled certificate should be available in the AppViewX CERT+ Inventory. If the new certificate is not available in the AppViewX CERT+ Inventory, even after 5 minutes from triggering the request from the device, then logon to the CLI and verify the logs for avx_vendor_cert_intune_agent plugin.

Following errors may appear in the logs -

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Request might have failed due to a specific error from CA	Verify the vendor logs to see if there is any CA specific error.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry given below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"},{$set: {"constant":"no"}})"

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Note: This would allow multiple CSR's with the same parameters in the certificate inventory.
Challenge in PKCS#10 request (Transaction ID: <<transactionID>>) is not valid. Certificate enrollment will not be processed.	Challenge password validation with Microsoft Intune has failed. Possible reasons - 1. Connectivity issue with Microsoft Intune. 2. Intune credentials configured in agent settings might be incorrect.	1. Validate the internet access in the AppViewX server. 2. Check and correct the Intune Client Id/Tenant Id/Client Secret configured in the MS Intune agent setting.
No error message but enrollment request does not get triggered after the getCACert call from the client device.	A mismatch between the CA certificate configured in the MS Intune Agent setting and that configured in the Intune portal.	Verify and ensure that the root and intermediate CA certificates of the Server certificate available in the AppViewX MS Intune agent setting match with the Root and Intermediate certificates configured in the MS Intune portal (Azure) SCEP profile.

Troubleshooting Auto-enrolment of SCEP

- Introduction
- Issues in SCEP setting addition and check the settings
- Issues in Auto Enrolling certificate via SCEP
- Issues in Obtaining CA certificate via SCEP

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using SCEP functionalities like setting addition, enrolment, and obtaining.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Supported SCEP Client

- SSCEP client
- Cisco Routers
- Mobileiron Cloud portal

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in SCEP setting addition and check the settings

Issues in the SCEP Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **SCEP**. The **Auto Enrollment SCEP** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	A SCEP setting with the same name already exists on SCEP Page.	Check the SCEP Setting name, it should be unique.
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields are missing or invalid.	Add all the valid information in the mandatory section.
SCEP setting is invalid - Agent ip is not reachable	The SCEP agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
SCEP setting is invalid - Certificate does not belong to the selected CA.	The server certificate provided does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.

Issues in Auto Enrolling certificate via SCEP

Note: From the client machine hit the auto-enroll call using AppvViewX SCEP server URL which is displayed on the SCEP setting page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the SCEP settings.	Check for the agent IP and agent name in the client machine.
Unable to establish connection with SCEP server.	There might be an issue with reaching the AppViewX SCEP agent IP from the client.	Check whether the SCEP agent IP is reachable from the client machine. Check whether the SCEP agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the SCEP setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check the reason for submission failure in logs and failed Work order.
Unable to submit the CSR request to	There might be an error in the work order log - “**Denied due to policy module**”.	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase it in the CSR.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
certificate authority - For MSCA		
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as mentioned below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR's with the same parameters in the certificate inventory.

Issues in Obtaining CA certificate via SCEP

Troubleshooting AWS, CLOUD

- Overview
- Troubleshooting of AWS - CLOUD (ACM and IAM)
- Troubleshooting AWS CLOUD CloudFront
- Troubleshooting AWS CLOUD ELB
- Troubleshooting Azure CLOUD
- Troubleshooting CLOUD - Common Functionality

Overview

This section of the guide will help you tackle the various issues that arise while using the functionalities of CLOUD services. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting of AWS - CLOUD (ACM and IAM)

- Introduction
- Issues in Server Addition using AppViewX GUI
- Issues in Fetch Regions
- Issues in Discovery in IAM & ACM
- Issues in Push and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

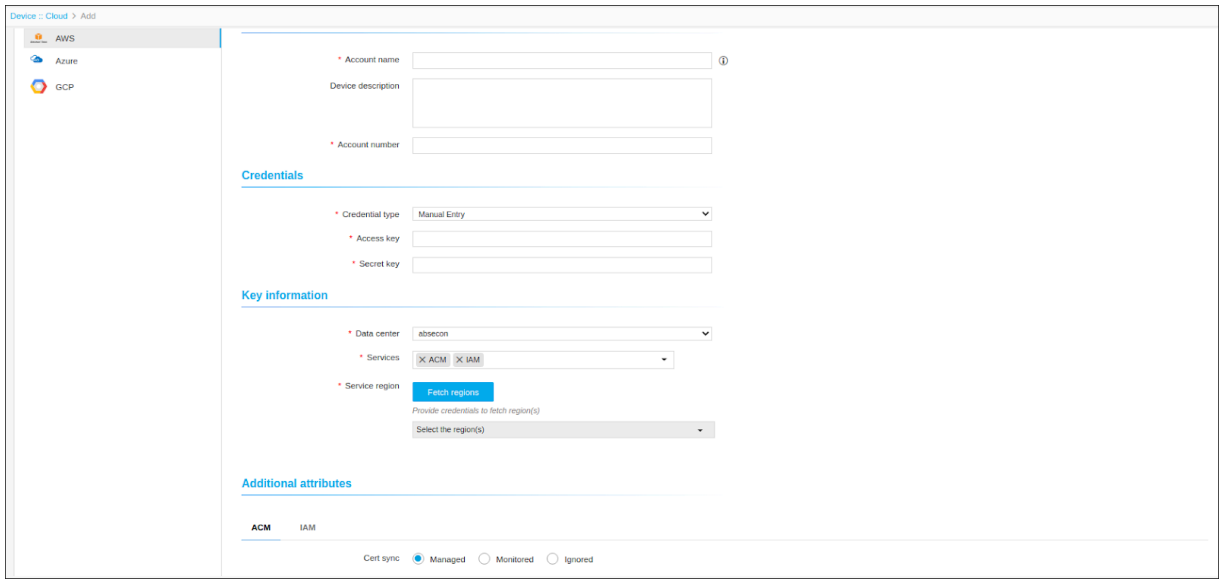
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

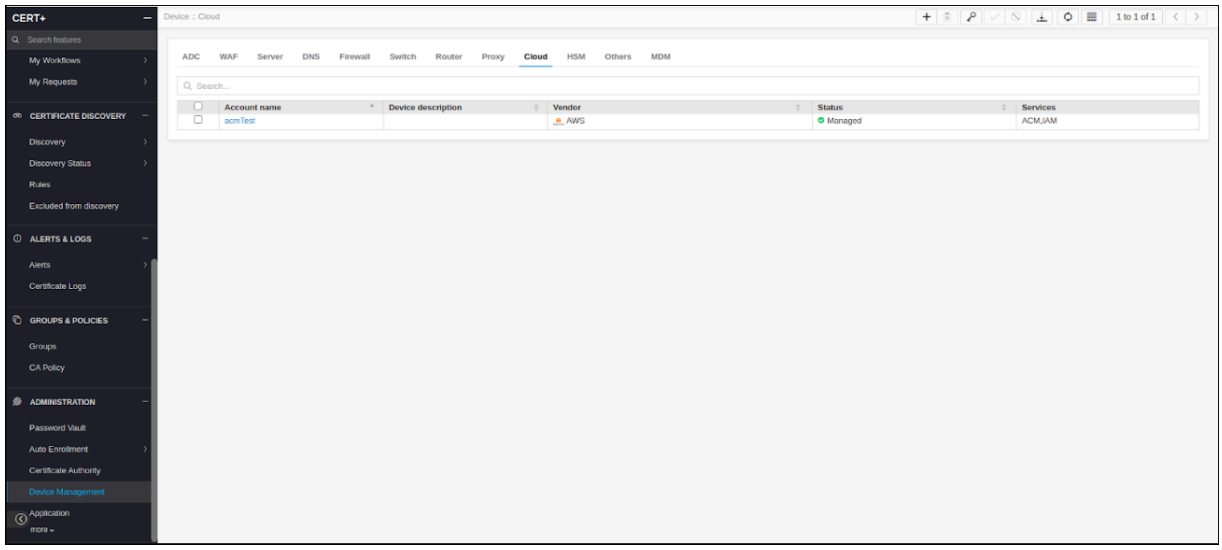
Issues in Server Addition using AppViewX GUI

Issues in the Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details** section on the left, Click **AWS**.
7. Fill in the appropriate details.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center 5. Services 6. Regions

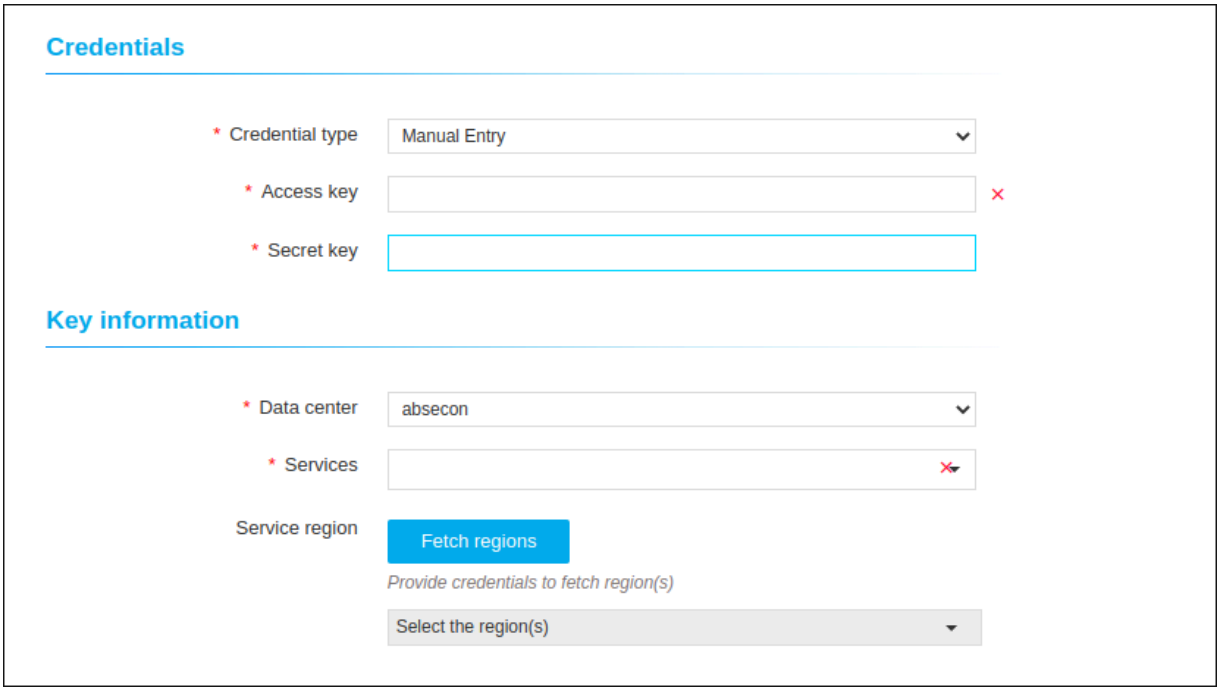
Issues in Fetch Regions

Issues in Fetch Regions

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, select **AWS**.
5. Fill in **Access Key** and **Secret Key** in the **Credentials** section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Click **Fetch Regions**.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

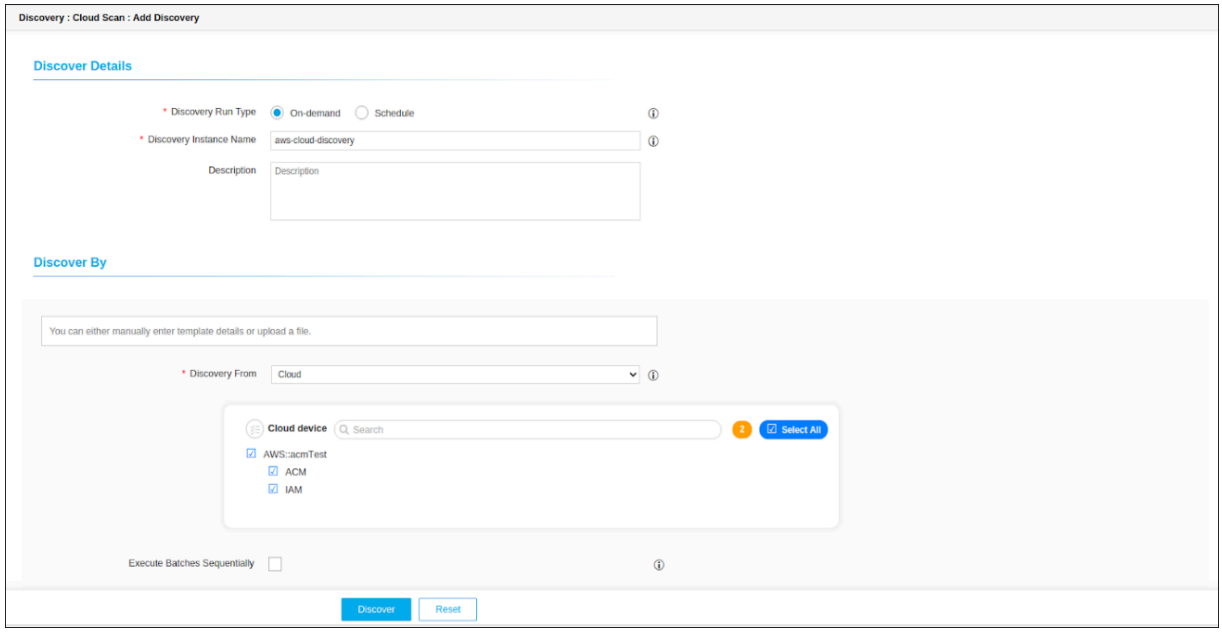
Issues in Discovery in IAM & ACM

Issues in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Cloud Scan**. The **Discovery Cloud Scan Add Discovery page** will be displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.

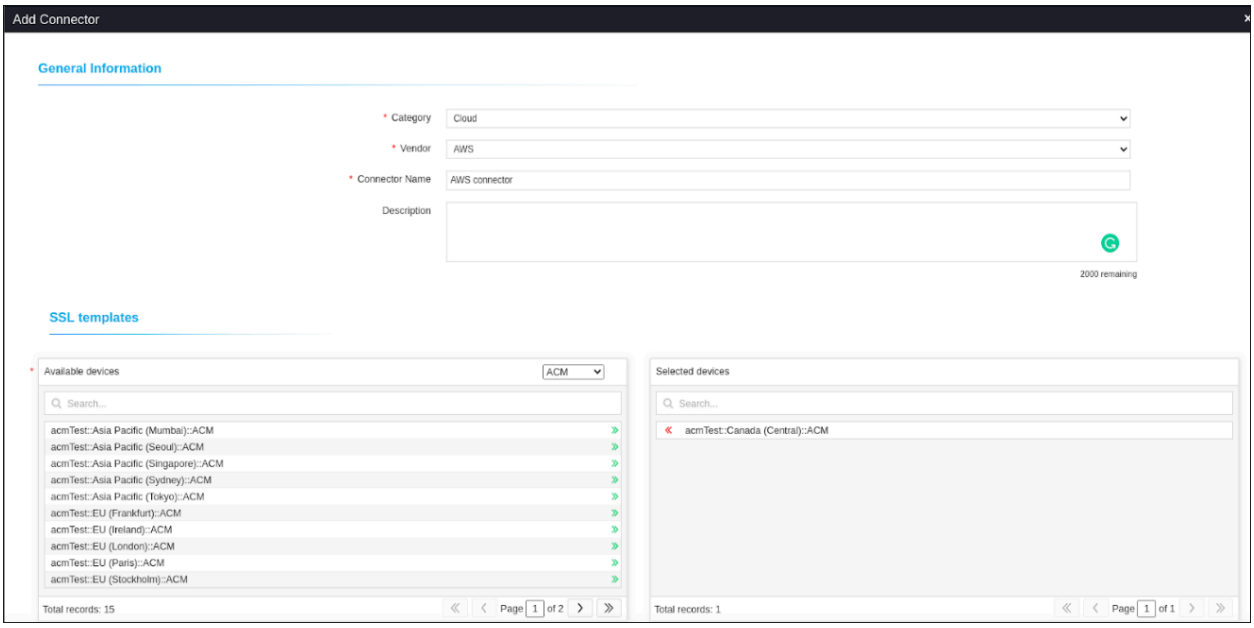


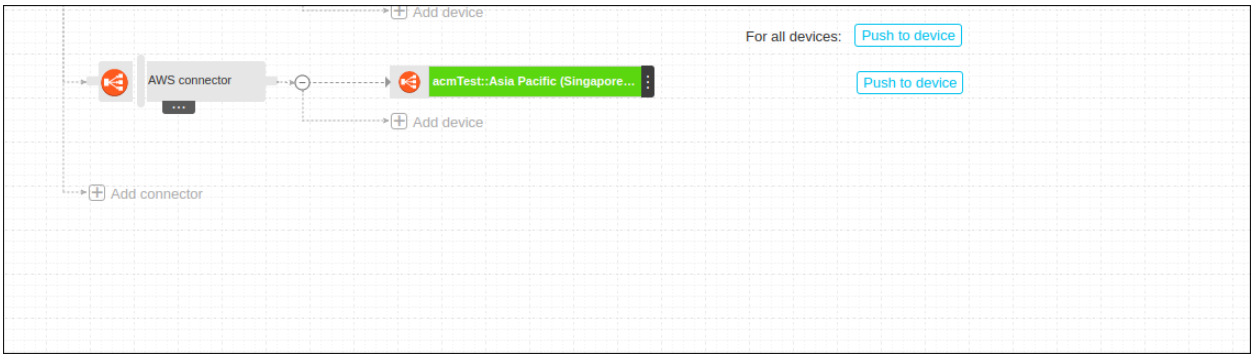
Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, such as in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	Userdoes not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

Troubleshooting AWS CLOUD CloudFront

- Introduction
- Issues in CloudFront Service

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for CloudFront service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

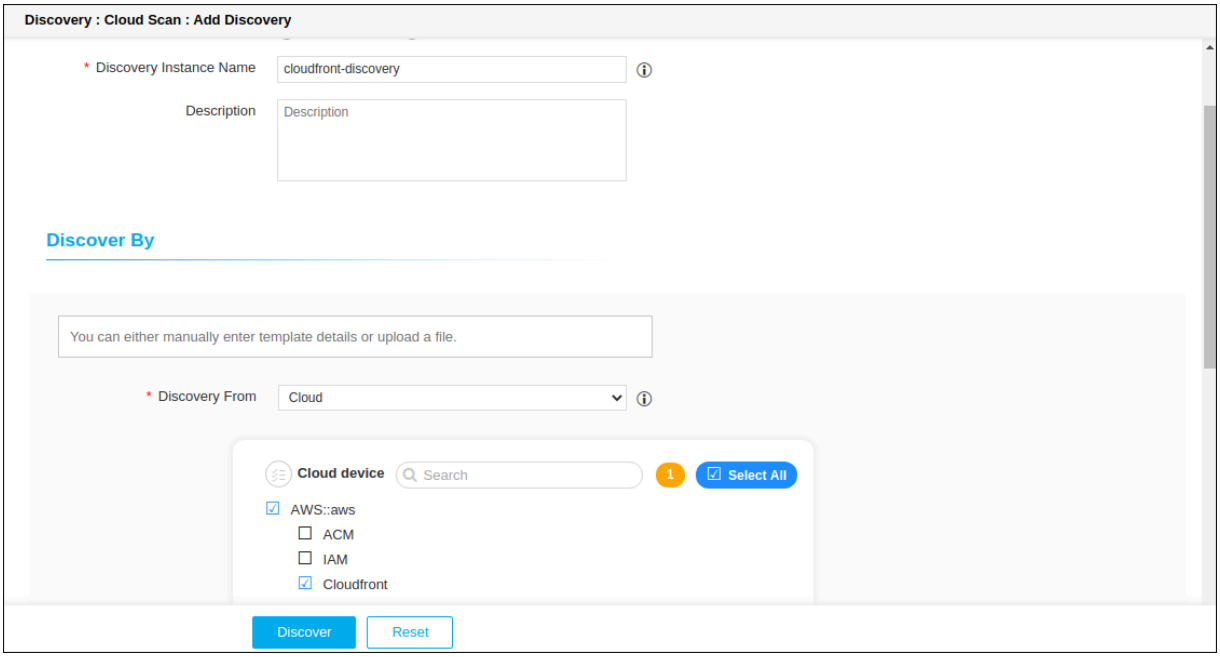
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CloudFront Service

Issues in the Discovery in Cloudfront

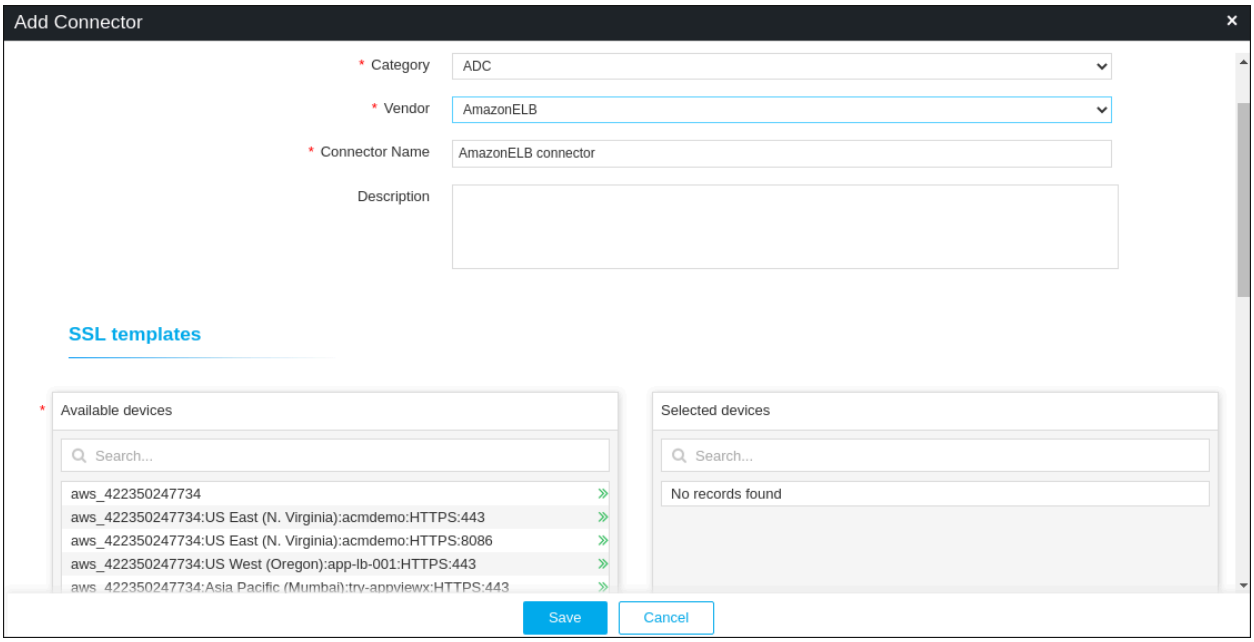
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Cloud Scan**. The **Discovery Cloud Scan Add Discovery** page will be displayed.

> **Note:** To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in the Push-Bind and Rollback





Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private Key is required to push certificate to ACM inventory	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide “Modify” access for the resource and retry.
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.
Certificate cannot be pushed as selected Amazon CA certificate is in <SOURCE_REGION> region and region you tried is <DESTINATION_REGION>	Selected certificate is in ACM in a different region than the region to be pushed	Use certificates available in the <DESTINATION_REGION> (or) Push a new certificate to the <DESTINATION_REGION>

Troubleshooting AWS CLOUD ELB

- Introduction
- Issues in Discovery in ELB
- Issues in Push-Bind and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ELB service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

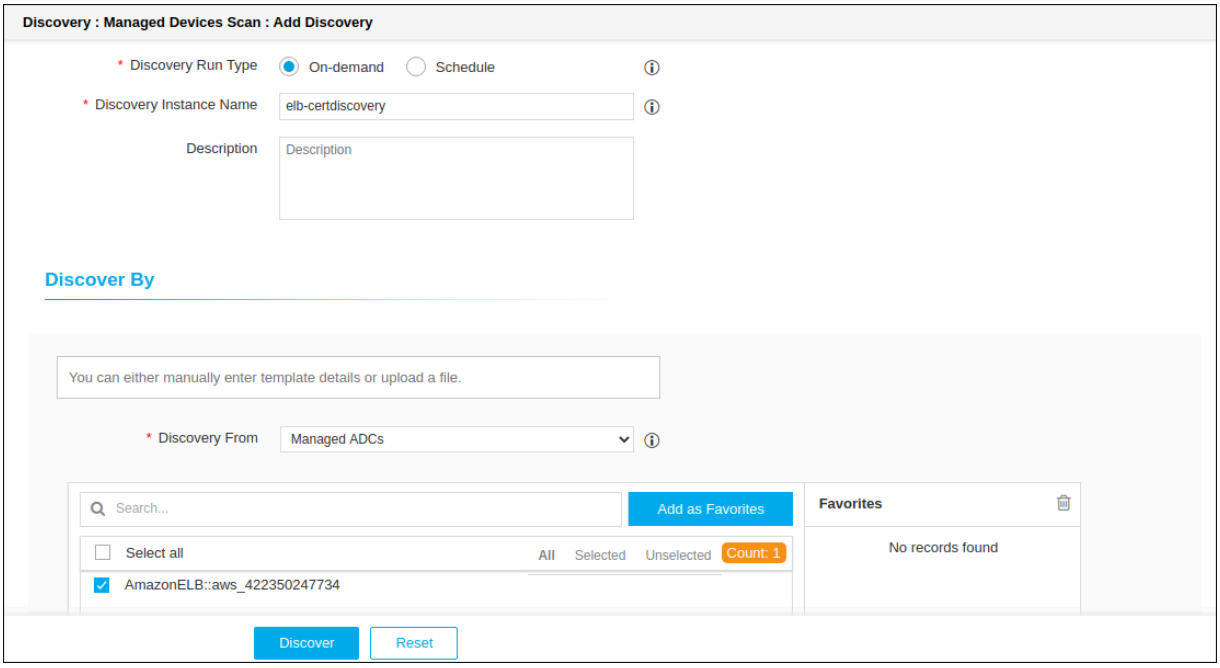
Issues in Discovery in ELB

Issues in the Discovery in ELB

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.
4. Click **Cloud Scan**. The **Discovery Cloud Scan Add Discovery** page will be displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory.

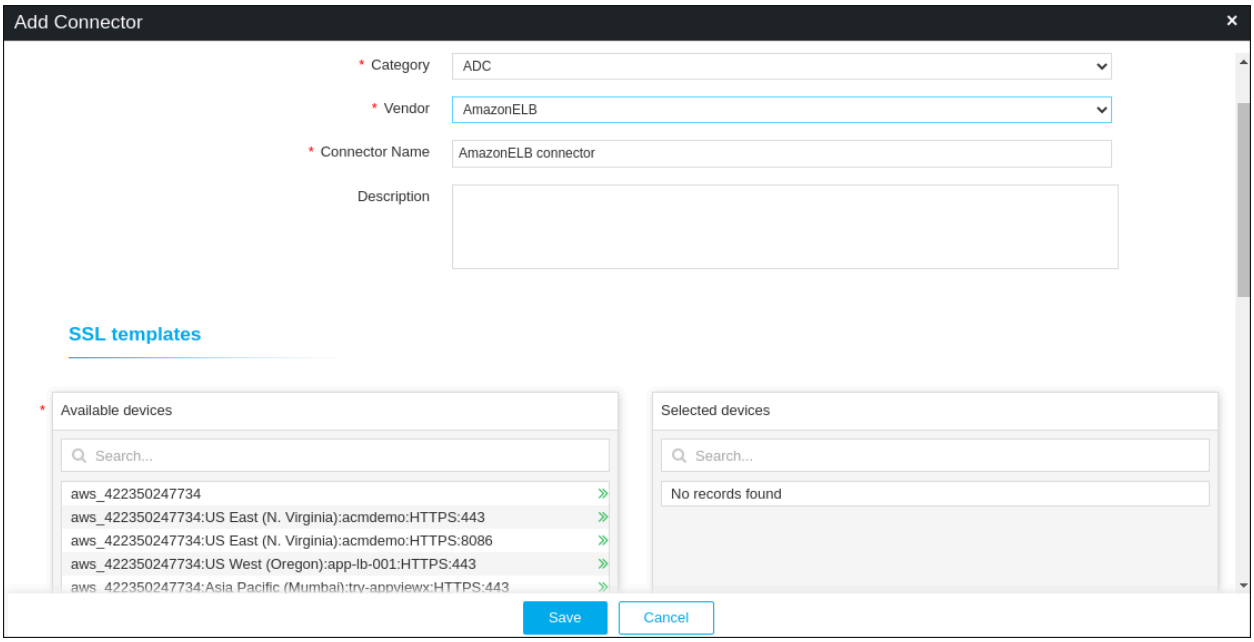


Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Push-Bind and Rollback





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in an enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
1 validation error detected: Value at 'privateKey' failed to satisfy constraint.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because the push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to the device when certificate is unavailable, i.e, in a new state.	Push to the device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	The provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide Modify access for the resource and retry
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.

Troubleshooting Azure CLOUD

- Introduction
- Issues in Azure Cloud Addition using AppViewX GUI
- Issues in Communicating to Azure Cloud
- Issues in Accessing Azure Cloud
- Issues in Managed Cloud
- Issues in Unmanaged Cloud
- Issues in Fetch Config
- Issues in Certificate Discovery
- Issues in Certificate Import

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, push, bind, rollback, and other actions associated with Azure cloud.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

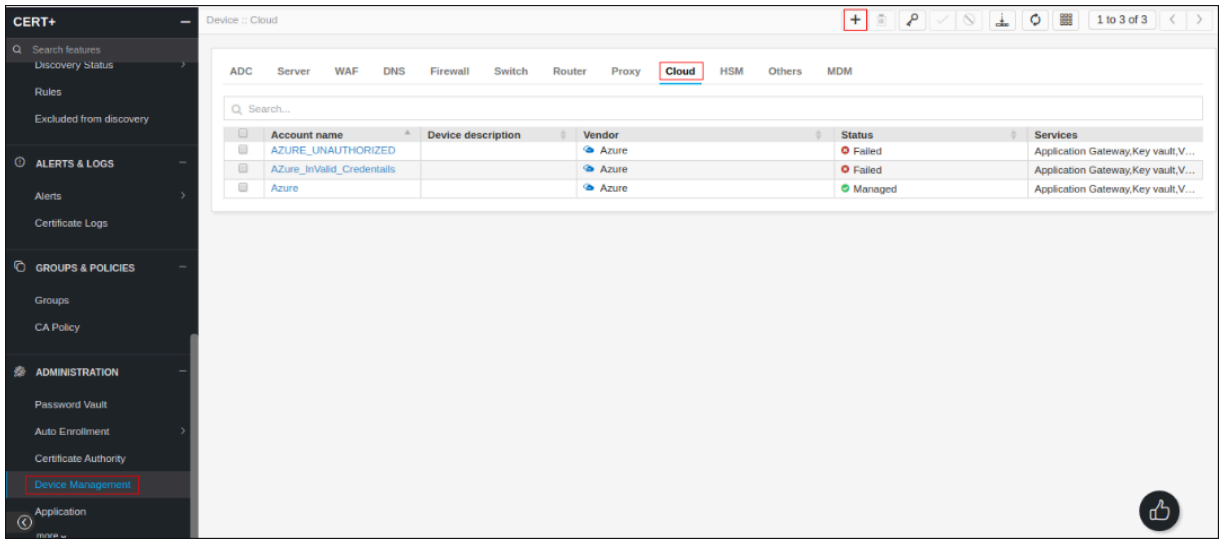
Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

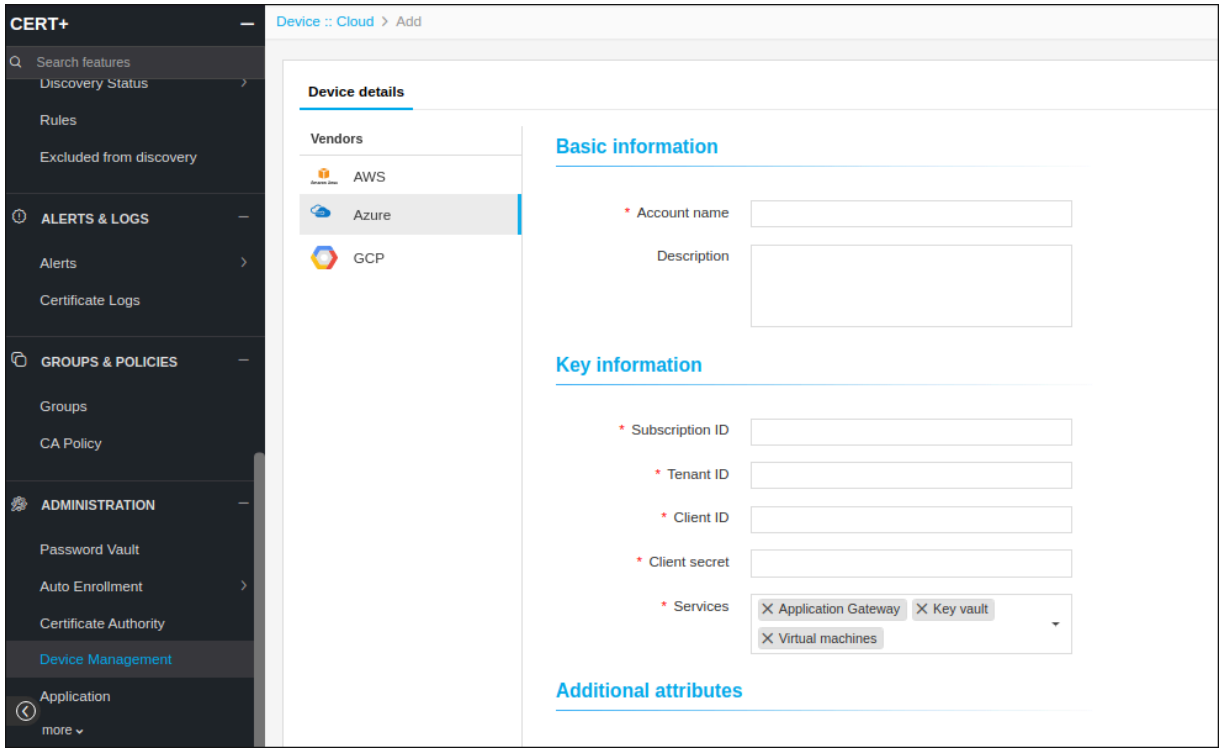
Issues in Azure Cloud Addition using AppViewX GUI

Issues in the Azure Cloud Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. On the **Device Addition** page, select **Azure** from the **Vendors details section**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A Cloud Account with the same name exists in inventory.	Check the Account name, it should be unique.

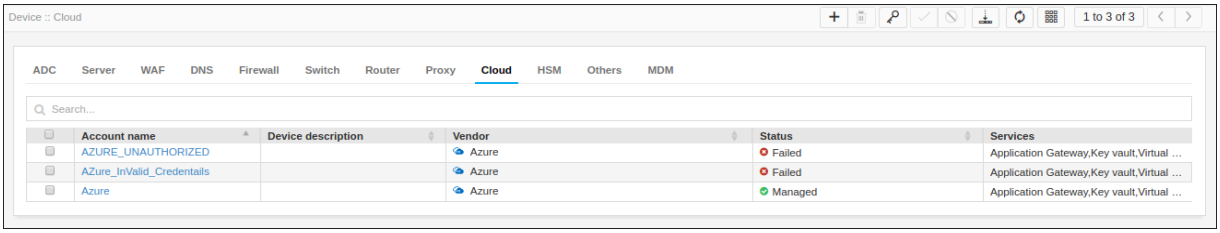
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

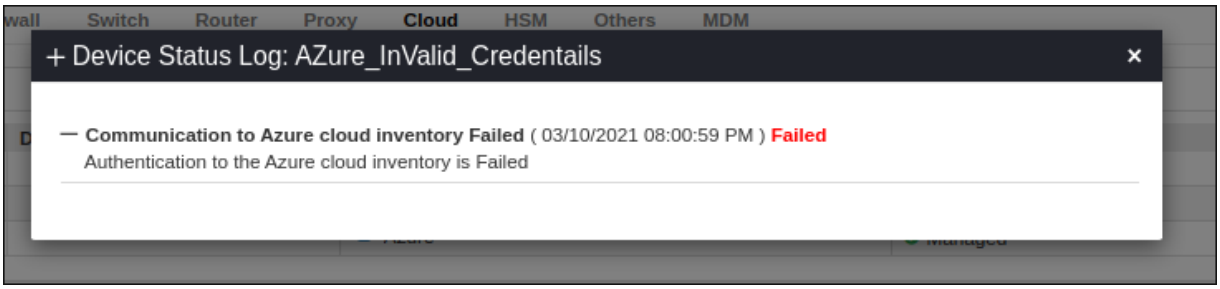
Issues in Communicating to Azure Cloud

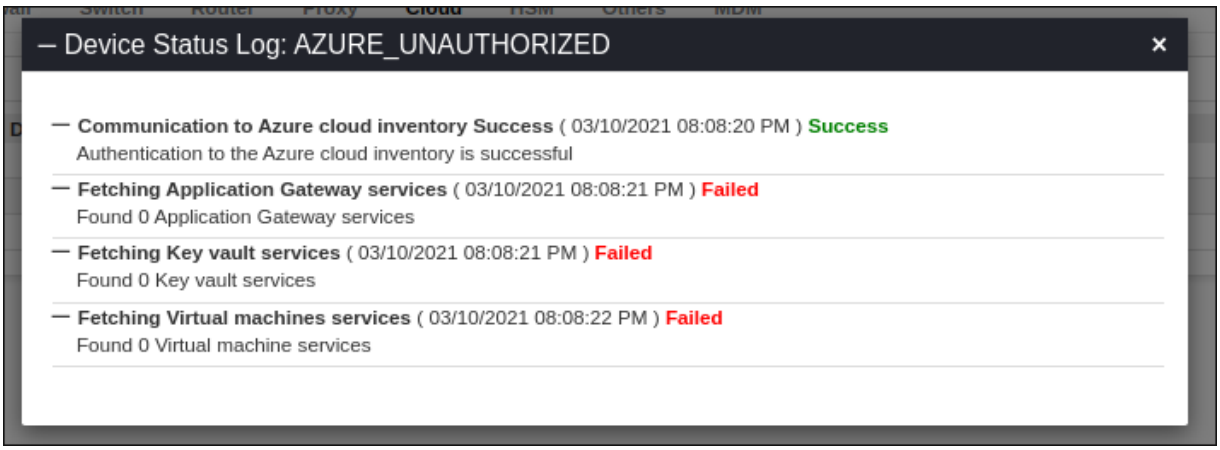
Issues in the Communicating to Azure Cloud

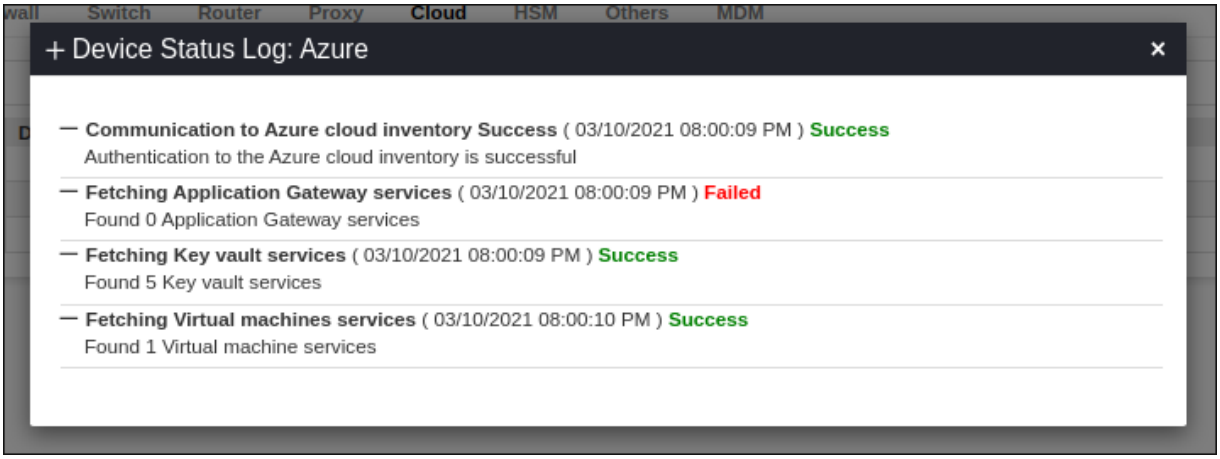
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Status**. The **Device Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.







Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Authentication to the Azure cloud inventory is Failed	Subscription ID, Tenant ID Client ID and Client secret of the Azure cloud account are incorrect. Check each of the provided ID is valid and active.	Login to Azure portal and get all the valid IDs.
Found 0 Key vault services	No Keyvault instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Keyvault instances.
Found 0 Application Gateway services	No Application Gateway instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Application Gateway instances.
Found 0 Virtual machine services	No Virtual Machine instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Virtual machine instances.

Issues in Accessing Azure Cloud

Access Issues might be reproduced when communicating with Azure cloud account, while discovering or fetching the services. These errors can be collected either from logs, API responses, or in the status field for that particular server.

Error Message	Possible Cause	Possible Solution
Connection timeout	Internet / Proxy connection is not provided from the AppViewX node. Firewall settings blocking the REST API request.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution

No Keyvault instances are discovered	Subscription ID doesn't have an appropriate role to access the Azure services.	Check if the following role is assigned for the provided subscription ID in Azure cloud account.
		{
		"properties": {
		"roleName": "AppViewX_KeyVault_Role",
		"description": "",
		"assignableScopes": [
		"/subscriptions/f2689969- 42f6-4fb5-b3be-e3a02e33751c"
		],
		"permissions": [
		{
		"actions": [
		"Microsoft.KeyVault/vaults/read"
		],
		"notActions": [
		],
		"dataActions": [
		"Microsoft.KeyVault/vaults/certificates/import/action",
		"Microsoft.KeyVault/vaults/certificates/create/action",
		"Microsoft.KeyVault/vaults/certificates/update/action",
		"Microsoft.KeyVault/vaults/certificates/read"
		],
		"notDataActions": [
		]
		}
		]
		}}

No Keyvault instances are discovered	Azure Keyvault doesn’t have certificate Get/List permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check if the Certificate management Operations has Get and List permissions.

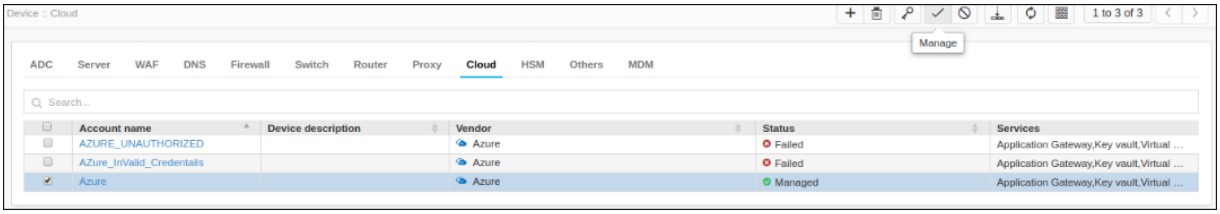
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
No Keyvault instances are discovered	Azure Keyvault Networking blocking the certificate discovery.	Login to Azure portal and navigate to Azure KeyVault -> Networking and check if the If IP is allowed to access the Keyvault in Firewalls and virtual networks.

Issues in Managed Cloud

Issues in the Managed Cloud

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the device and click **Manage**.



Error Messages

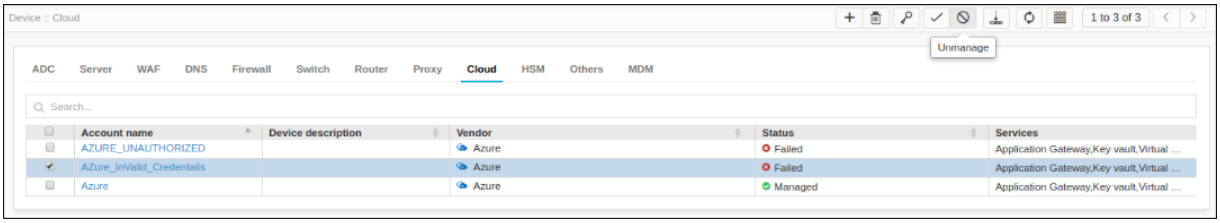
Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Unmanaged Cloud

Issues in the Unmanaged Cloud

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** Page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the device and click **Unmanage**.



Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

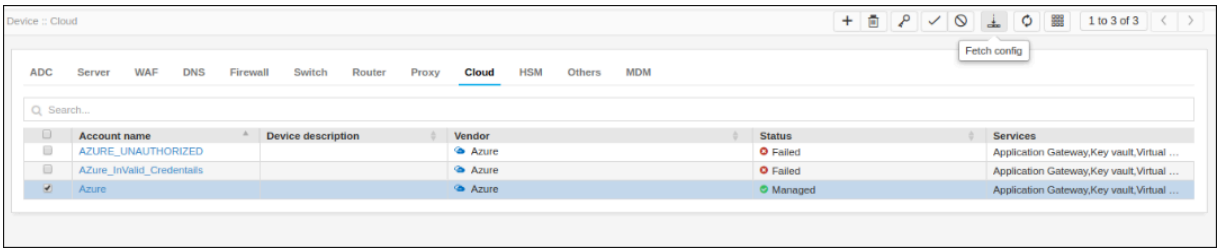
Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Subscription ID, Tenant ID Client ID and Client secret of the azure cloud account is incorrect.	Login to Azure portal and get all the valid IDs. Check if each of the provided ID is valid and active.

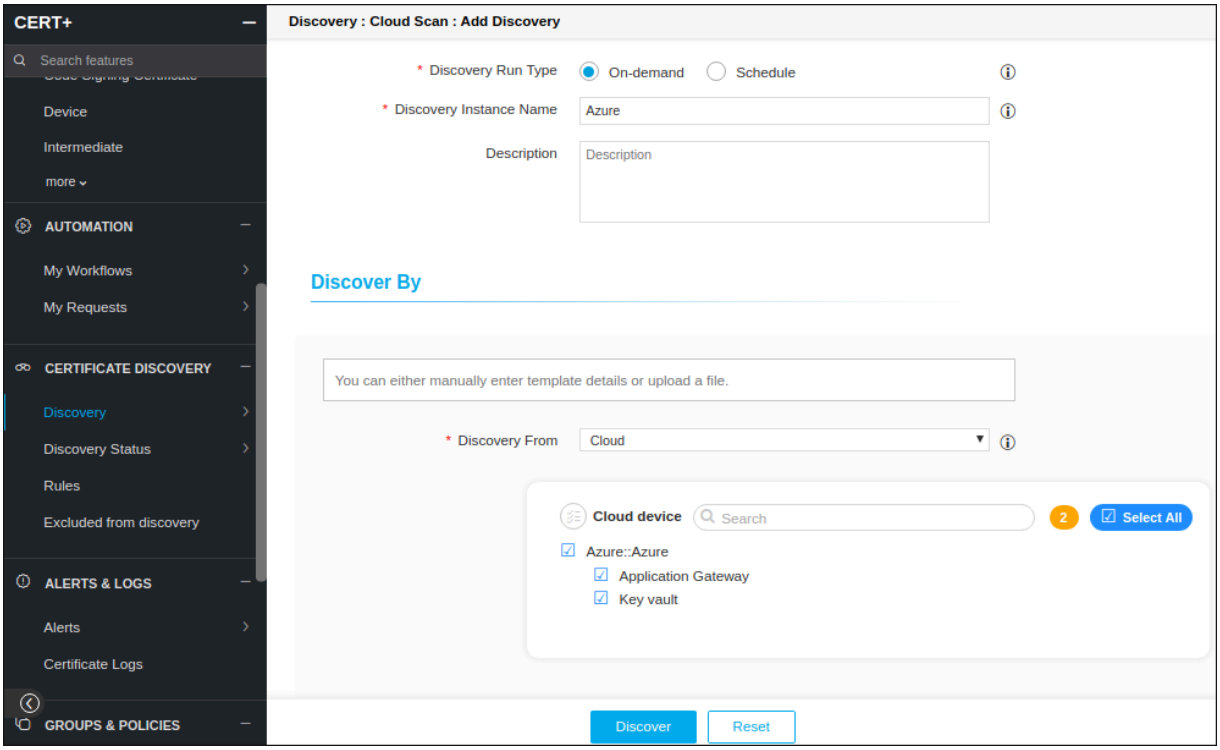
Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Cloud Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed cloud accounts, the cloud account should be managed under the AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name not given or length is less than 2 characters. 2. Interval between batches info. is	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	missing when execution type is sequential.	
Please select a devices	No cloud account is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Discovery Status Failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
No Certificates discovered from Azure KeyVault	Keyvault instance is not discovered from Azure cloud account.	Check device status in device addition page for Azure keyvault, if we have a Keyvault instance discovered count.
No Certificates discovered from Azure KeyVault	Azure Keyvault doesn’t have certificate Get/List permissions in access policies	Login to azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Get and List permissions (refer below snapshot)
No Certificates discovered from Azure KeyVault	Azure Keyvault Networking blocking the certificate discovery	Login to Azure portal and navigate to Azure KeyVault -> Networking and check the Firewalls and virtual networks If IP is allowed to access the Keyvault. (refer below snapshot)

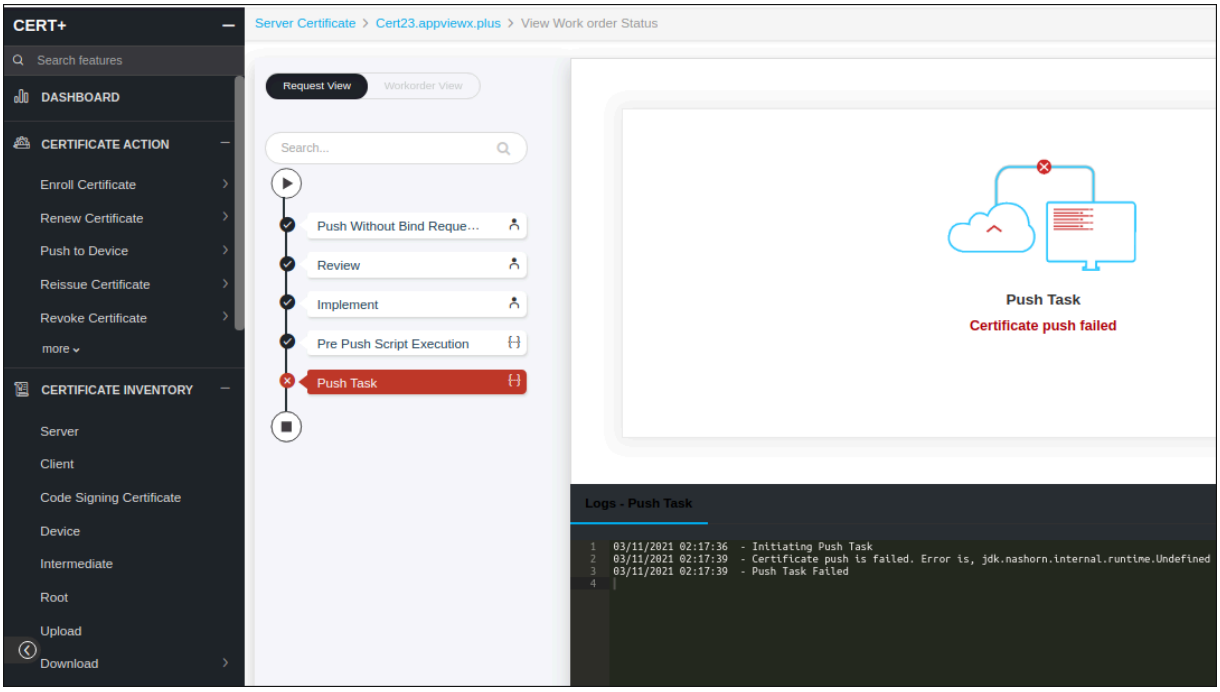
Issues in Certificate Import

Issues in the Certificate Import

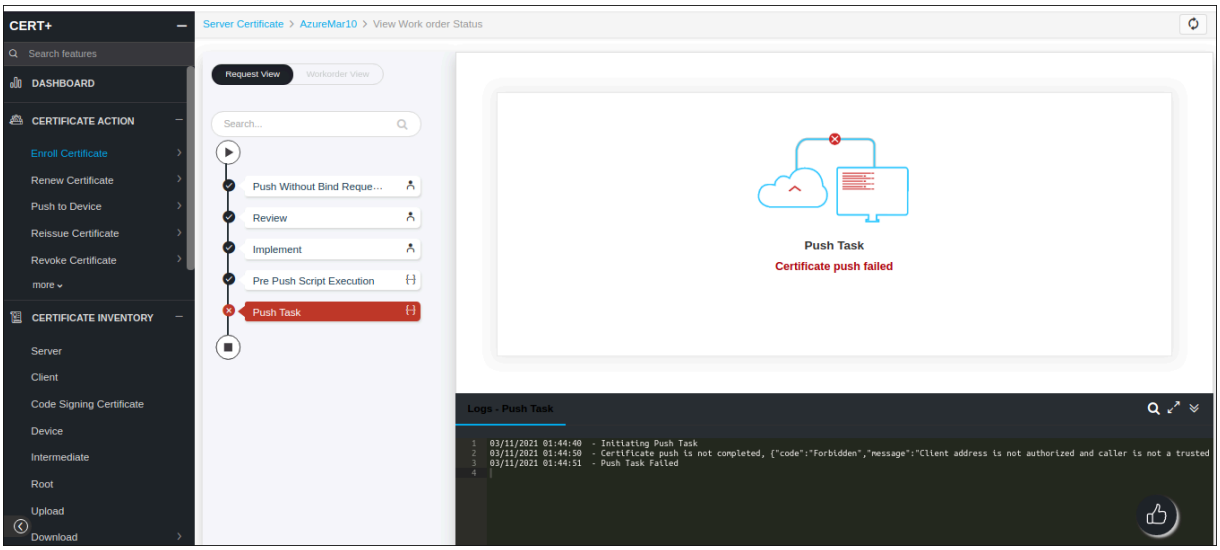
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

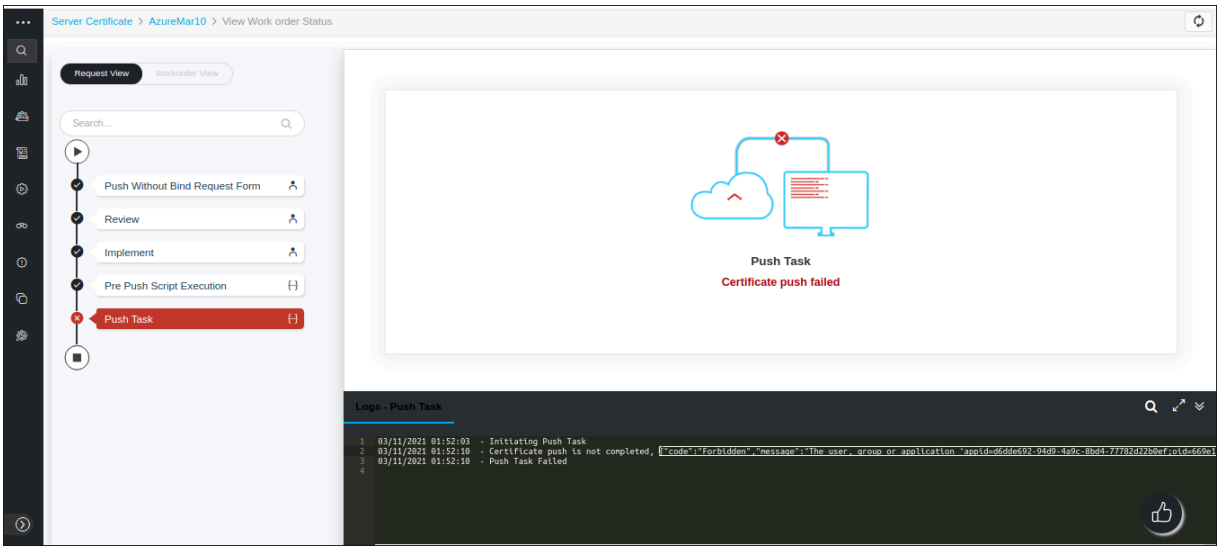
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Inventory**, select **Cloud**.
4. Create an **Application connector** for Azure
5. **Push** the certificate to the device



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state.	1. Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in the enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate push failed. Error is, jdk.nashorn.internal.runtime.Undefined	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Certificate push failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
{"code":"Forbidden","message":"The user, group or application 'appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;numgroups=0;iss=https://sts.windows.net/e5f90d85-3cdf-457d-a611-1aca82b0843b/' does not have Certificates import permission on key vault 'keyvault-type-1;location=eastus'. For help resolving this issue, please see https://go.microsoft.com/fwlink/?linkid=2125287","innererror":{"code":"ForbiddenByPolicy"}}	Azure Keyvault instance doesn't have certificate Import permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Import permission.
{"code":"Forbidden","message":"Client address is not authorized and caller is not a trusted service.\r\nClient address: 125.21.72.158\r\nCaller: appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;iss=https://sts.windows.net/e5f90d85-3cdf-457d-	Azure Keyvault Network blocking the Certificate Push.	Login to Azure portal and navigate to Azure KeyVault ->

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
a611-1aca82b0843b/\r\nVault: keyvault-type-2;location=eastus","innererror": {"code":"ForbiddenByFirewall"}}		Networking and check the Firewalls and virtual networks if IP is allowed to access the Keyvault.

Troubleshooting CLOUD - Common Functionality

- Introduction
- Issues in Cloud Addition using AppViewX UI - AWS
- Issues in Cloud Addition using AppViewX UI - Azure, GCP
- Issues in Communicating to Cloud accounts
- Issues in Managed Cloud Account
- Issues in Unmanaged Cloud Account
- Issue in Discovery

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using cloud functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, and other actions available with the cloud module.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	rom AppViewX Version 11.1

Supported Devices

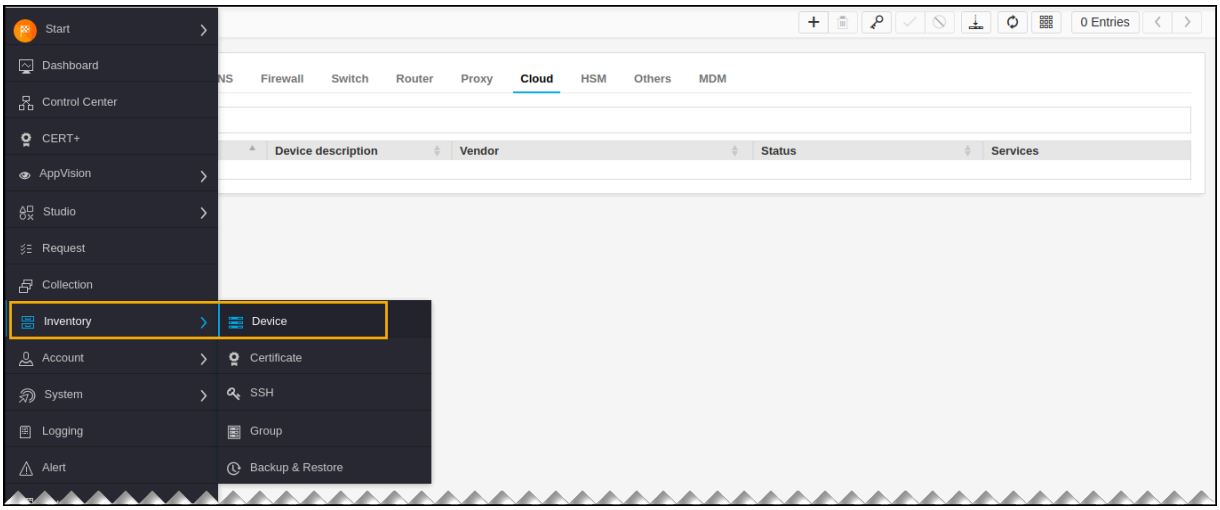
Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

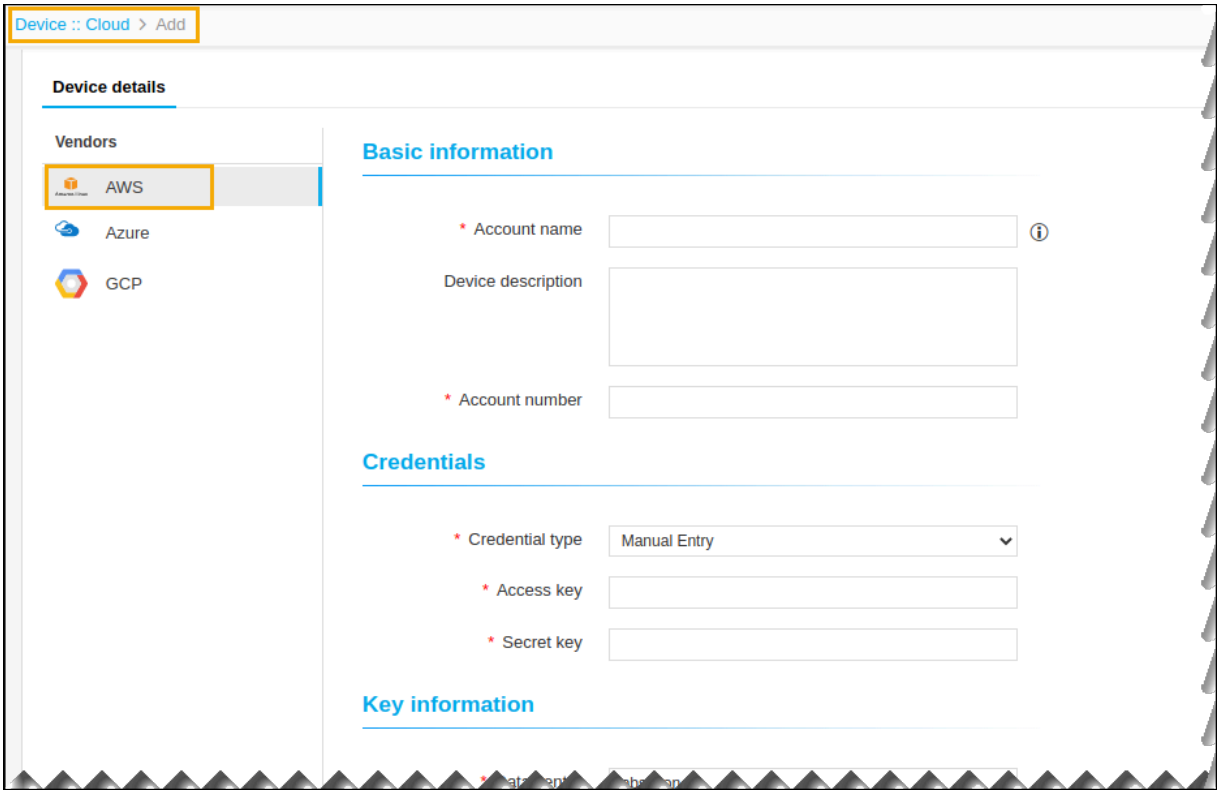
Issues in Cloud Addition using AppViewX UI - AWS

Issues in the Cloud Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details** Section on the left, Click **AWS**.
7. Fill in the appropriate details.
8. Select services to be managed.
9. Click **Fetch regions**.
10. Fill in additional attributes and click **Save** in the footer.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in the inventory.	Check the Account name, it should be unique.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

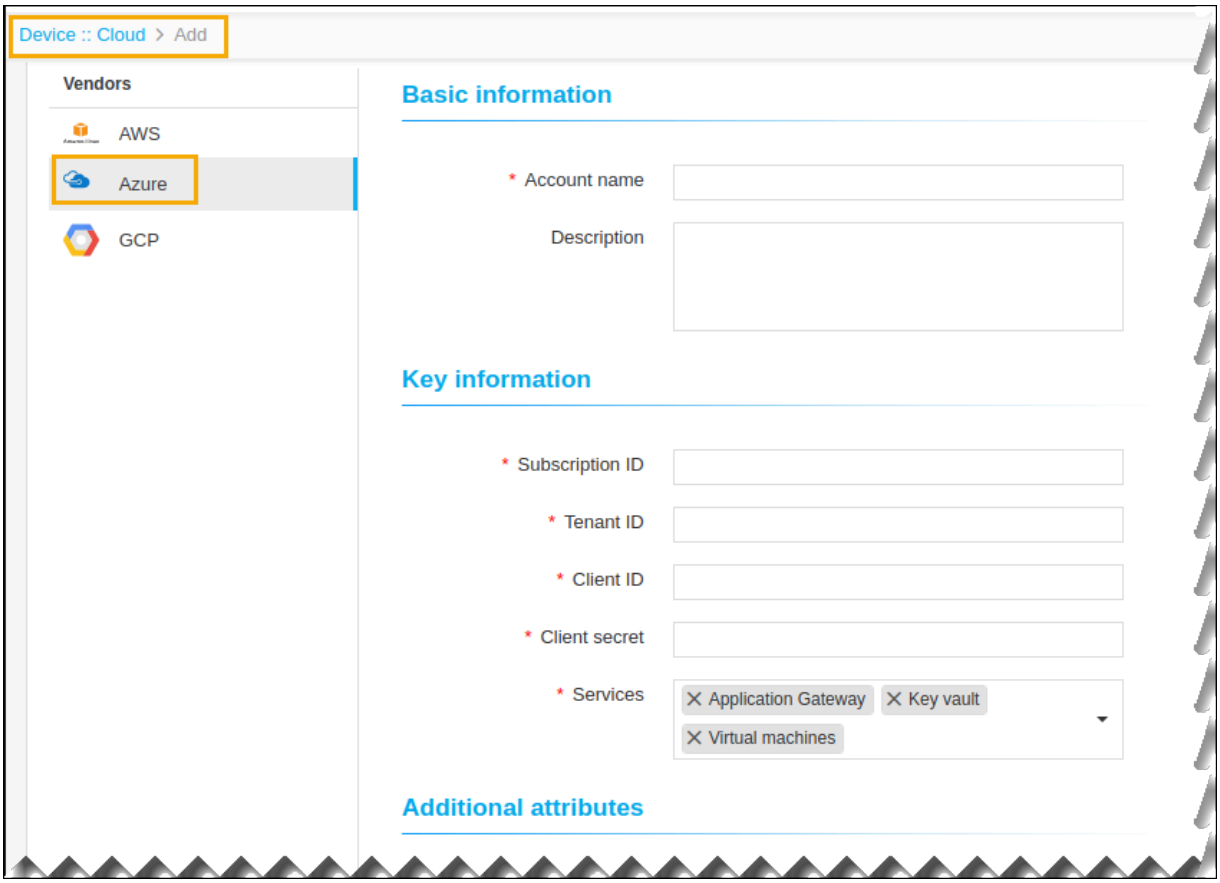
Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please provide valid credentials	The credentials provided are invalid/ has no access to fetch regions	Provide valid credentials/ credentials with needed access

Issues in Cloud Addition using AppViewX UI - Azure, GCP

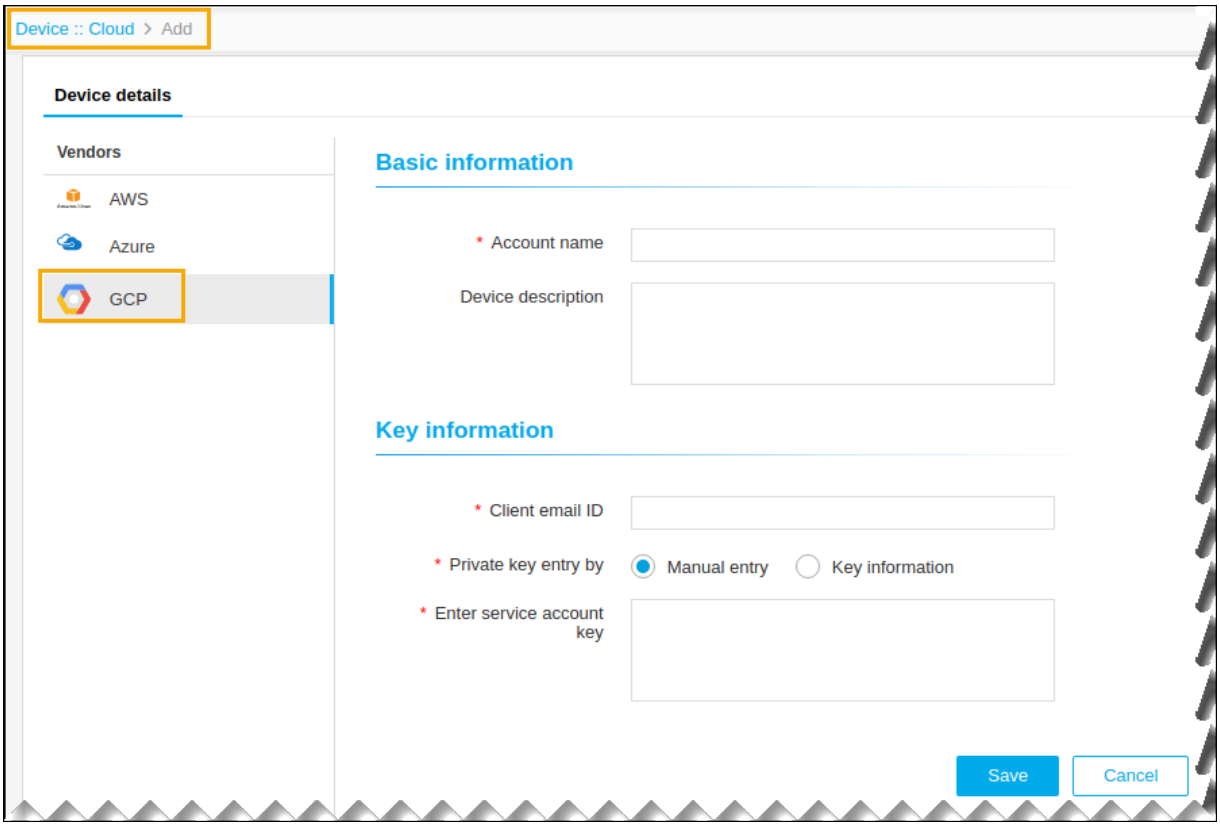
Issues in the Cloud Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Azure/GCP**.
7. Fill in the appropriate details.
8. Select **services** to be managed.
9. Click **Fetch regions**.
10. Fill in additional attributes and click **Save** in the footer.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Error Messages

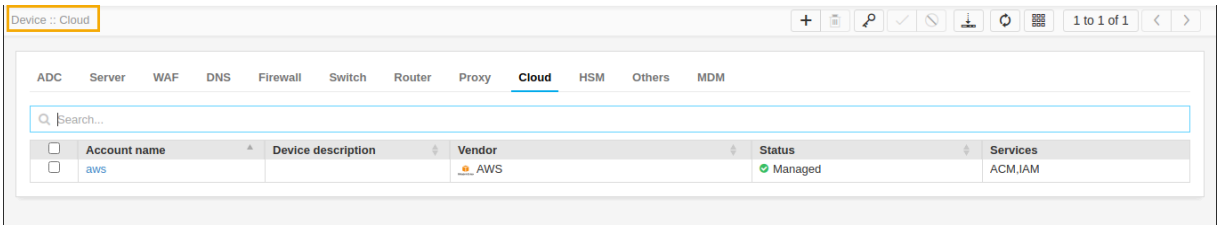
Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

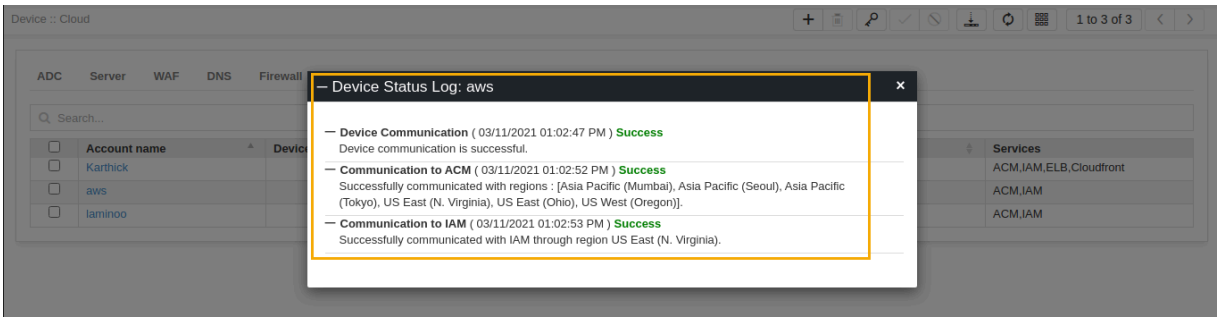
Issues in Communicating to Cloud accounts

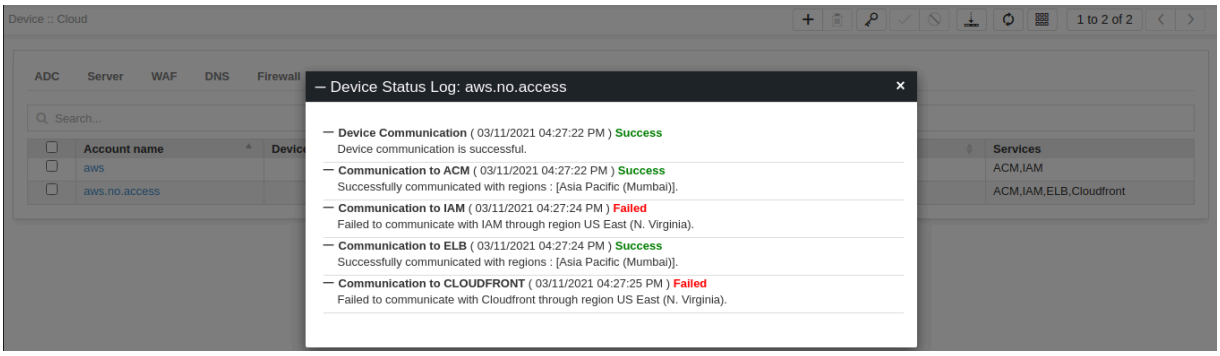
Issues in the Communicating to Cloud Accounts

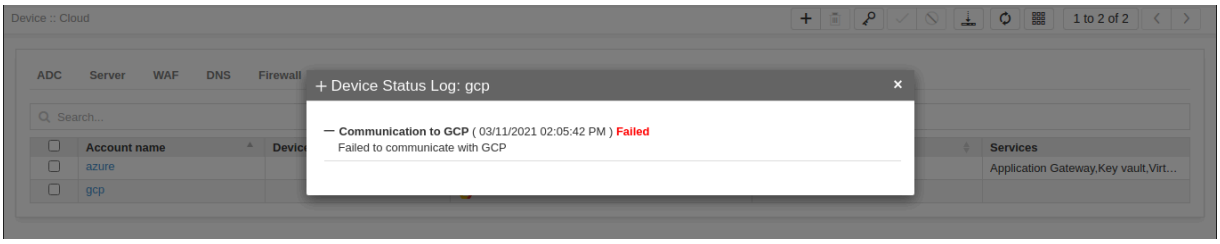
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Cloud** Tab.
5. Select the **Device**, click **Status**. The **Device Status** is displayed.

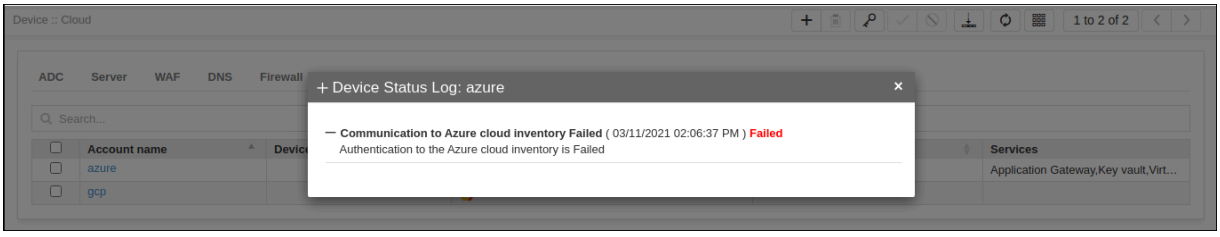
Copyright © 2024 AppViewX, Inc. All Rights Reserved.











Copyright © 2024 AppViewX, Inc. All Rights Reserved.

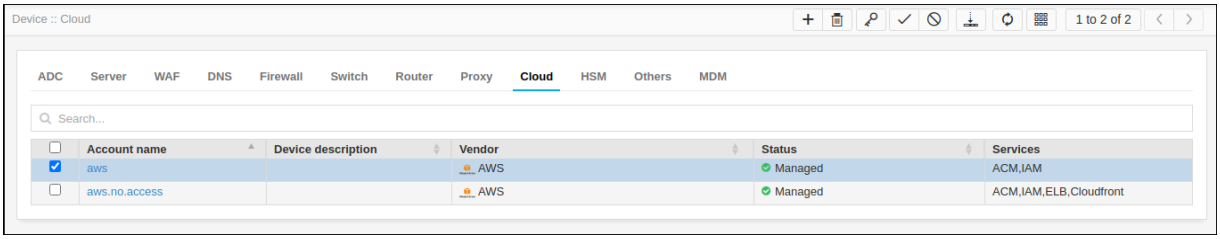
Error Messages

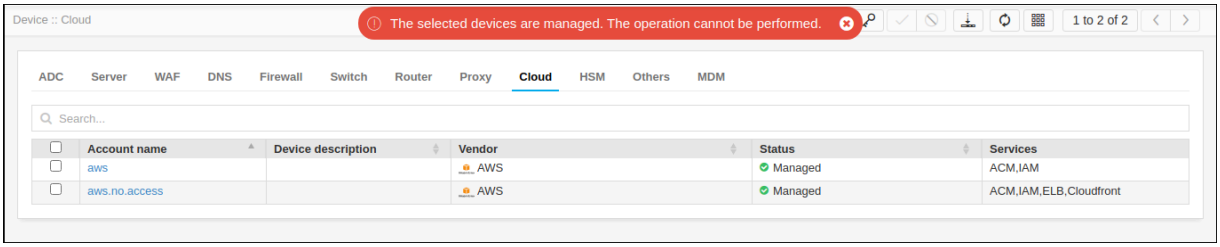
Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Credentials provided are invalid/ credentials do not have the required access.	Validate the credentials and Check if credentials are provided required access.
Failed to communicate with GCP	Unable to connect to the endpoint.	Check if the node can reach the endpoint via proxy/internet as configured.
Failed to communicate with <SERVICE> through region <REGIONS>.	Credentials do not have required access	Provide credentials the required access

Issues in Managed Cloud Account

Issues in the Managed Cloud Account

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**. The **Device Management** Page is displayed.
4. On the **Device Management** Page, click **Cloud** Tab.
5. Select the device and click **Manage**.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

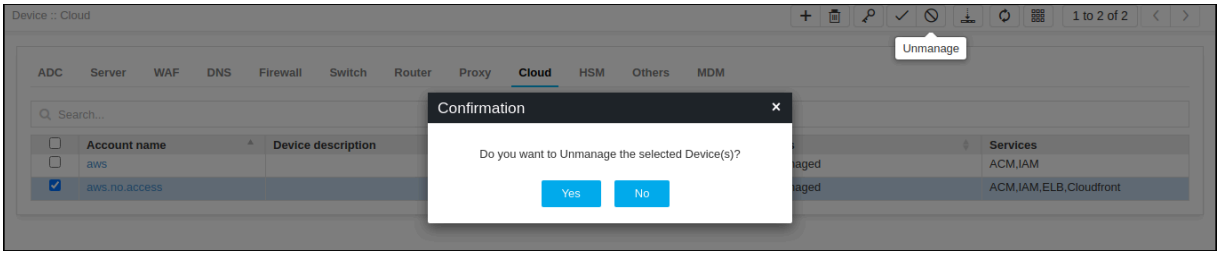
Error Messages

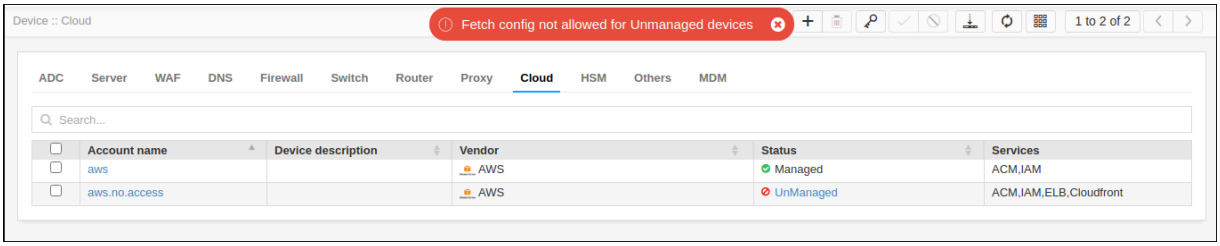
Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	The device cannot be managed because it is already in the managed state.	Unmanage the device(s) before performing the action.

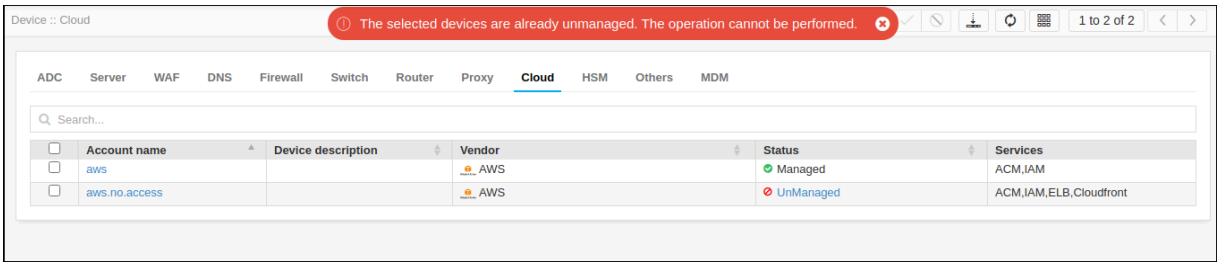
Issues in Unmanaged Cloud Account

Issues in the Unmanaged Cloud Account

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Inventory** and click **Device**. The **Device Management** Page is displayed.
4. On the **Device Management** Page, click **Cloud** Tab.
5. Select the device and click **Unmanage**.







Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	The device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) before performing the action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in a managed state.	Manage the device(s) in an unmanaged/in-progress state before performing an action.

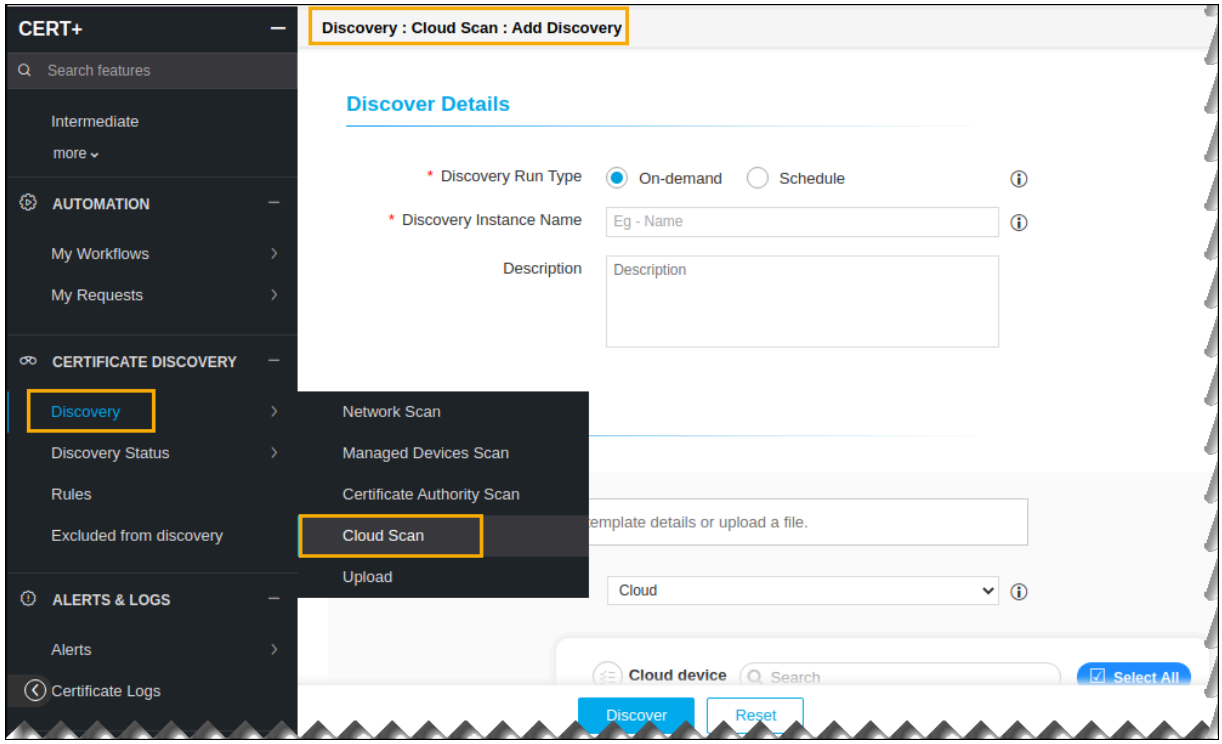
Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Cloud Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed cloud accounts, the cloud account should be managed under the AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. The Discovery name is not given or the length is less than 2 characters. 2. The interval between batches info is missing when the execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

- Overview
- Troubleshooting Apache Linux
- Troubleshooting Barracuda WAF
- Troubleshooting Cisco ASA Firewall
- Troubleshooting Cisco CallManager
- Troubleshooting Common Functionality of Servers
- Troubleshooting Data Power Server
- Troubleshooting F5 WAF
- Troubleshooting Fortigate Firewall
- Troubleshooting HP ILO
- Troubleshooting IBMClient Linux
- Troubleshooting IBMClient Windows
- Troubleshooting Imperva WAF
- Troubleshooting Linux JBoss Server
- Troubleshooting Microsoft Enterprise CA
- Troubleshooting Microsoft Tomcat
- Troubleshooting MQServer Linux
- Troubleshooting MQServer Windows
- Troubleshooting MS SQL Windows
- Troubleshooting Nginx Server
- Troubleshooting NginxPlus ADC
- Troubleshooting Paloalto Firewall
- Troubleshooting Panorama Firewall
- Troubleshooting RabbitMQ Server
- Troubleshooting Rapid SB Server Inventory
- Troubleshooting Rapid SB Linux Server
- Troubleshooting Tomcat Linux
- Troubleshooting Weblogic Linux
- Troubleshooting Websphere Linux

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Troubleshooting Websphere Windows
• Troubleshooting Windows Apache Server
• Troubleshooting Windows JBoss Server
• Troubleshooting Windows Weblogic Server

Overview

This section of the guide will help you tackle the issues encountered while using the functionalities of servers, firewalls, WAF, and Rapid SB Connectors. It deals with common functionalities of these devices at the beginning of each guide and the rest of the guide deals with functionalities of specific devices. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

Troubleshooting Apache Linux

• Overview
• Issues in Device Addition using AppViewX UI
• Issues in Communicating to the Server
• Issues in CSR Generation
• Issue in Access
• Issues in Fetch Config
• Issue in Discovery
• Issues in Push and Rollback

Overview

This document helps you troubleshoot the common problems that you might encounter when using Apache Linux functionalities. This guide will give more troubleshooting processes on issues related to Apache Linux server. The issues are device addition, communication to the server, CSR generation, access to server, fetch configuration, discovery along with push and rollback.

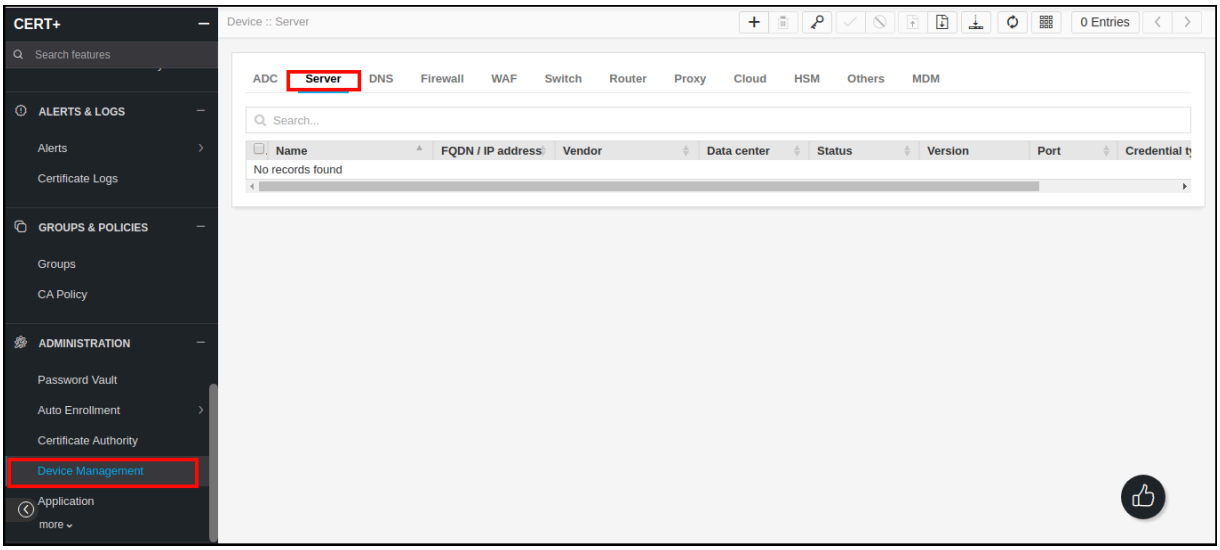
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

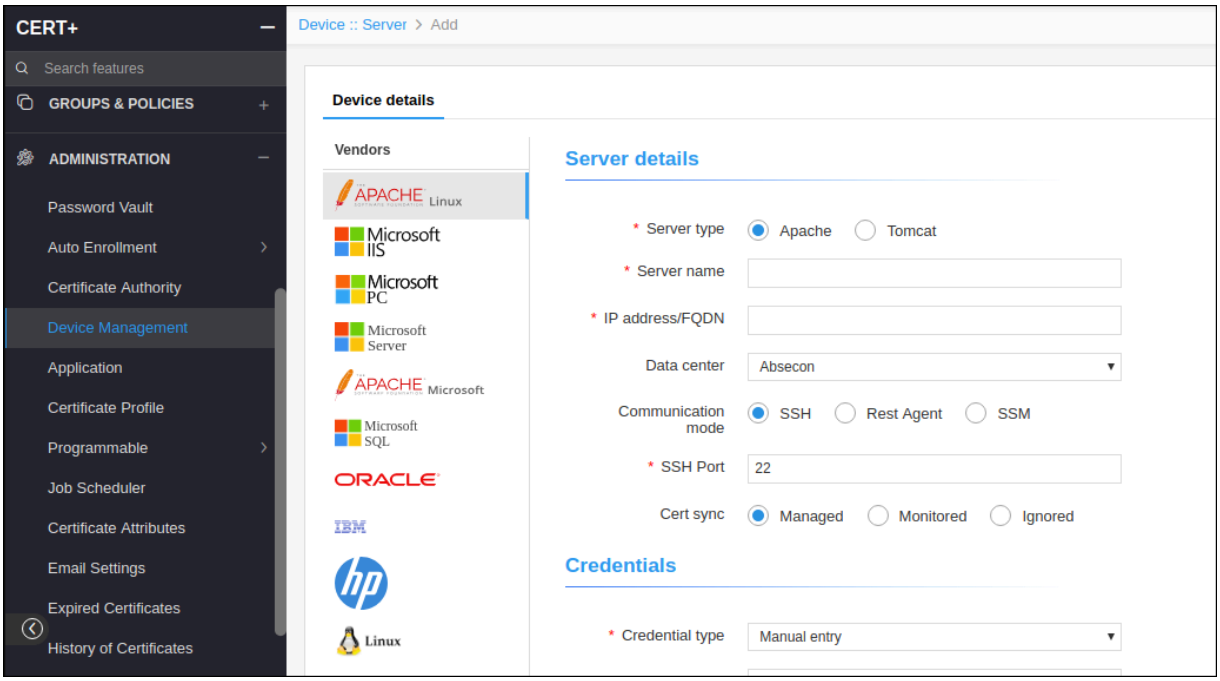
Issues in Device Addition using AppViewX UI

Issues in the Device Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the Device Management page, click Server Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details** Section on the left, click **Apache Linux**.
7. Click **Server type** as **Apache**.
8. Fill in the appropriate details.
9. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

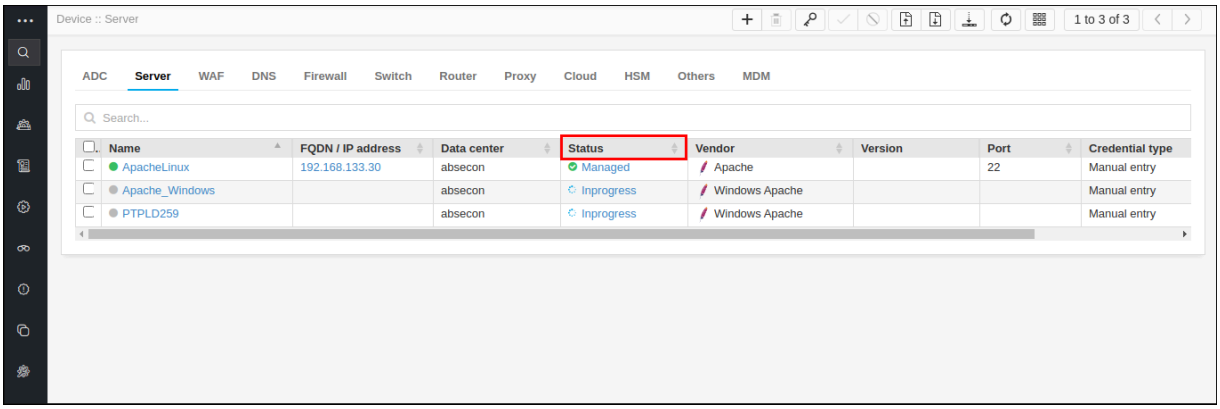
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

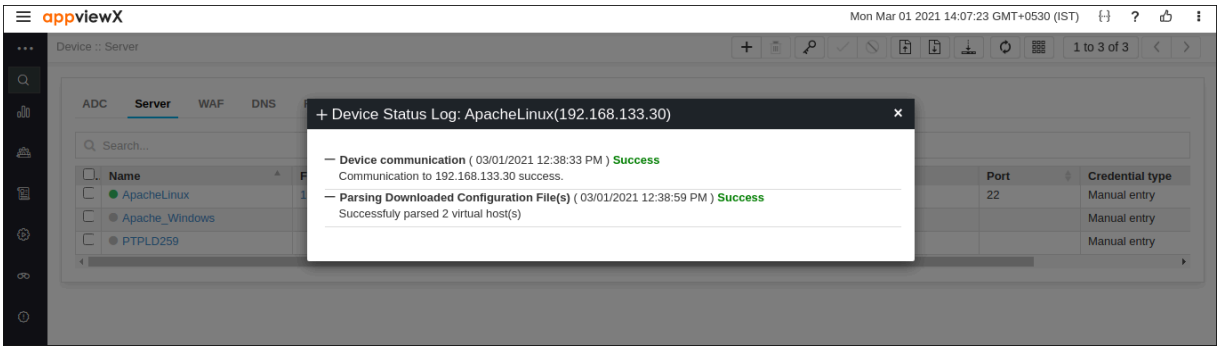
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

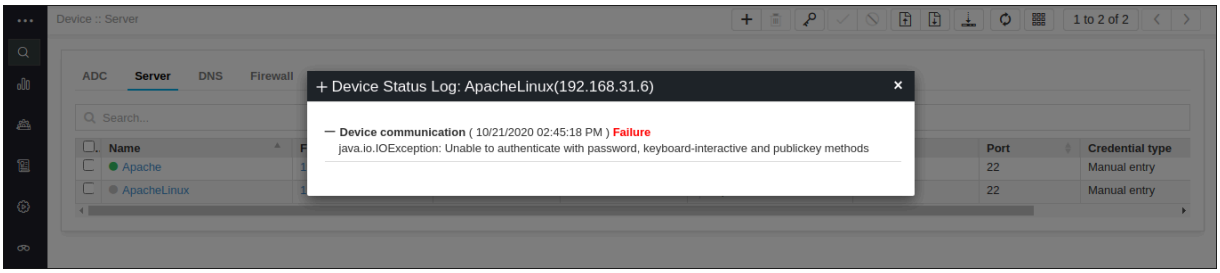
Issues in Communicating to the Server

Issues in Communicating to the Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.







Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device ip/fqdn as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Ip is not reachable/invalid.	Invalid credentials	Kindly check the credentials provided.
	IP is not reachable	Kindly check if IP is pingable or not and make it up and running.
	IP is blocked by the firewall	Kindly check firewall settings.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Communication Failed	Username or password may be invalid	Check and provide the correct username and password.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods.	Authentication Failure	Provide correct credentials for authentication. Make sure SSH is enabled on the given server.
Linux rest agent communication failed.	Rest agent running on the destination machine might be down.	Please check the status of the rest agent in the destination machine.

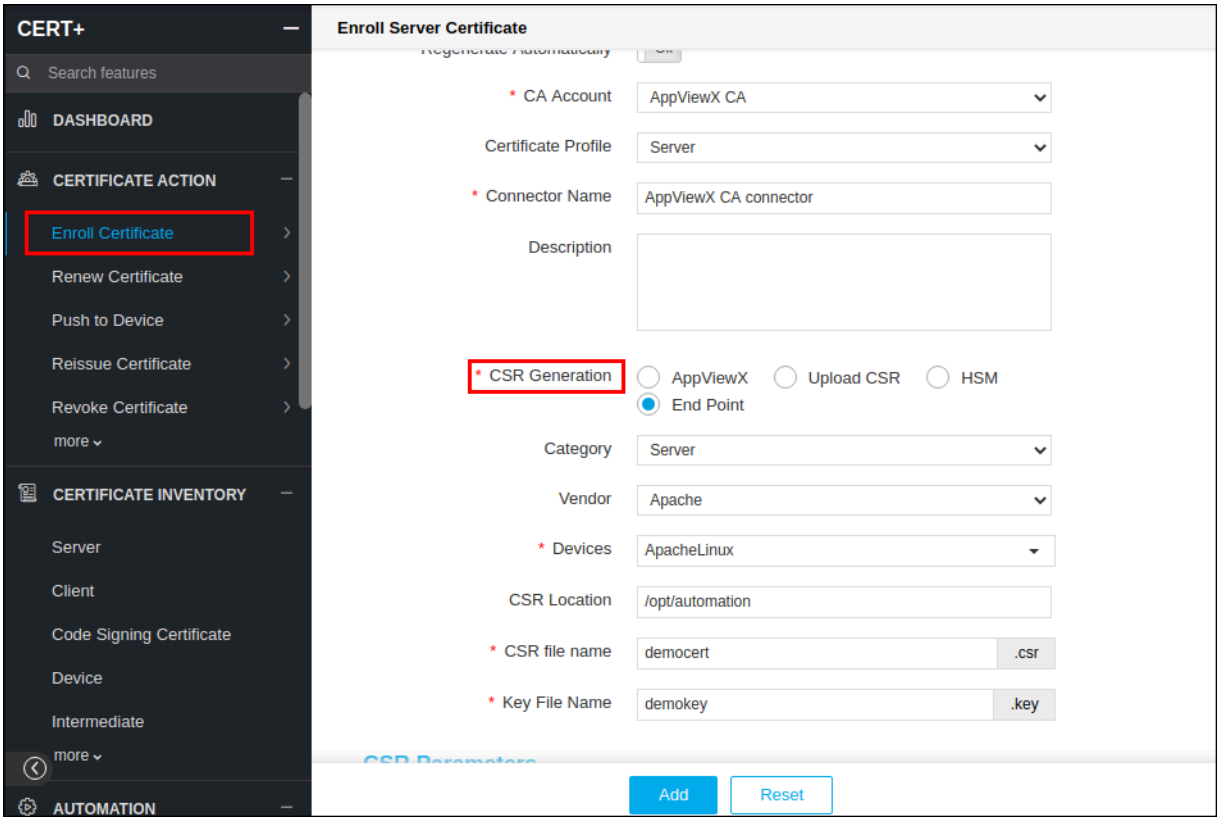
Issues in CSR Generation

Issues in the CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the **Category** from the dropdown.
7. Click the correct **Vendor** from the dropdown. A list of devices will be generated in the **Devices dropdown**.
8. Select the **Apache** device for generating **CSR**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. Click **Add**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issue in Access

Access Issues occur while communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	File might not be present in the avx environment.	Check whether someone deleted the file from AppViewX environment.
	user might not have permission to read in the given source location.	Verify if read permission is given for the location.
	Device communication might not be established when service has started.	Verify the device connection and restart the service.

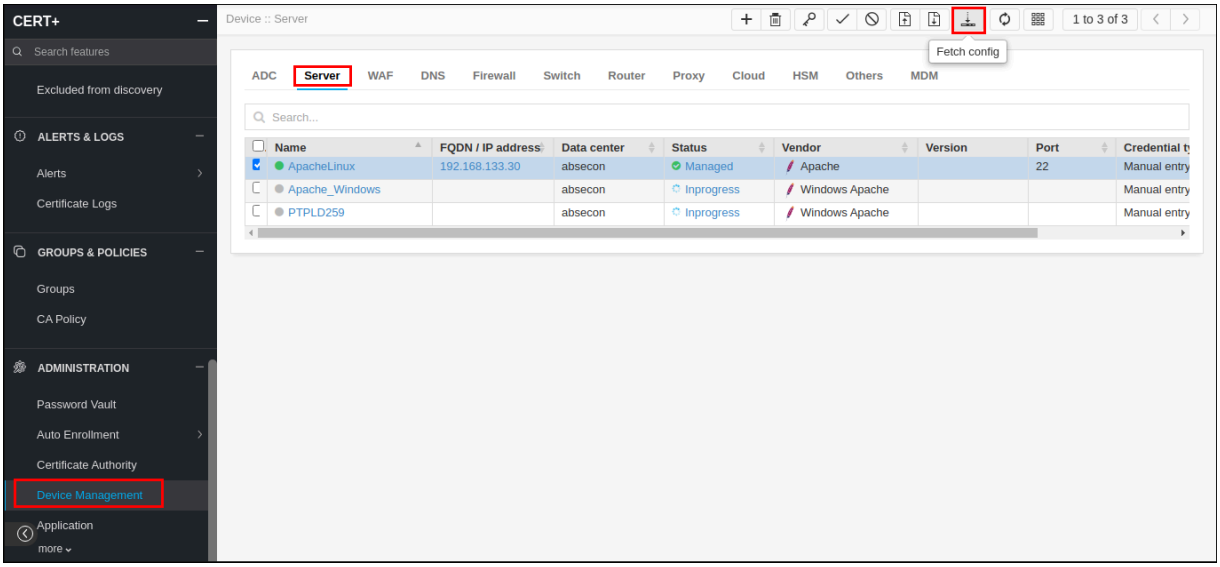
Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Parsing apache configuration failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
	AppViewX is not able to read/ parse the Config files from the server.	Check if the server has proper config files related to Apache Server and AppViewX has proper read permissions.

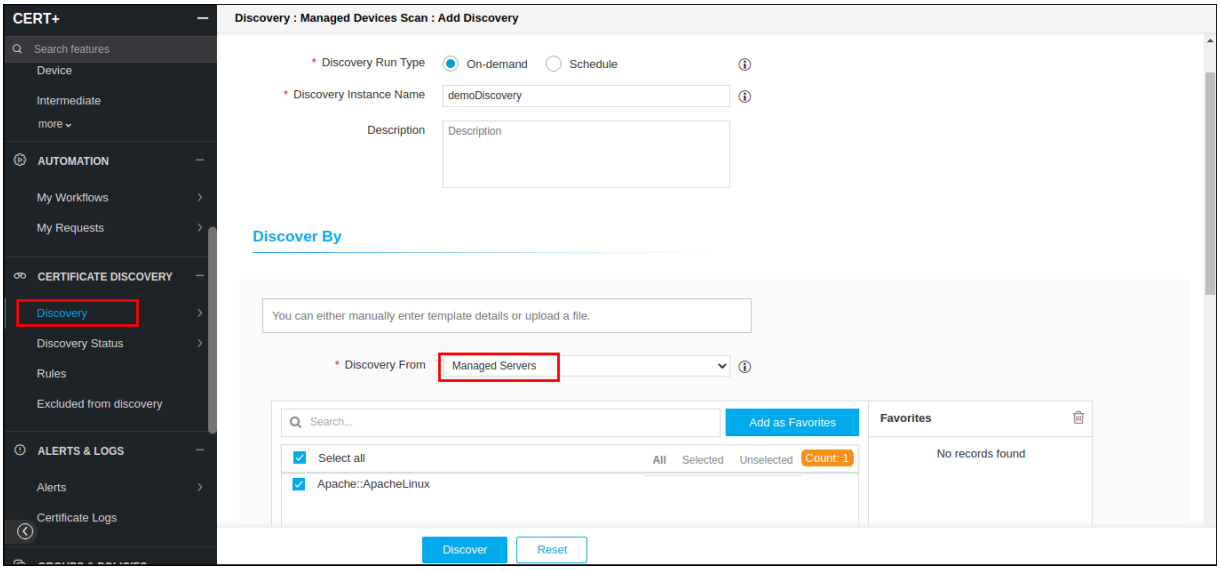
Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

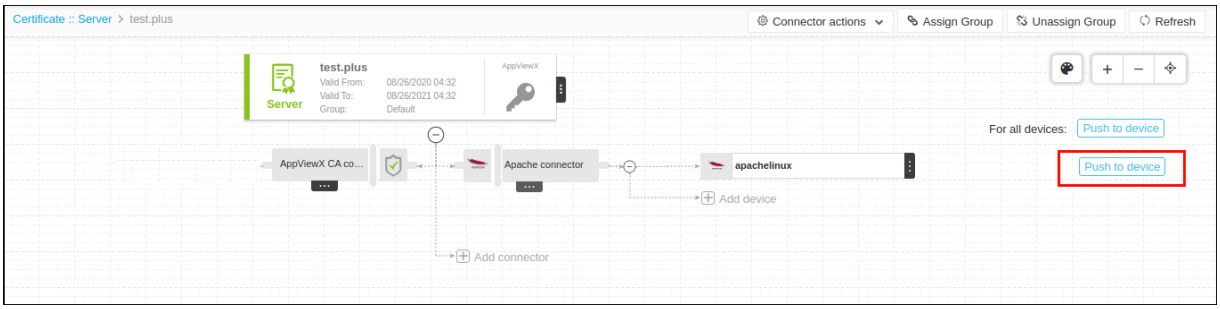
Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

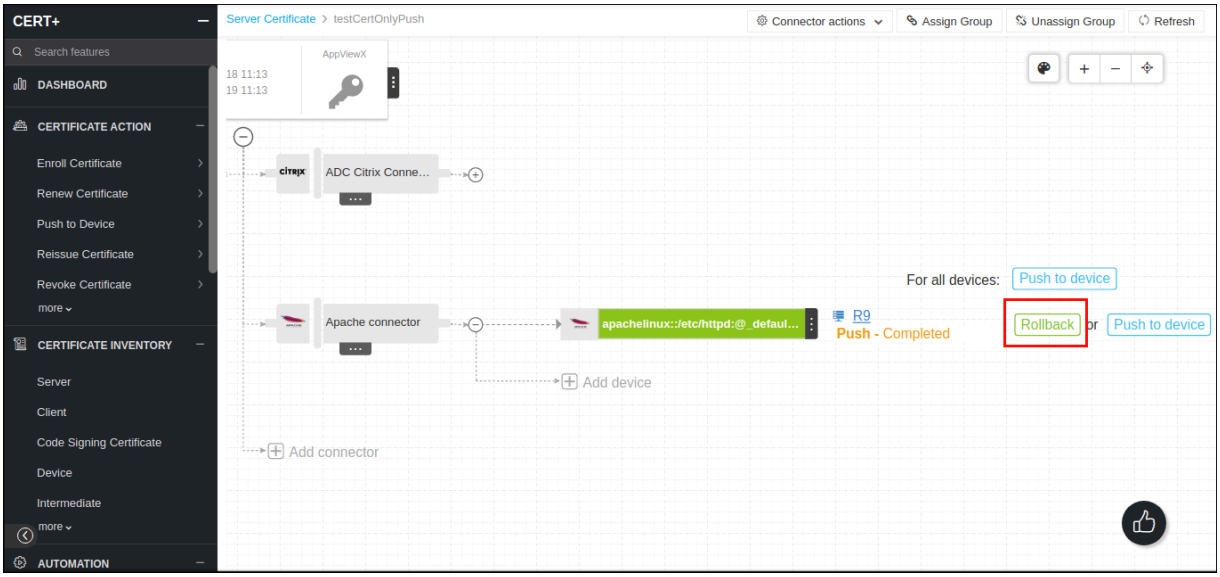
Issues in Push and Rollback

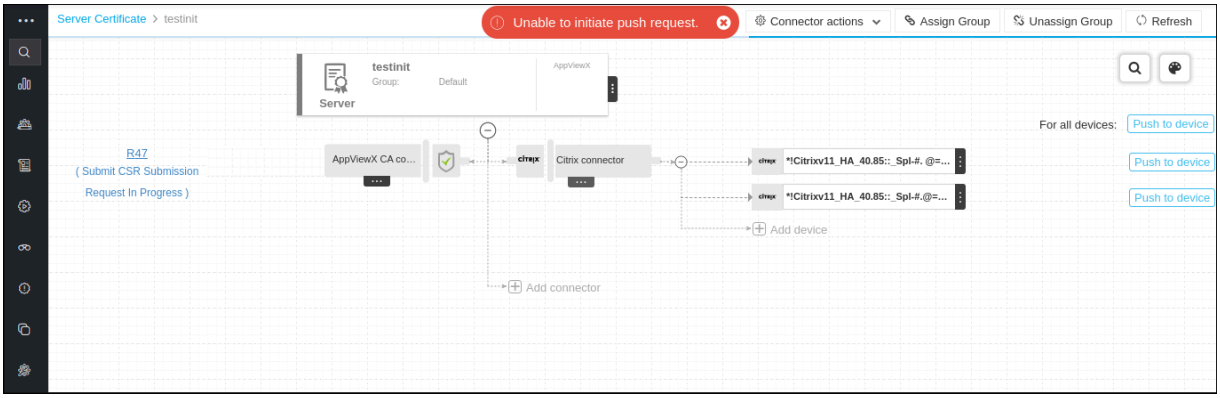
Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **server**.
4. On the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.







Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Barracuda WAF

- Overview
- Issues in Device communication
- Issue in Discovery
- Issues in Certificate Push

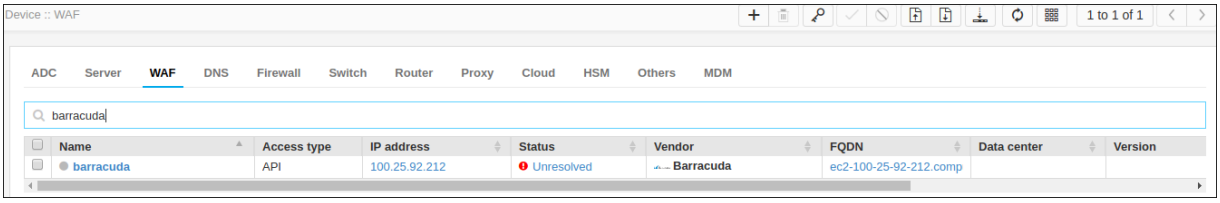
Overview

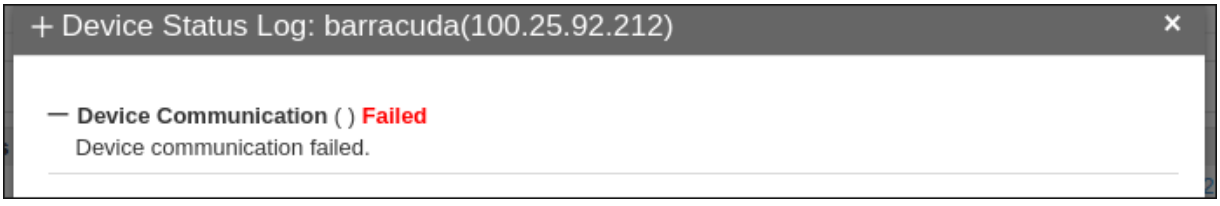
This section helps you deal with the various issues faced by you during the use of Barracuda WAF functionalities.

Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select a **Barracuda Device**, click **Status**. The **Device Communication Status** is displayed.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

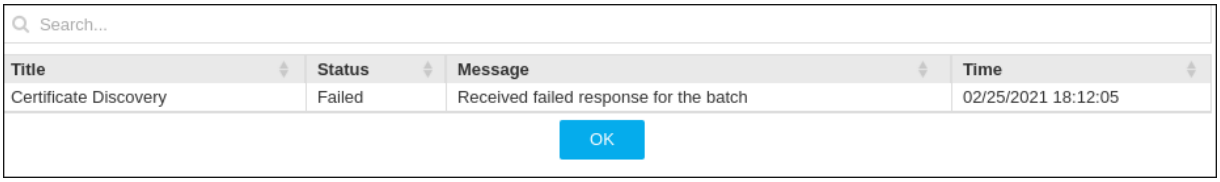
Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. The given IP/FQDN and Port may be incorrect. 3. Device not reachable.	1. Check and input the correct credential. 2. Check and input the correct IP/FQDN and Port. 3. Ensure the device is up and accessible.

Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.
5. From the dropdown of **Discovery From**, select **Managed WAFs**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

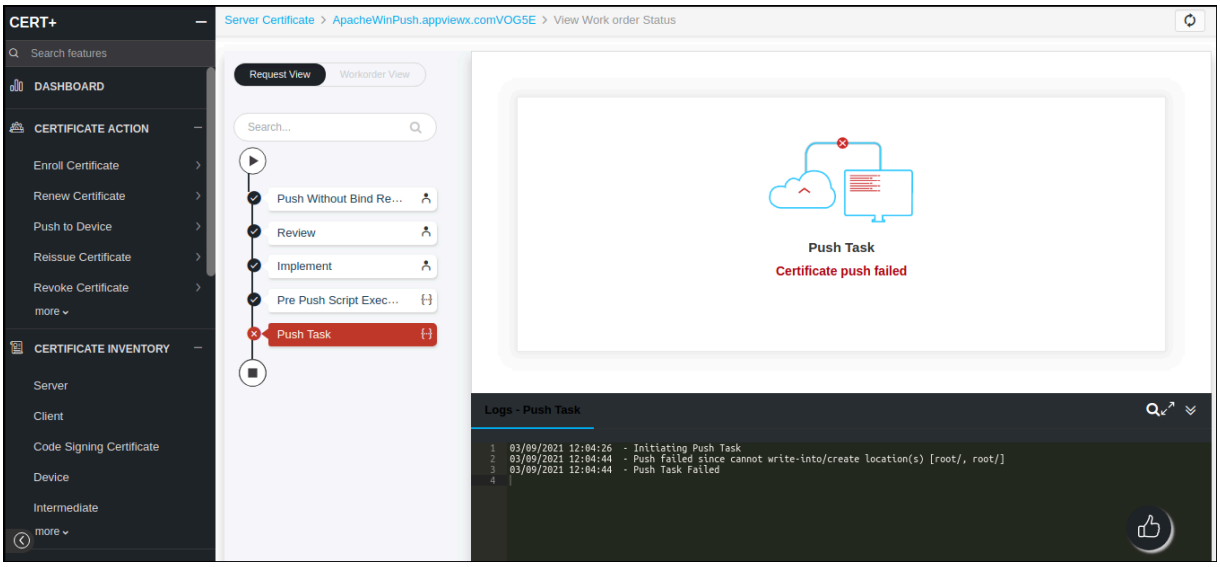
Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible. 2. No valid certificates available.	1. Ensure target device is up and running. 2. Check the device has valid certificate files.

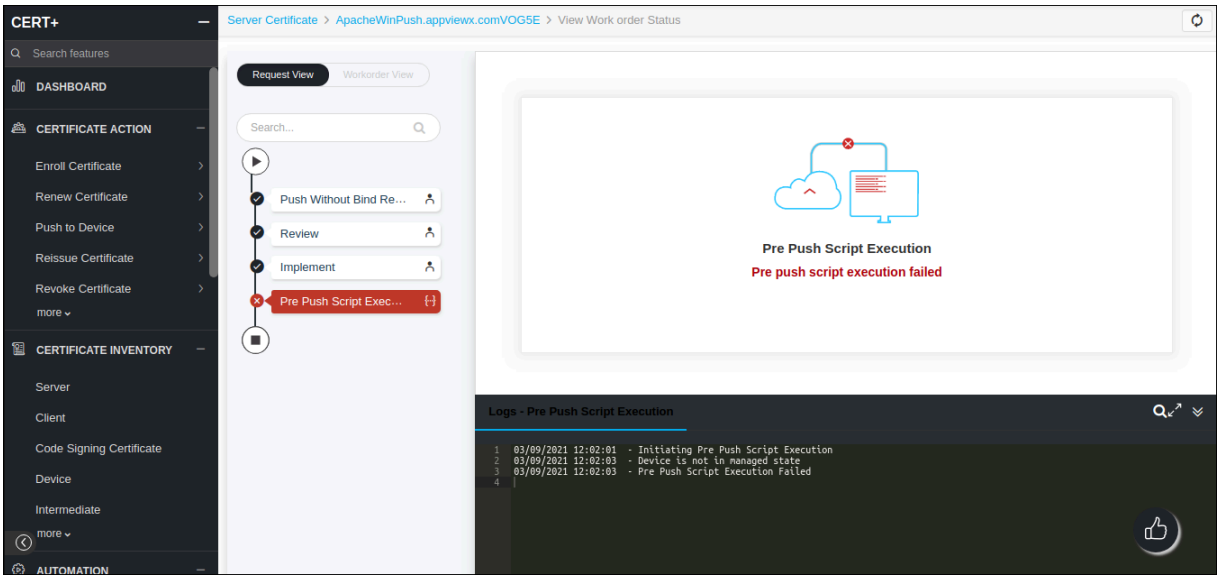
Issues in Certificate Push

Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page will be displayed.
3. From the left pane, expand **Certificate Inventory** menu and select **Server**. The **Server Certificate** page will be displayed.
4. Select any **Barracuda server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector actions**, select **Add App Connector**.
6. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Push failed due to invalid certificate	Push failed when pushing a certificate without key.	Ensure the certificate matches with the key associated in the device on pushing without the key file.
Device is not in managed state	Device is not available in “managed list”.	Please check the device status in device inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Cisco ASA Firewall

- Overview
- Issues in Server Addition using AppViewX UI
- Issues in Device communication
- Issue in Discovery
- Issues in Certificate Push
- Issues in Certificate Bind

Overview

This section will guide you to overcome the various issues faced by you during the use of Firewall Cisco ASA and its various functionalities.

Issues in Server Addition using AppViewX UI

Issues in the Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Cisco**.
7. Fill in the appropriate details.
8. Click **Add**.

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

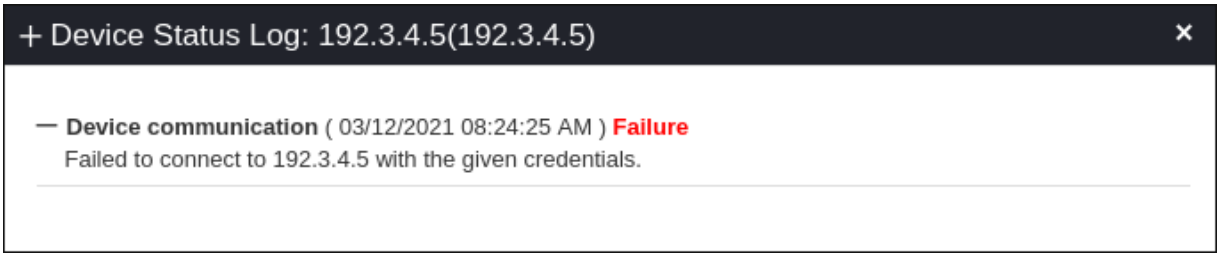
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the Device, click **Status**. The **Device Communication Status** is displayed.





Error Messages

Error Message	Possible Cause	Possible Solution
Failed to connect to <device name> with the given credentials.	1. Device unreachable. 2. Invalid credential. 3. Invalid port.	1. Kindly check if the given IP/FQDN is reachable. 2. Kindly check the credentials provided. 3. Kindly check the port and firewall settings. 4. Kindly ensure the CiscoASA version is supported by AppViewX and has proper privilege to login.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Interfaces are not associated with any trustpoints.	Kindly ensure the interfaces are bounded with required trustpoints. Command to verify SSL-config: show running-config SSL

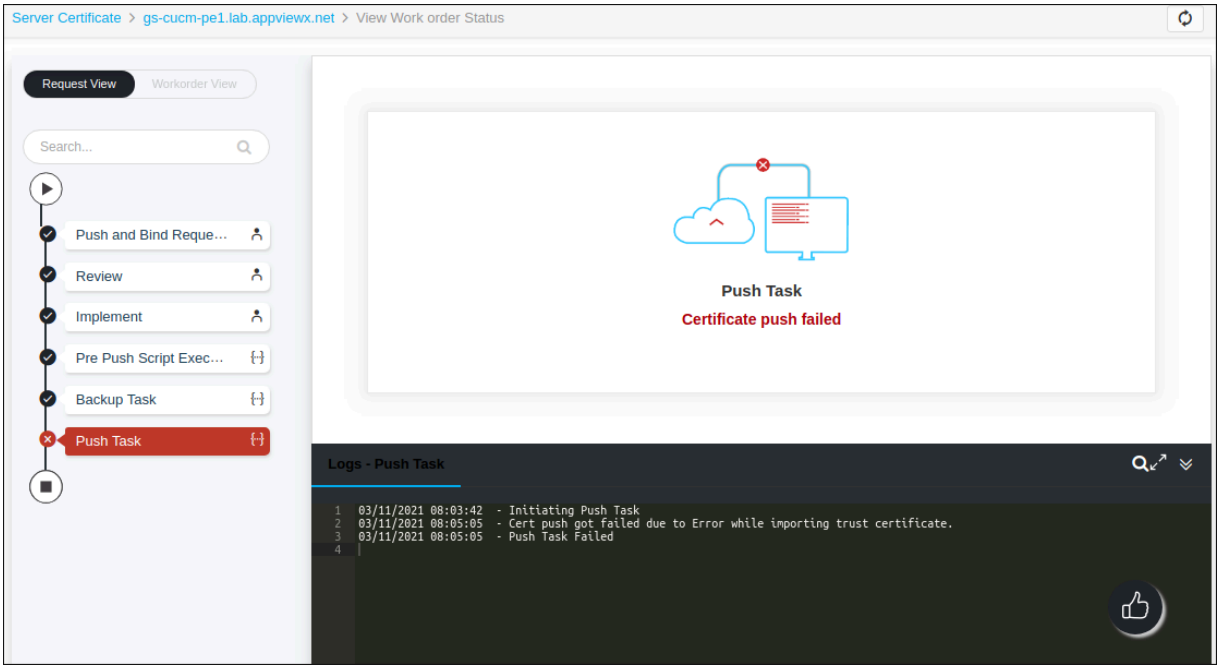
Issues in Certificate Push

Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Cisco ASA Firewall**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Push the certificate to the device.



Error Messages

Error Message	Possible Cause	Possible Solution
Certificate push failed due to Unsupported bit length.Please provide valid one.	Unsupported bit length.	Kindly ensure the bit length of certificate is supported by ciscoASA
Cert push got failed due to ERROR: Import PKCS12 operation failed	Issues in creating trustpoints	Kindly ensure that the trust points get created successfully.

Issues in Certificate Bind

Issues in the Certificate Bind

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Cisco ASA Firewall**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Edit Connector**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. On the **Edit Connector**, select **interfaces** to be associated with the trust point.
7. Push the certificate to the device.

Error Messages

Error Message	Possible Cause	Possible Solution
Certificate bind failed due to invalid interface name or error while communicating with device.	Invalid trustpoint.	Kindly ensure the trustpoint is available on the device.

Troubleshooting Cisco CallManager

• Overview of Cisco CallManager Troubleshooting Guide
• Issues in Server Addition using AppViewX UI
• Issues in Device communication
• Issue in Discovery
• Issues in CSR generation at Endpoint
• Issues in Certificate Push
• Issues in Certificate Bind

Overview of Cisco CallManager Troubleshooting Guide

This section will guide you to overcome the various issues faced by you during the use of Cisco CallManager and its various functionalities.

Issues in Server Addition using AppViewX UI

Issues in Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **CISCO**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Click **CUCM**.
8. Fill in the appropriate details.
9. Click **Add**.

Error Messages

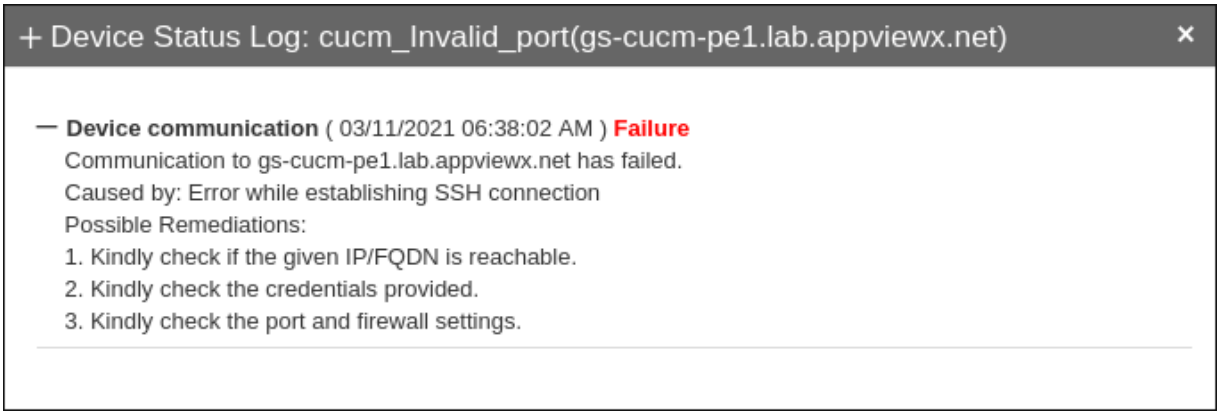
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A Cisco CallManager device exists in inventory with the same name.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname name> has failed.	1. Device unreachable. 2. Invalid credential. 3. Invalid port.	1. Kindly check if the given IP/FQDN is reachable. 2. Kindly check the credentials provided. 3. Kindly check the port and firewall settings.
Cisco Tomcat service is not active	Cisco Tomcat service is not in an up and running state.	Kindly restart the Cisco Tomcat Service. Command to verify the status of services is: utils service list

Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Required Services may not be in an up and running state.	Please ensure the supported services are up and running state and services are associated with SSL configs. Services supported by AppViewX : Cisco tomcat Command to verify the status of services is: utils service list

Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Cisco CallManager**. A list of devices will be generated in the **Devices dropdown**.

Error Messages

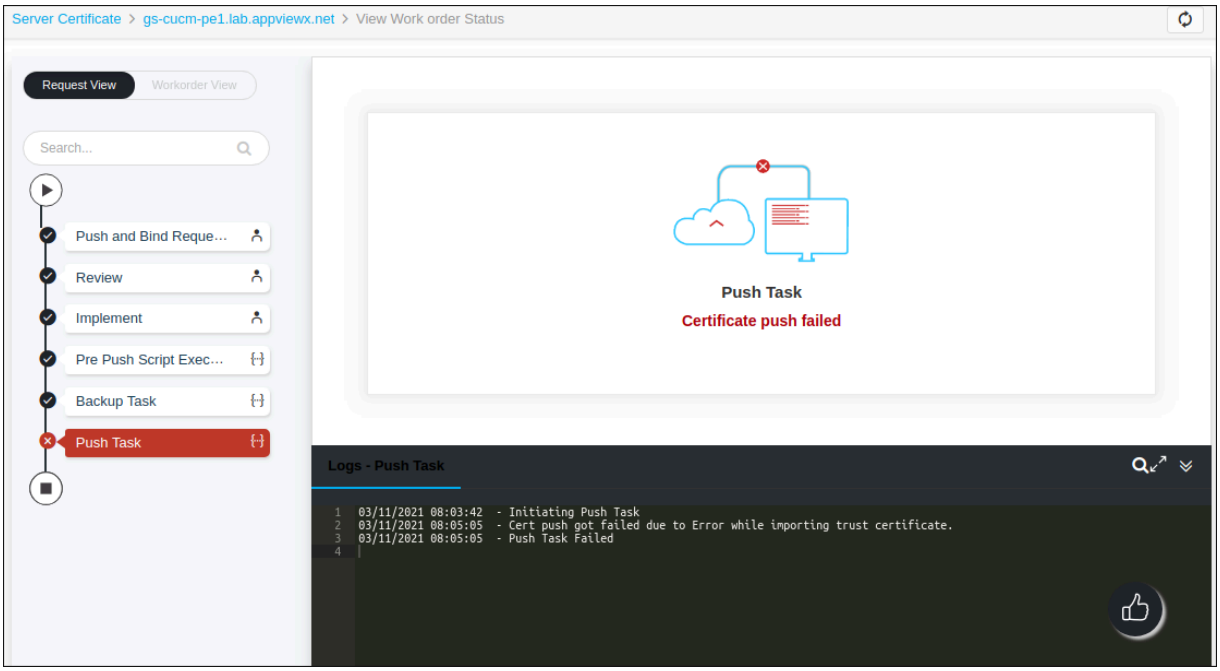
Error Message	Possible Cause	Possible Solution
CUCM CSR gen command failed	Command execution may fail.	Kindly ensure all CSR gen commands are executed properly.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server**. The **Server Certificate** page is displayed.
4. Click any **Server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, click **Add App Connector**.
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Cert push got failed due to Error while importing server certificate.	1. The certificate should be issued from CSR generated by device. 2. CUCM will not allow to push the same cert again.	1. Kindly ensure the certificate issued by the CSR generated from Device.CUCM will not support to push any other certs. 2. CUCM will delete the CSR information from the device on successful cert push. Kindly ensure you are pushing the newly issued certificate and respective CSR information for the same should be available in the device.
Cert push got failed due to Error while importing trust certificate.	CA/Intermediate cert with the same name may already exist in the device.	AppViewX will not overwrite the existing CA configurations. Kindly delete/rename the old certificates to proceed with push.

Issues in Certificate Bind

Issues in the Certificate Bind

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and Click **Server**. The **Server Certificate** page is displayed.
4. Click any **Server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, click **Add App Connector**.
6. On successful certificate push, Select the services to be restarted.
7. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Cert bind got failed.Cause : Service restart failure.	Connection timeout or Invalid Services	Kindly check if the device is in a reachable state to execute the command.

Troubleshooting Common Functionality of Servers

• Overview

• Issues in Device Addition using Import Option

• Issues in Credential List Addition

• Issues in Server Unmanage Functionality

• Issues in Server Manage functionality

• Issues in Server Export

Overview

This section helps you troubleshoot the common problems that you might encounter when dealing with the common functionality of servers. The guide will give more troubleshooting processes on issues encountered during handling of devices like addition using import option, adding to credential list, including the server in managed servers, unmanaging the server or server export.

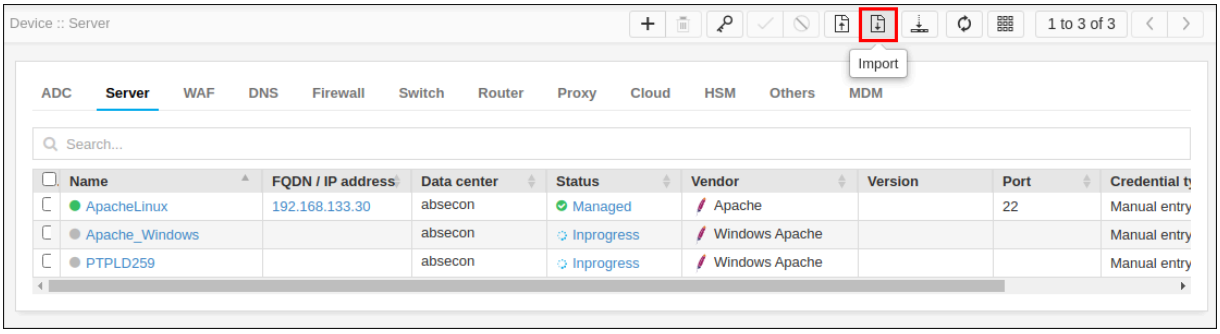
Issues in Device Addition using Import Option

Issues in the Device Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device and click **Import**.



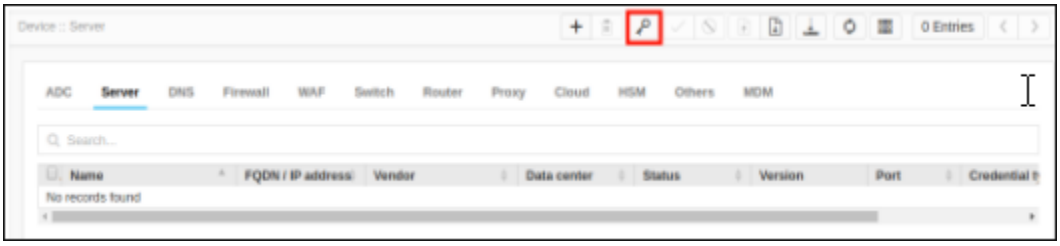
Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum 5 files can be maintained.	Delete any of the parsed/completed files to upload a new one.

Issues in Credential List Addition

Issues in the Credential List Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** Page, click **Server** Tab.
5. Select the device and click **Credential**. The **Credentials List** page will be displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

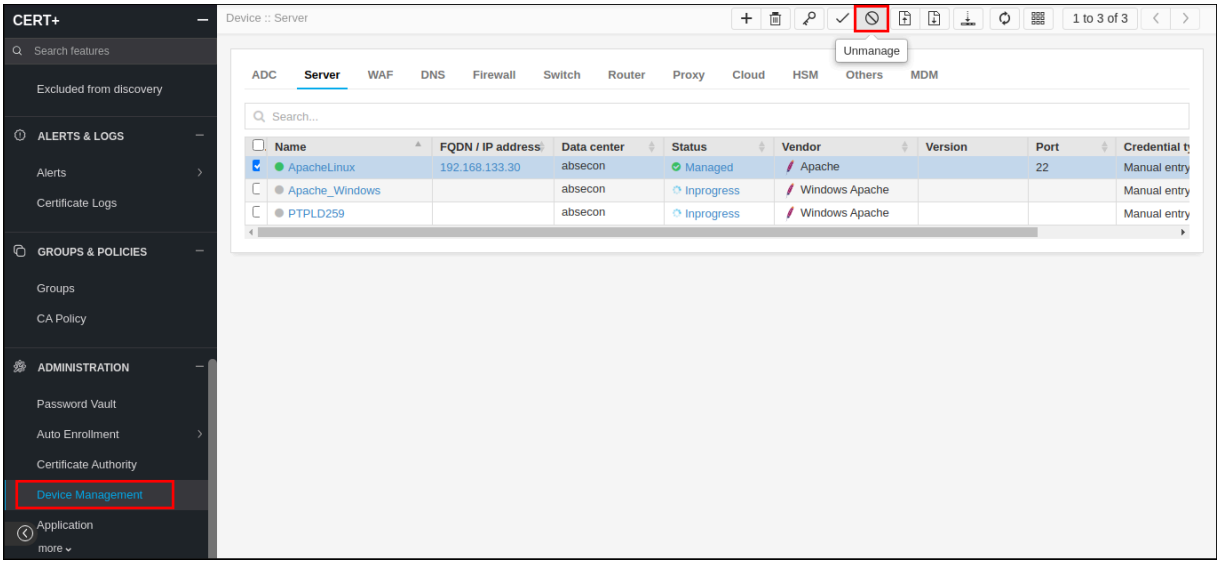
Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt.	The Identity Key file uploaded is not in the correct format.	Provide key file with correct format (.pem or .txt)

Issues in Server Unmanage Functionality

Issues in the Server Unmanage Functionality

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

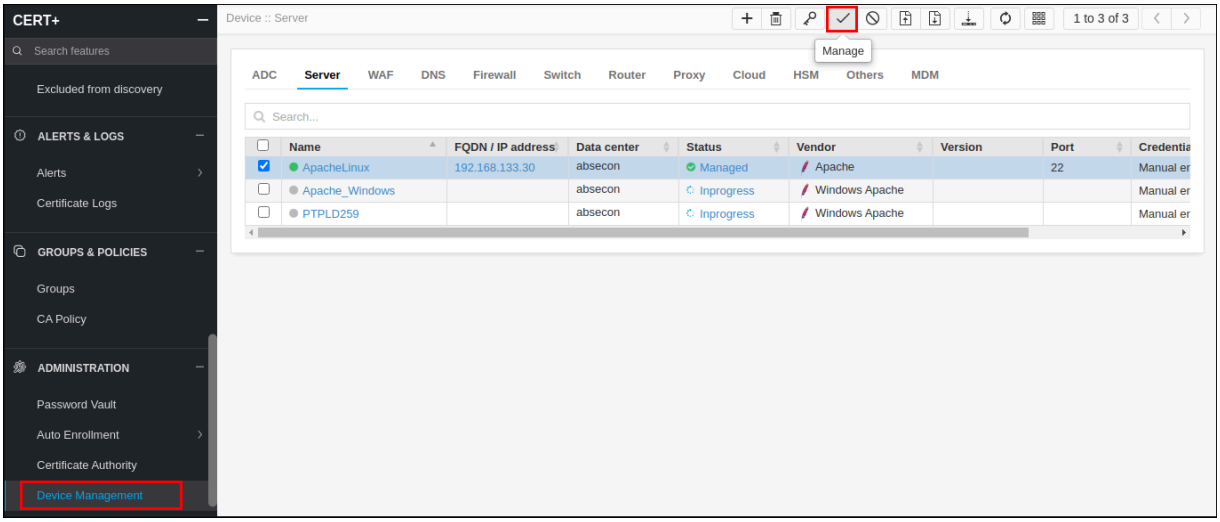
Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Server Manage functionality

Issues in the Server Manage functionality

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click on **Server** Tab.
5. Select the device and click **Manage**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

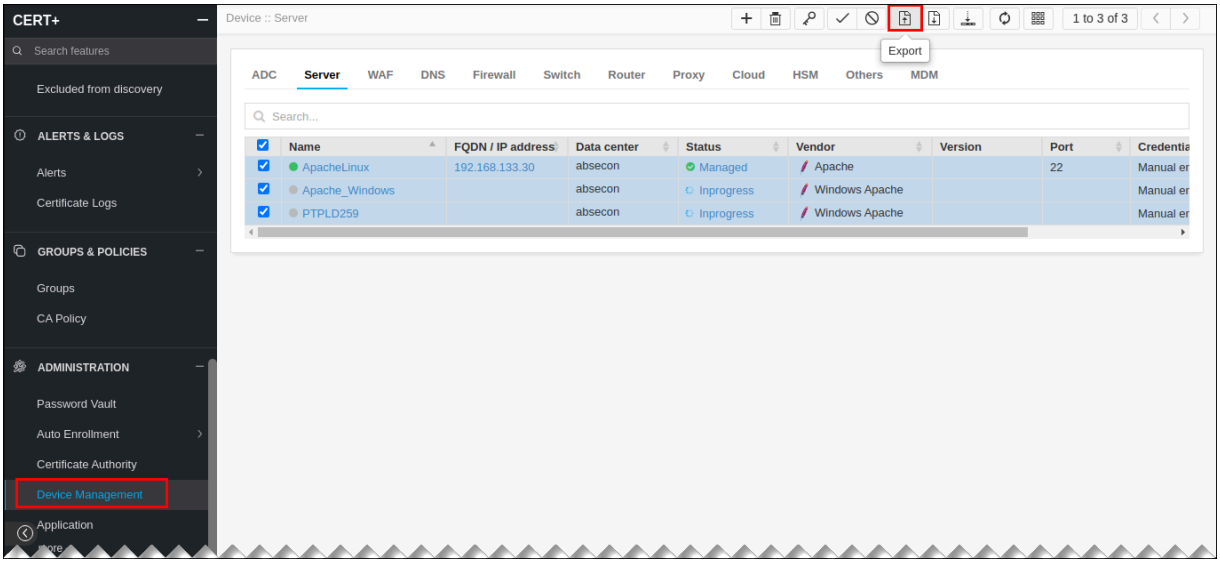
Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Server Export

Issues in the Server Export

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. Click on **Server** Tab on the **Device Management** Page.
5. Select the device and click **Export**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue.	Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.)
	Unable to fetch device list from the database.	Make sure the database is running and has correct data.

Troubleshooting Data Power Server

- Overview
- Issues in Data Power Server Addition using AppViewX UI
- Issues in Communicating to Data power Server
- Issues in Accessing Server
- Issues in Certificate Discovery
- Issues in Push and Rollback

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with the Data Power server.

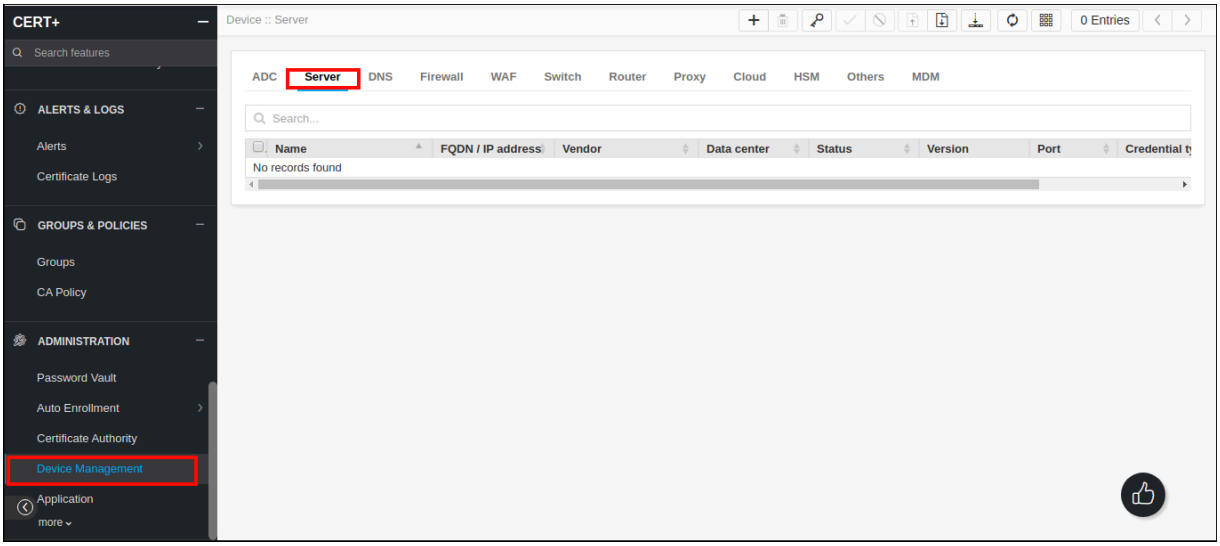
Issues in Data Power Server Addition using AppViewX UI

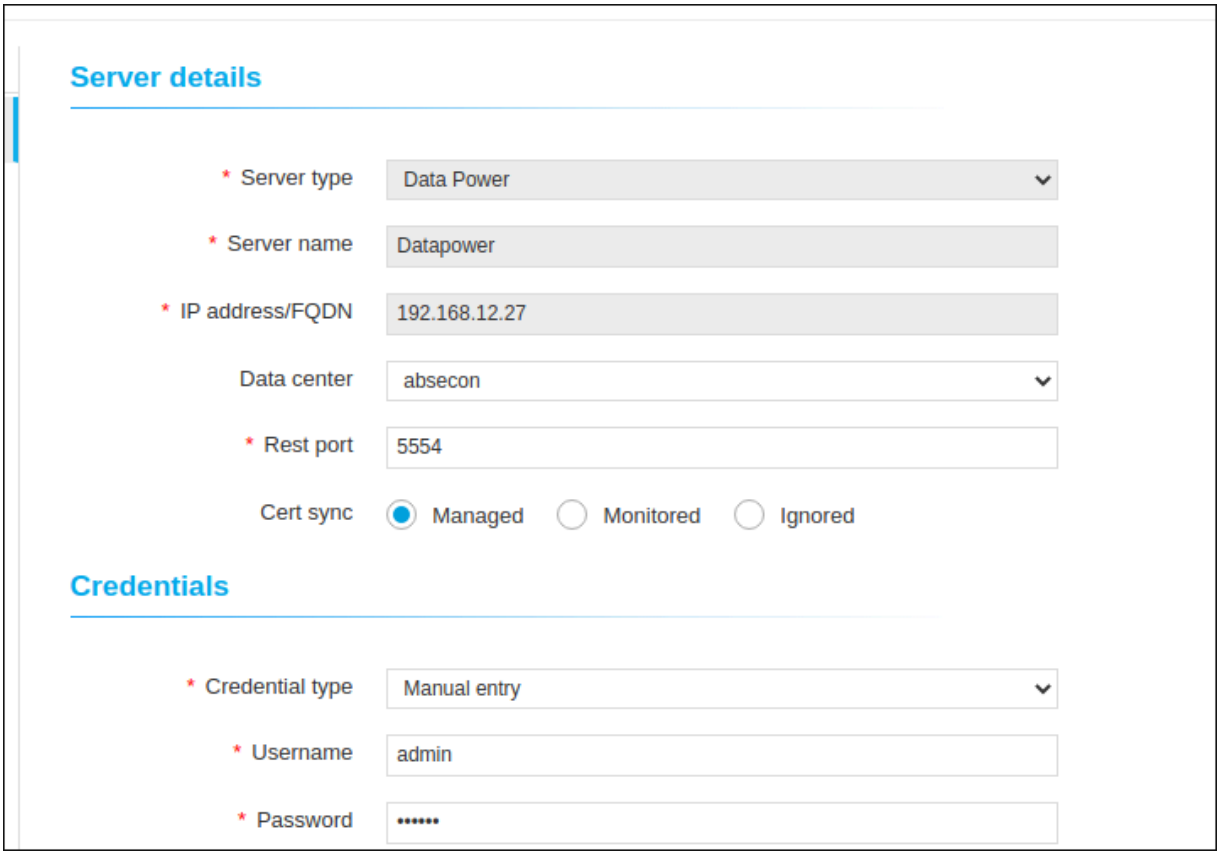
Issues in the Data Power Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Data Power**.
7. Fill in the appropriate details.
8. Click **Add**.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

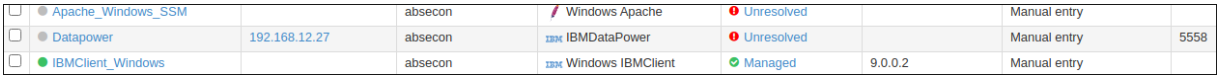
Error Messages

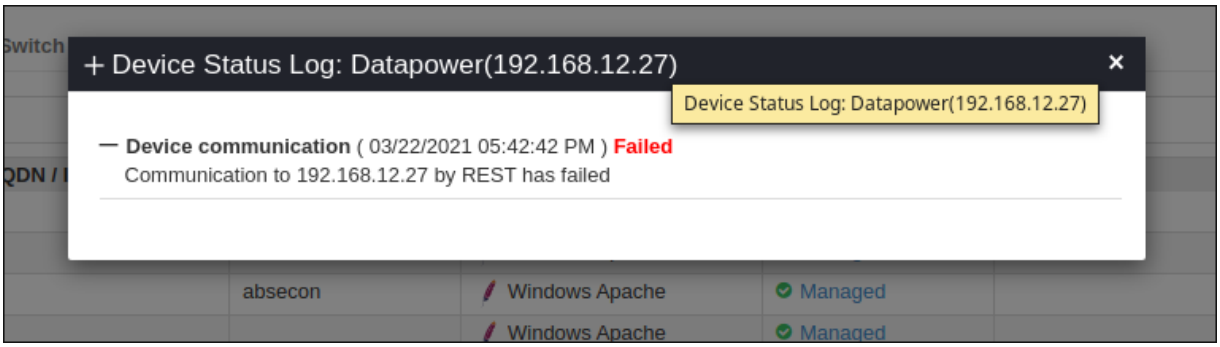
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Data power Server

Issues in the Communicating to Data power Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.





Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Domain fetch has failed.	Domain not configured in Data Power	Check manually if domains are configured.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching domains. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Rest communication failed	Unable to access the Rest APIs exposed by Data Power	Login via Postman to check if the APIs are accessible

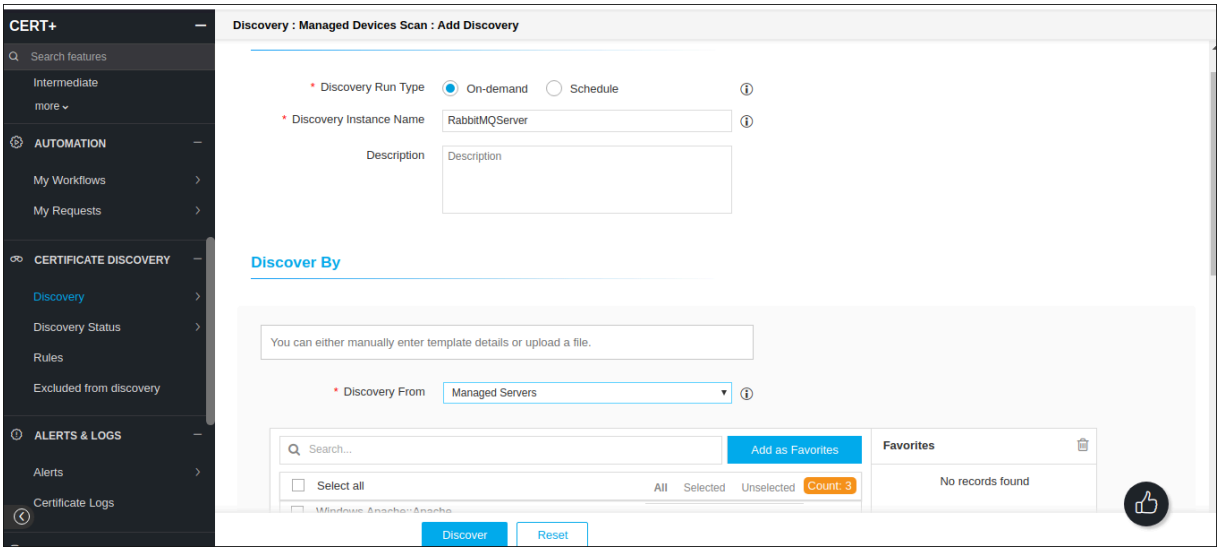
Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the "**Discover By**" section.	Select at least one device to discover certificates from.

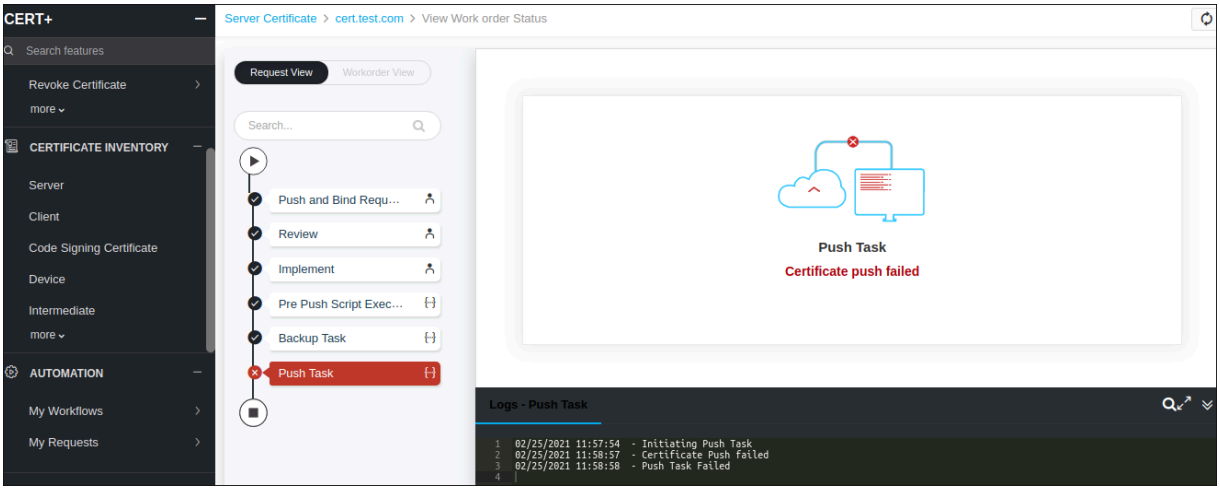
Issues in Push and Rollback

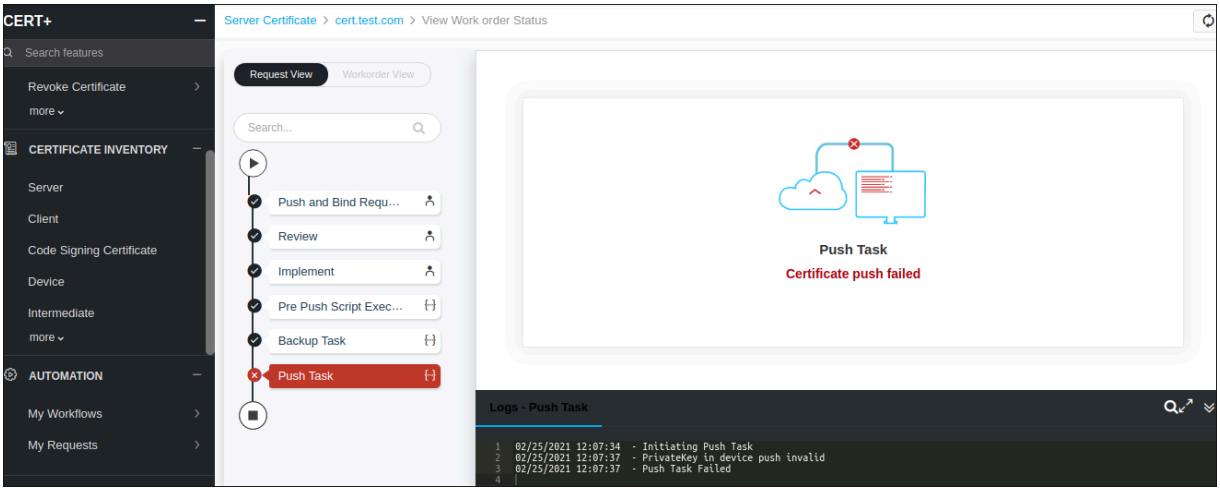
Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Data Power server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the store to push the certificate in the application connector	Kindly ensure the user has access to the store to push the certificates to.

Troubleshooting F5 WAF

- Introduction
- Issues in Fetch Config
- Issues in Discovery
- Issues in CSR Generation
- Issues in F5 WAF Backup, Push, Bind, and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using the F5 WAF functionalities. This guide will give more troubleshooting processes on F5 WAF certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with F5 WAF.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the device, click **Fetch Config**.

Error Messages

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the associated error message.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the error message associated.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in CSR Generation

Issues in the CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category dropdown**, click **Firewall**.
7. From the dropdown, click the correct **Vendor**. A list of devices will be generated in the **Devices dropdown**.
8. To generate **CSR**, select the F5 device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
CSR Generation using HSM on this device version is not supported.	Version not supported.	Please use the supported version device to create CSR using HSM. Supported versions are v13 and v12.
1) CSR content unavailable in device 2) Requested CSR is not available in device 3) Csr could not be fetched	CSR content unavailable on device.	For some reasons CSR creation has failed, please check the logs to reproduce.
CSR already exists in this scope with the same Key reference name	The name is already used on the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Thales HSM is not installed in the device. Please install and try again.	Thales is not installed in the device.	Please install Thales HSM and try again.
Invalid module. Please specify the valid module and try again.	Invalid module specified.	Specify a valid module and try again.
The CSR <name> was not found in the device.	CSR content is not available in the name specified.	Please check the name in the CA connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
NetHSM private key is not available/installed in device	NetHSM private key is not available/installed in the device.	Please install NetHSM private key on the device.

Issues in F5 WAF Backup, Push, Bind, and Rollback

Issues in the F5 WAF

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
Invalid profile type	Specified profile type is not supported.	Please use client-SSL or server-SSL.
Certificate fetch failed	Certificate fetch failed.	Check the error message associated to know more about the problem.
Certificate already exists	Certificate is already available with the same.	Either change the name or enable overwrite in the application connector.
Key already exists	Key is already available with the same.	Either change the name of the key or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates only can be pushed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Fortigate Firewall

- Introduction
- Issues in Fetch Config
- Issues in Discovery
- Issues in CSR Generation
- Issues in Fortigate Firewall Backup, Push, Bind and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using the Fortigate firewall in CERT+ functionalities. This guide will give more troubleshooting processes on Fortigate firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Fortigate firewall.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

Error Messages

Error Message	Possible Cause	Possible Solution
Error occurred in command execution - <Error message>	Error occurred in command execution	Command execution has failed. Please refer to the error message associated with this.

Issues in Discovery

Issues in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Error occurred in command execution - <Error message>	Error occurred in command execution.	Command execution has failed. Please refer to the associated error message.

Issues in CSR Generation

Issues in CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall .**
7. Click correct **Vendor** from the dropdown. A list of devices will be generated in the **Devices dropdown**.
8. For generating **CSR**, select devide as **Fortigate**.
9. Click **Add**.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr name exists in the device, and cannot be overwritten.	Name is already used in the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Fortigate Firewall Backup, Push, Bind and Rollback

Issues in the Fortigate Firewall

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate content is mandatory parameter	Certificate content should be available.	Please specify certificate content in the request.
Intermed certificate content is mandatory for pushing CA certificate	Intermediate certificate content should be available.	Please specify intermediate certificate content in the request.
Root certificate content is mandatory for pushing CA certificate	Root certificate content should be available.	Please specify root certificate content in the request.
Certificate name is mandatory parameter	Certificate file name is mandatory.	Please specify the certificate file name in the connector.
Profile details are missing in Application connector	Profile details are missing.	Please specify profile details in the request.
Private key password is mandatory parameter	Private key password is mandatory.	Specify private key password in the connector.
Given certificate name does not exist in a device with a private key. Certificate with private key should exist either in device or AppViewX	Private key not available in the certificate.	Certificate should be pushed with the private key to bind with the profile.
Root certificate name already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.
Intermediate certificate with name: <name> already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates can be pushed.

Troubleshooting HP ILO

- Overview
- Issues in Device communication
- Issues in Certificate Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

This section will guide you to overcome the various issues faced by you during the use of HP ILO and its various functionalities.

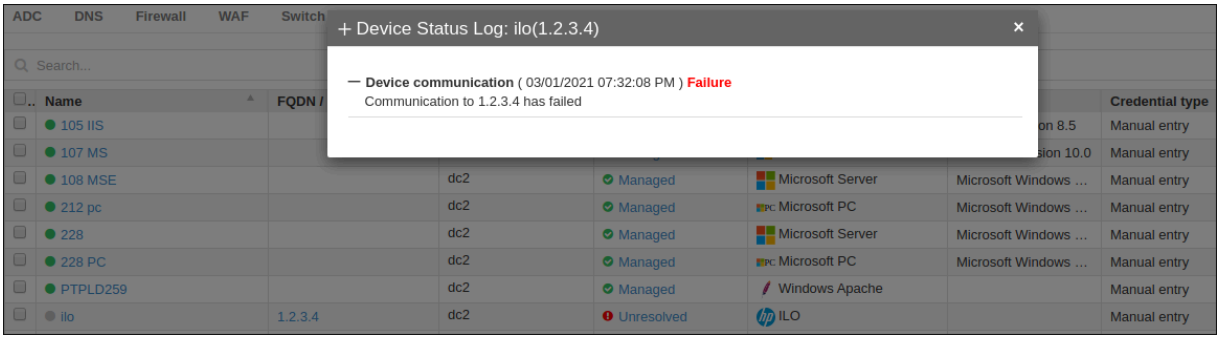
Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <ip/ fqdn> has failed.	IP/FQDN provided is not reachable. Credentials not valid.	Check if the provided IP/FQDN is correct Check if the provided username and password for device addition is correct The HPILO python package is not installed properly in AppViewX VM.

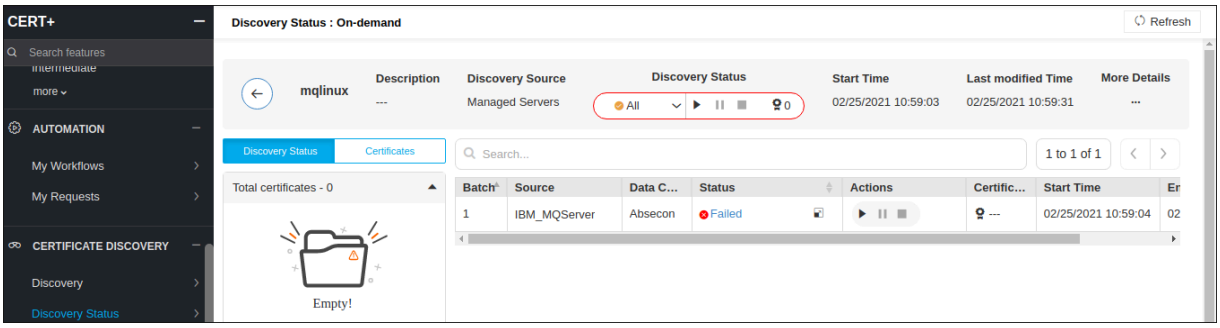
Issues in Certificate Discovery

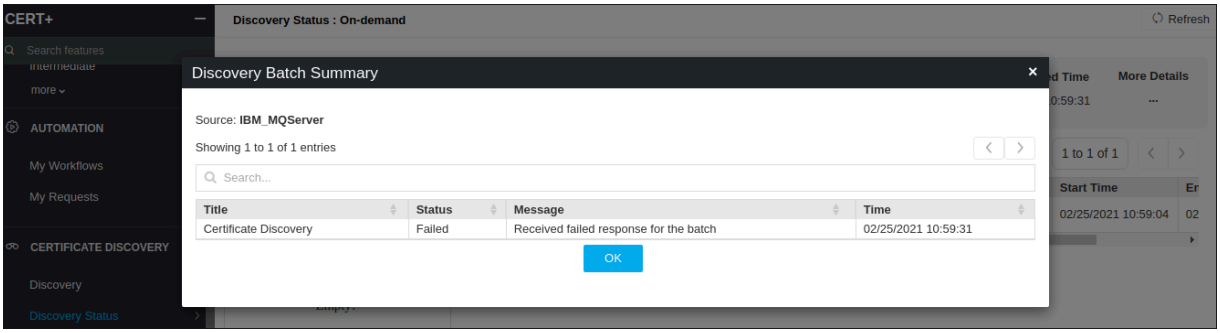
Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	ILO portal is not up and running Network issues in reaching the portal	Kindly ensure the ILO web portal is up and running. Kindly ensure a proper identity certificate is associated with the web portal

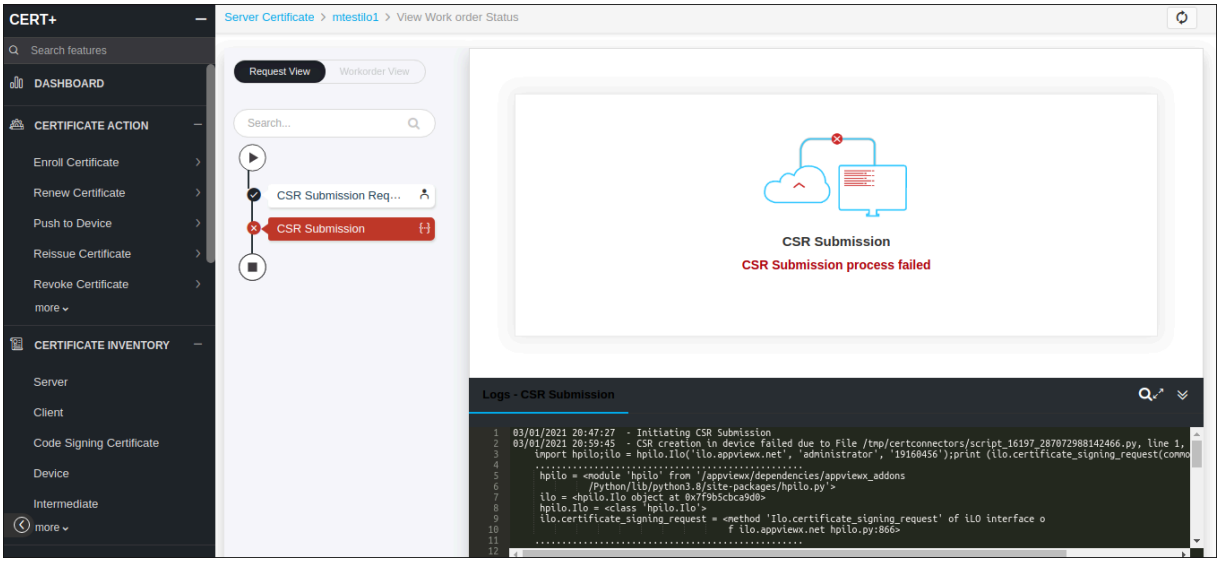
Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category.**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **ILO**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

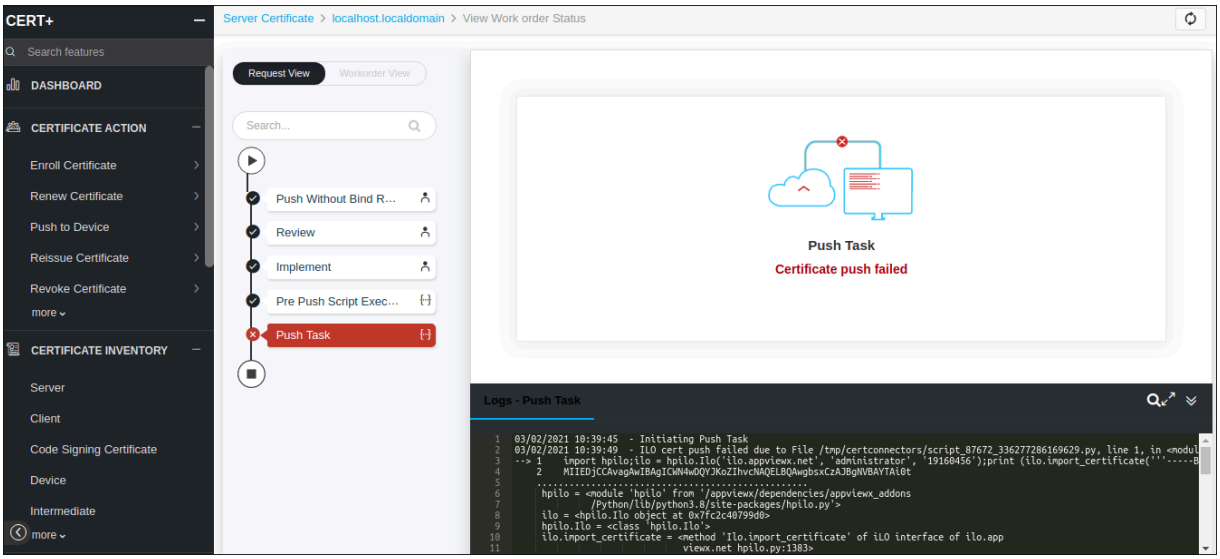
Error Message	Possible Cause	Possible Solution
CSR generation failed. 03/01/2021 20:59:45 - CSR creation in device failed due to File /tmp/certconnectors/ script_16197_287072988142466.py, line 1, in <module> import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.certificate_signing_request(common_name='mtestilo1')); IloGeneratingCSR: The iLO subsystem is currently generating a Certificate Signing Request(CSR), run script after 10 minutes or more to receive the CSR. 03/01/2021 20:59:45 - CSR Submission Failed	1. Input parameters might not be valid for the CSR request. 2. Multiple CSR requests might be triggered within a short span of time.	Kindly ensure the CSR parameters are configured properly. Kindly ensure multiple CSR requests are not submitted to the same device in any mode. Kindly ensure we keep at least 15mins interval between CSR request submission else the response for the previous request is triggered before submitting the next request.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **ILO device**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed 03/02/2021 10:39:49 - ILO cert push failed due to File /tmp/certconnectors/ script_87672_336277286169629.py, line 1, in <module> --> 1 import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.import_certificate('''-----BEGIN CERTIFICATE-----	Certificate is not generated with CSR from device	Kindly ensure the certificate is signed with a CSR request generated from the target device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
IloError: Invalid certificate common name 03/02/2021 10:39:49 - Push Task Failed		

Troubleshooting IBMClient Linux

- Overview
- Issues in Device communication
- Issue in Discovery
- Issues in CSR Generation at Endpoint
- Issues in Certificate Push

Overview

This section will guide you to overcome the various issues faced by you during the use of IBMClient Linux and its various functionalities.

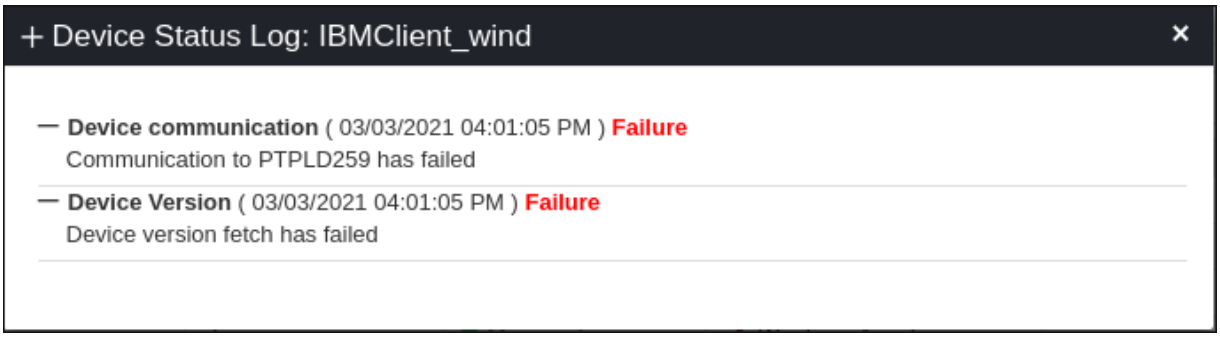
Issues in Device communication

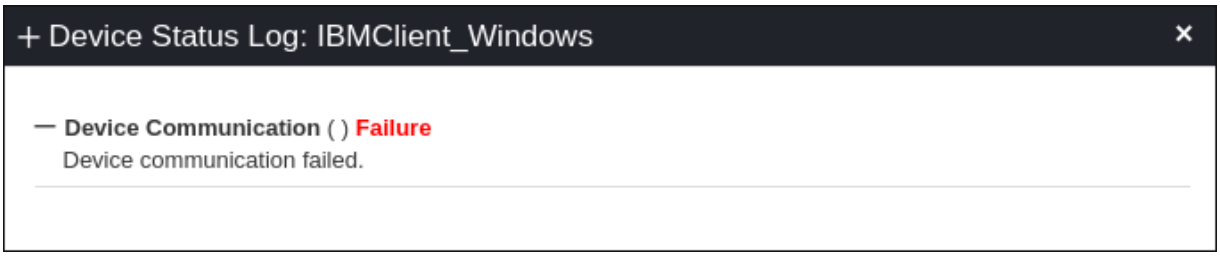
Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent GSKit is not installed on any given device.	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent. Please ensure GSKit is installed properly.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

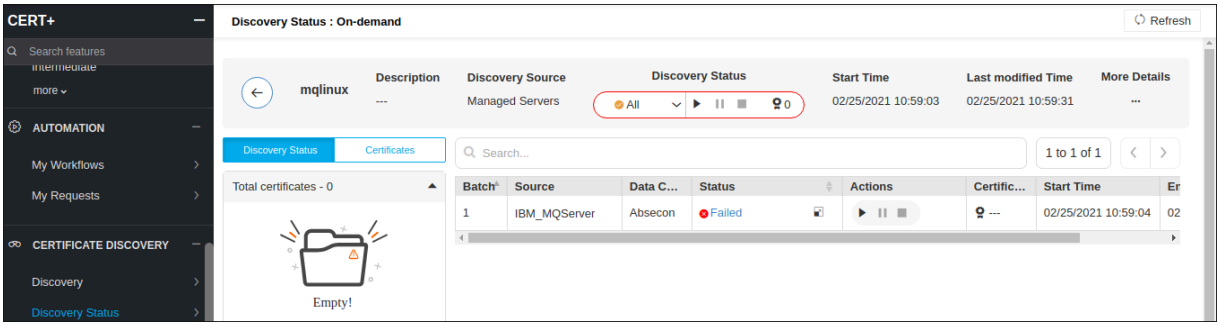
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

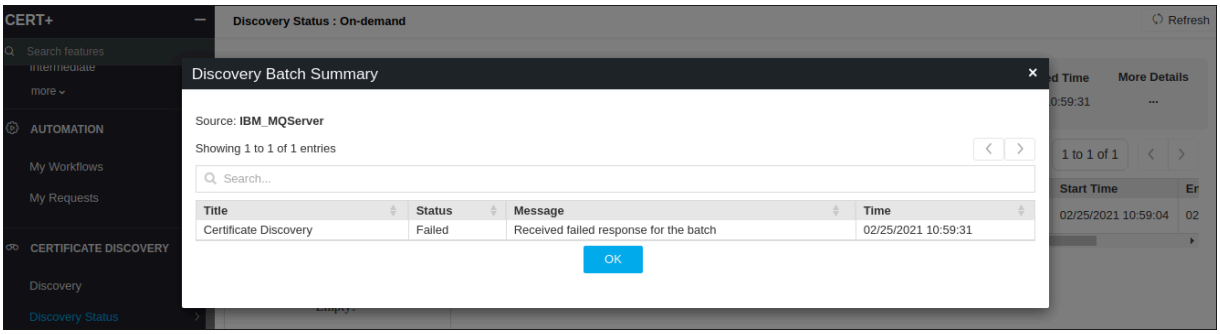
Issue in Discovery

Issue in Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

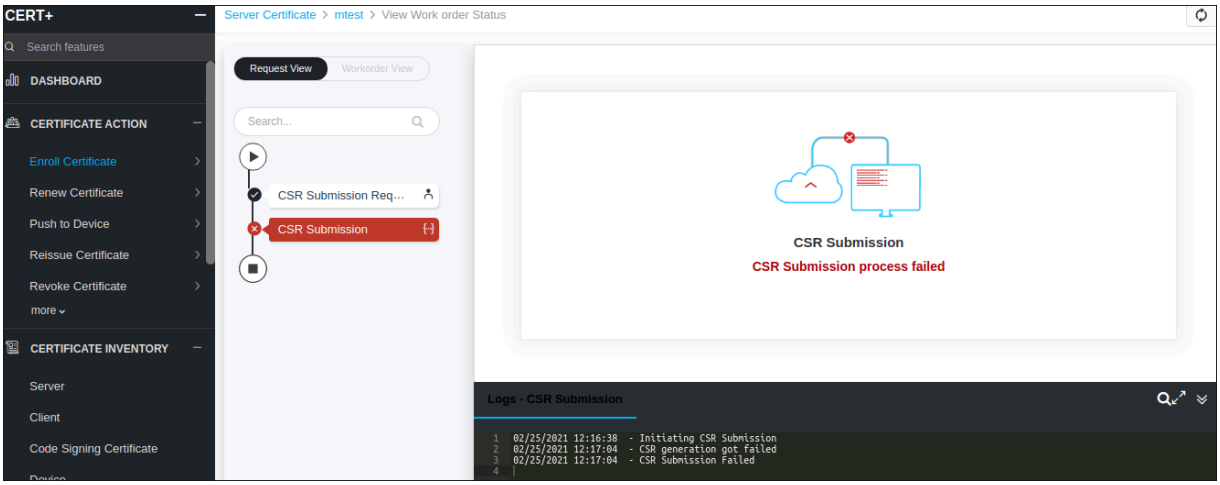
Issues in CSR Generation at Endpoint

Issues in the CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Select **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **Windows MQServer**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

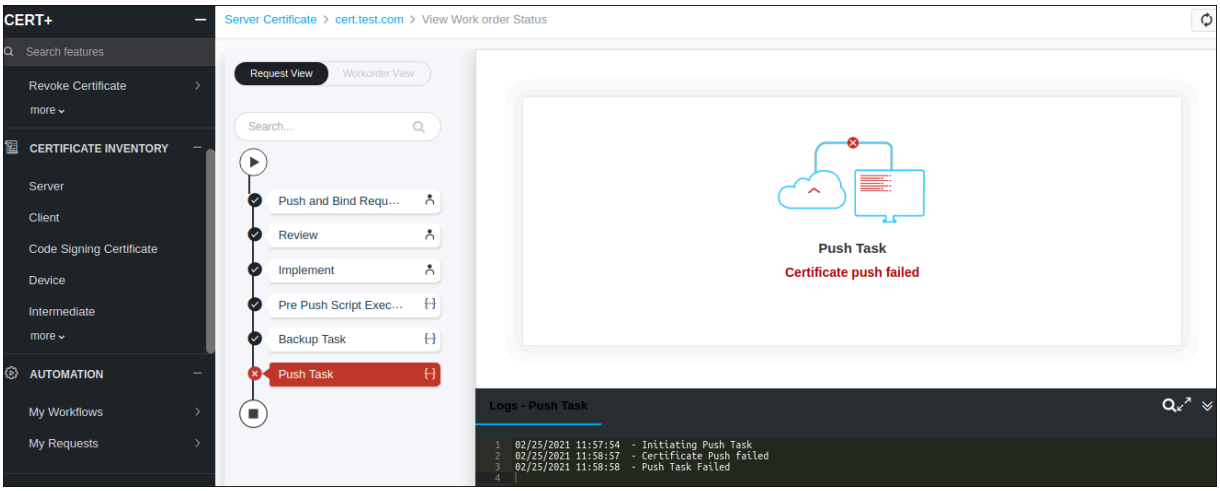
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

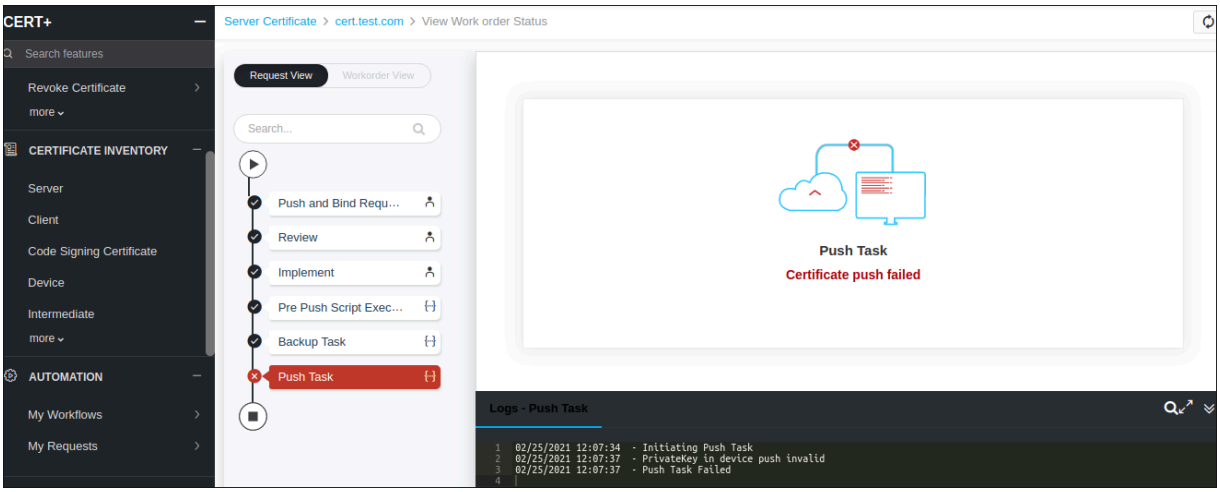
Issues in Certificate Push

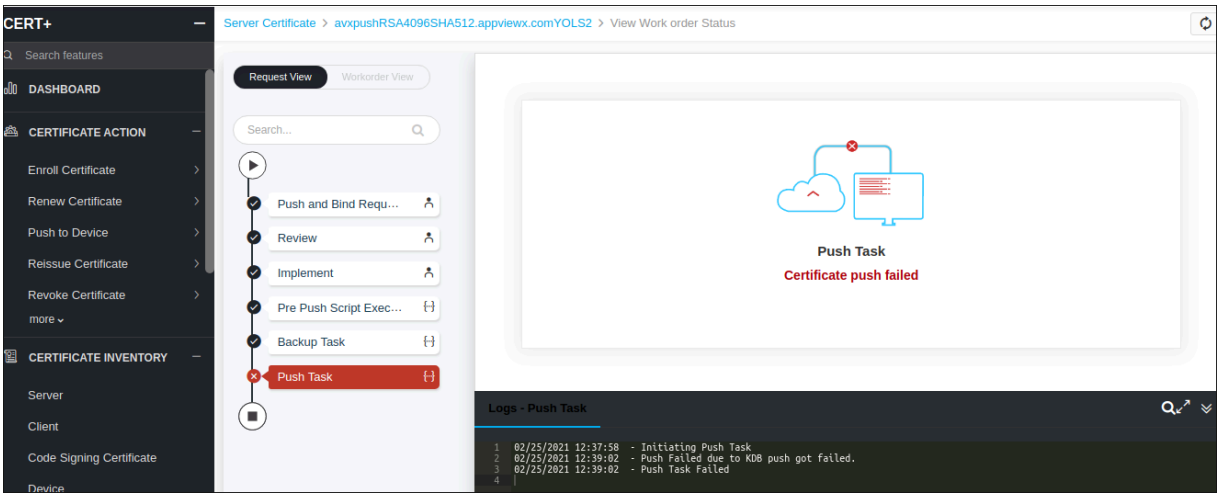
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Create an **Application connector** with “**Create KDB/Create Keystore**” profile
5. Push the certificate to the device.

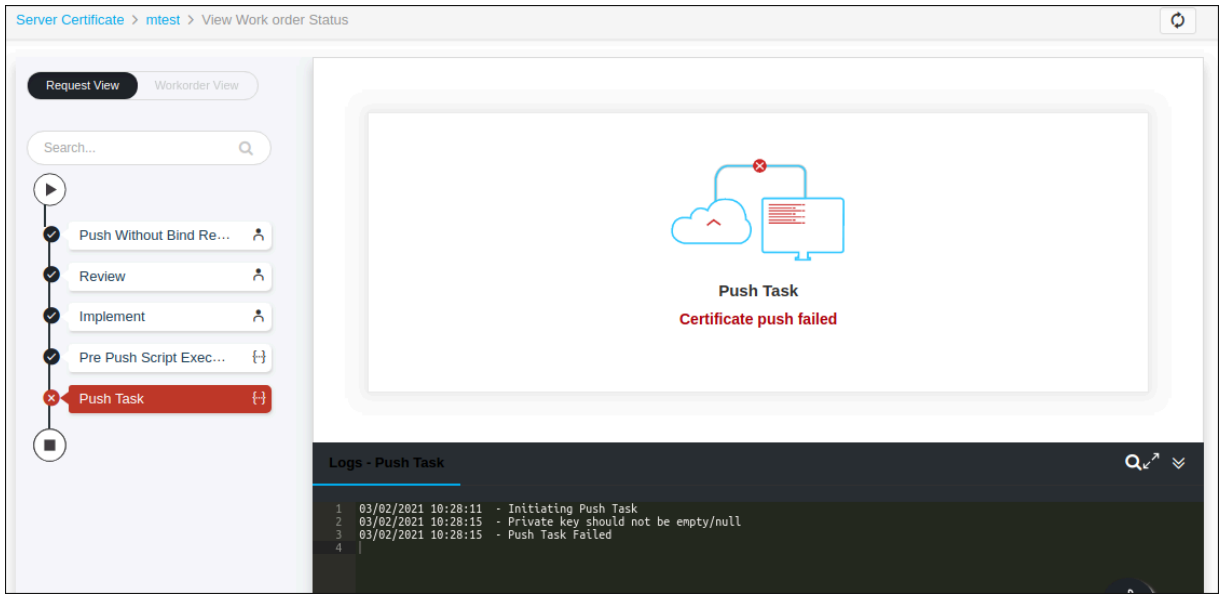
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

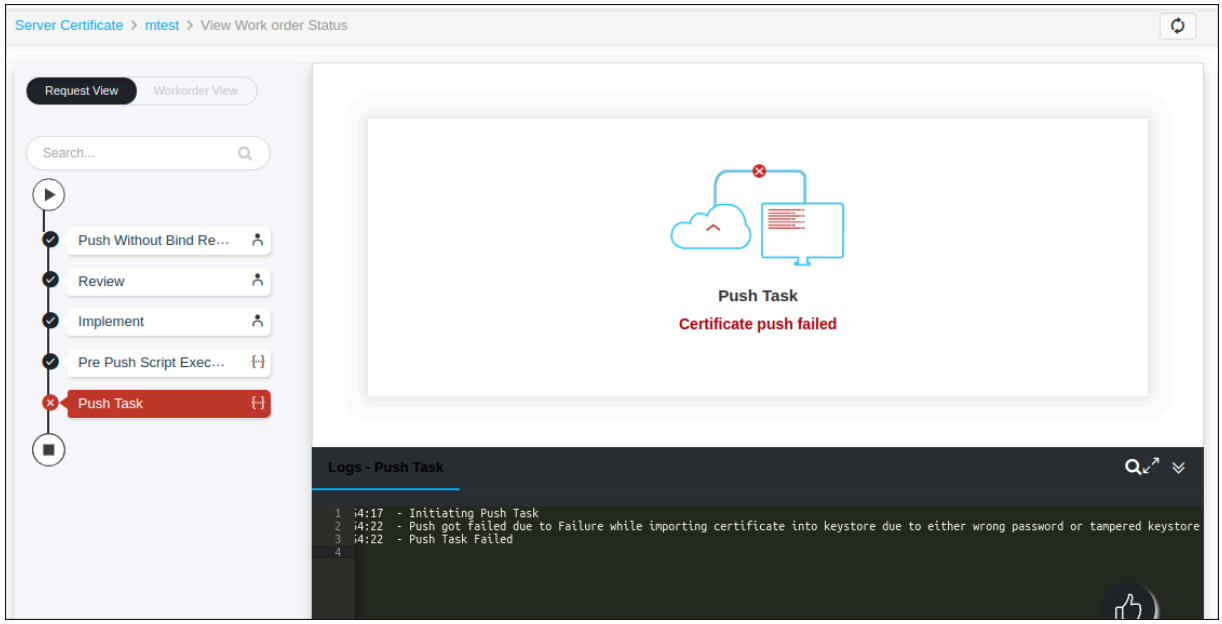






Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed. Or Push got failed due to User has no permission for the given location to perform the operation	User has restricted access to the path configured to push the certificate in the application connector	Please ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available on device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device.	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
1. Private key should not be empty/null. 2. Push failed due to Failure while importing certificate into keystore due to either wrong password or tampered keystore.	Trying to push certs without a keyfile.	Please ensure the certificate to be pushed has a private key file. Or if key file exists in device please select privateKeyInDevice option.

Troubleshooting IBMClient Windows

• Overview
• Issues in Server Addition using AppViewX GUI
• Issues in Device communication
• Issue in Discovery
• Issues in CSR generation at Endpoint
• Issues in Certificate Push

Overview

This document will guide you to overcome the various issues faced by you during the use of IBMClient Windows and its various functionalities.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Server Addition using AppViewX GUI

Issues in the Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, Click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **IBM**.
7. Click **IBMClient(Windows)**.
8. Fill in the appropriate details.
9. Click **Add**.

Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

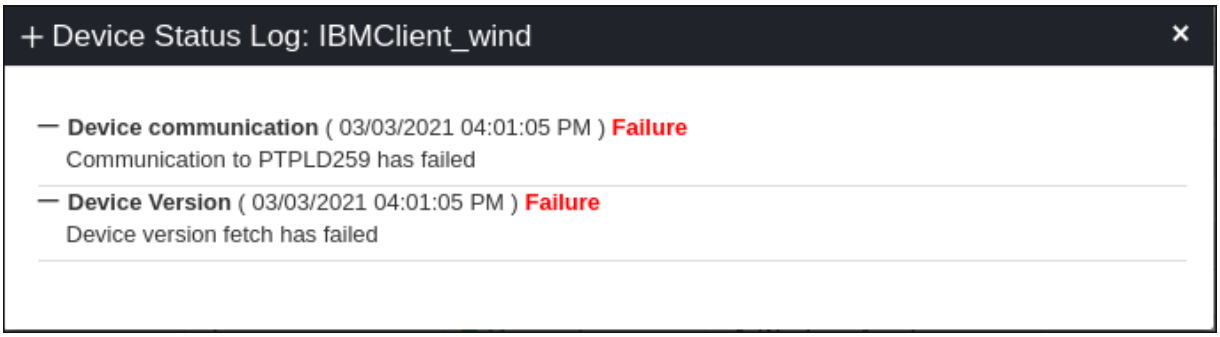
Issues in Device communication

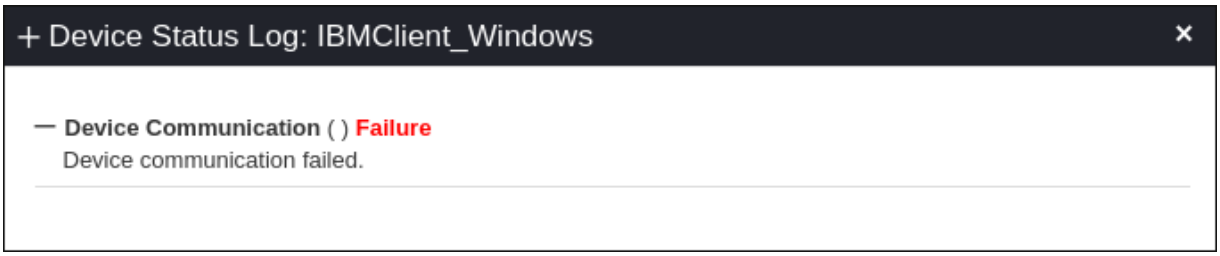
Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent GSKit is not installed on any given device.	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent. Please ensure GSKit is installed properly.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

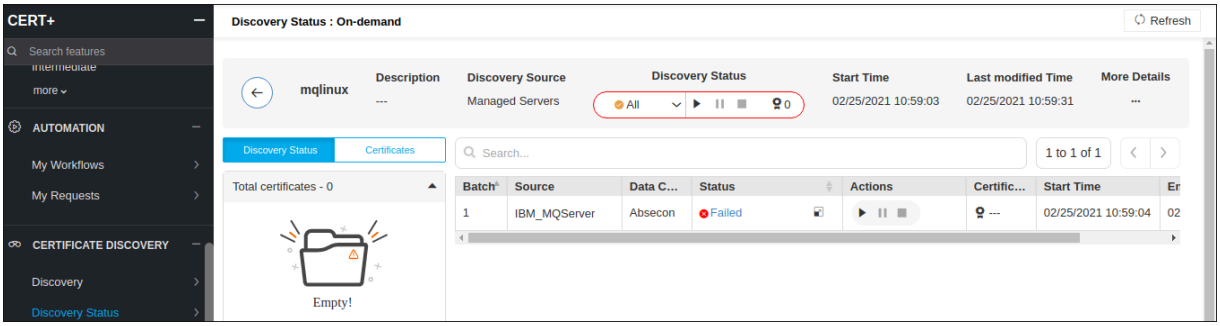
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

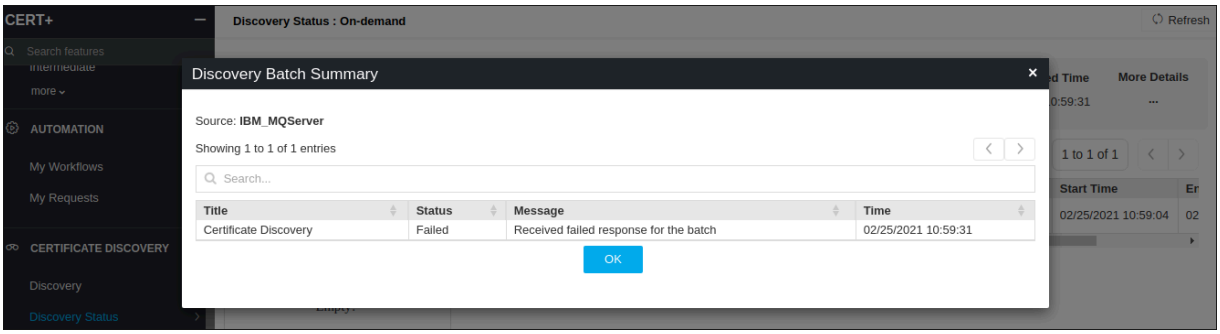
Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+** . The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

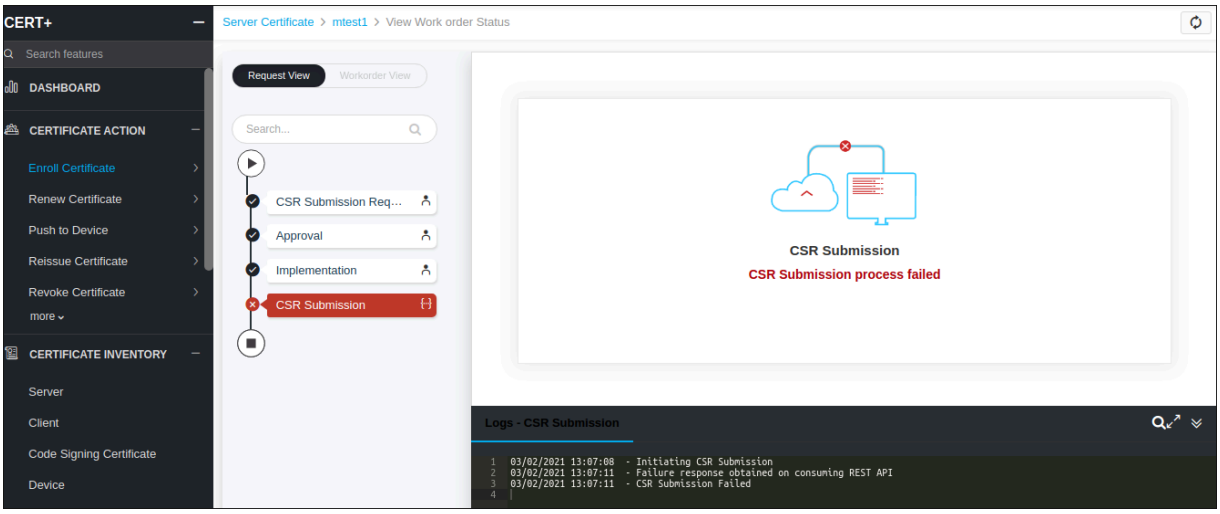
Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

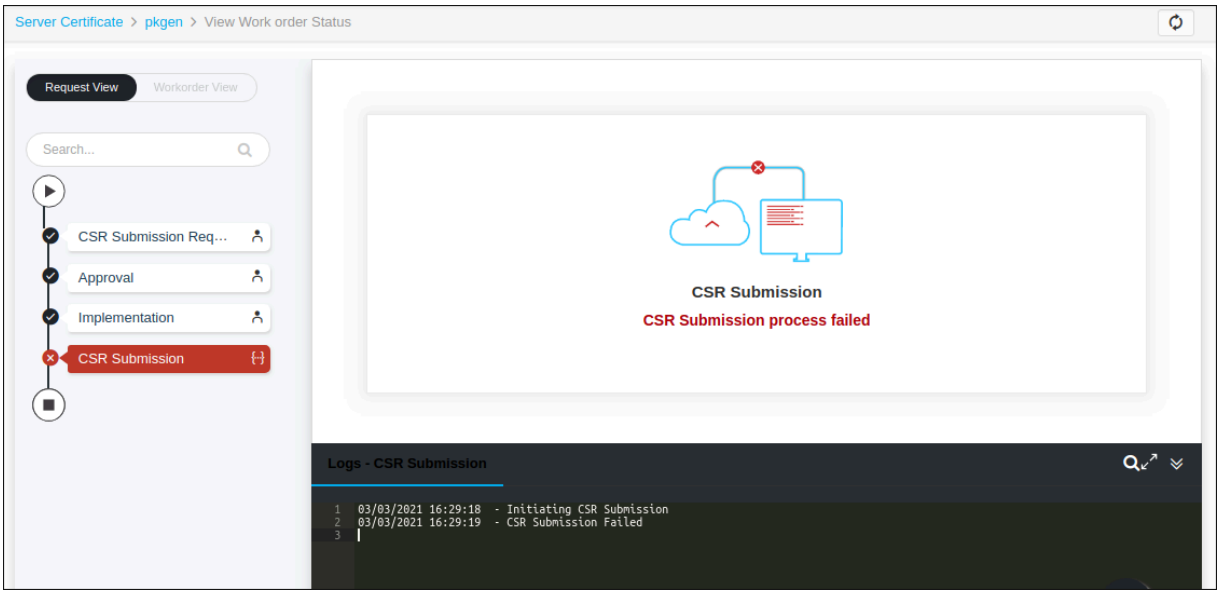
Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category.**
7. From the **Vendor** dropdown, click **Windows MQServer**. A list of devices will be generated in the **Devices dropdown**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messsages

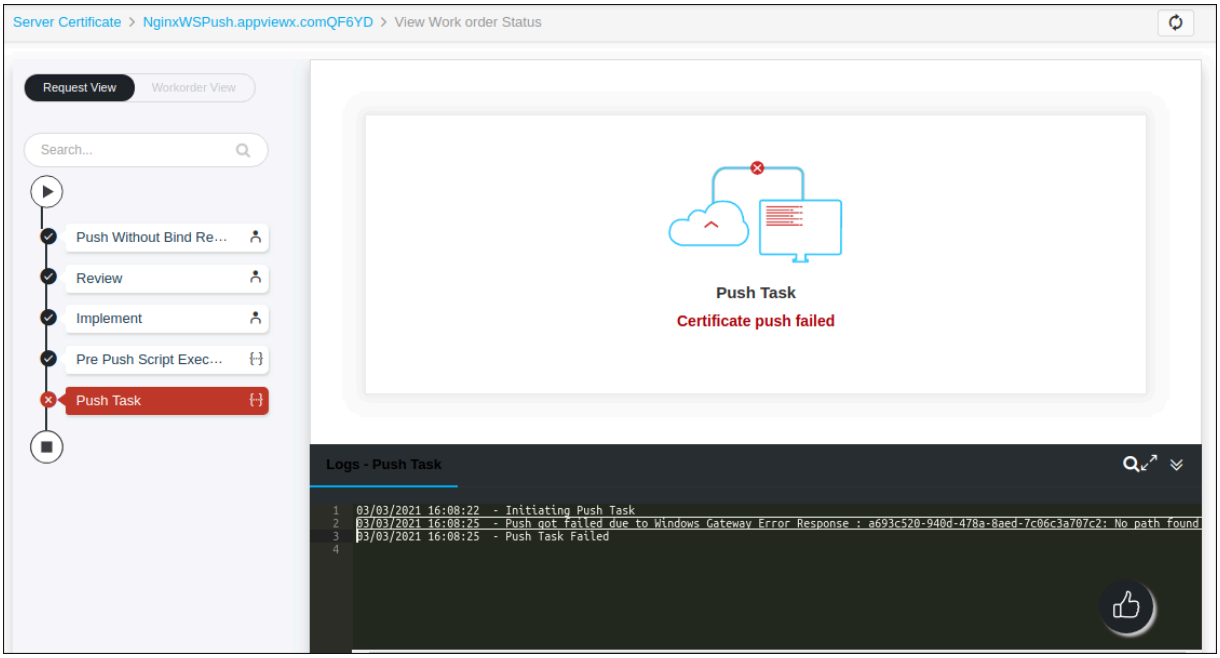
Error Message	Possible Cause	Possible Solution
1. Failure response obtained on consuming REST API. 2. CSR submission failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

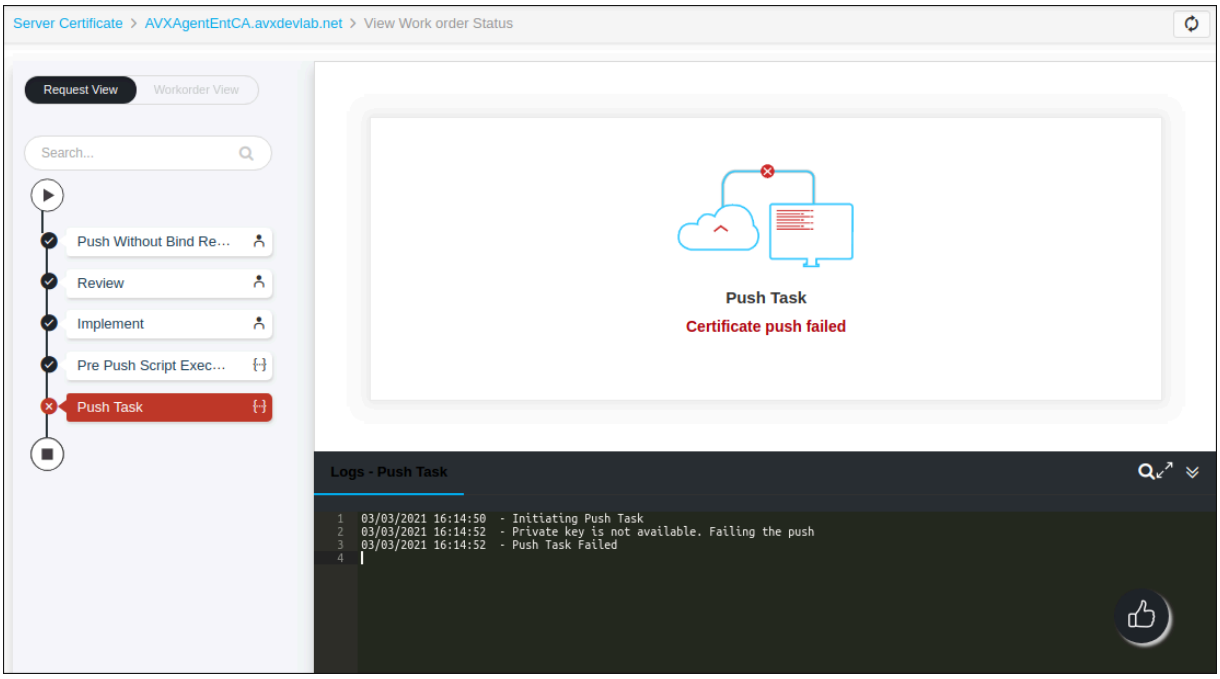
Issues in Certificate Push

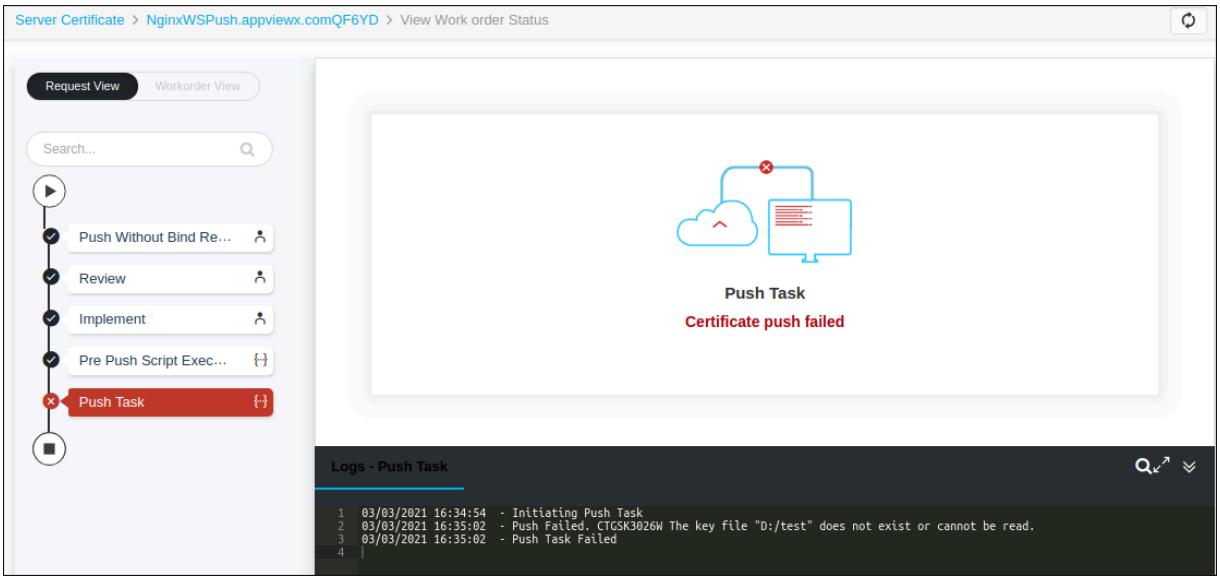
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **IBMClient server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with "**Create KDB/Create Keystore**" profile, select **Add App Connector**.
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
1. Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read. 2. Push got failed due to Windows Gateway Error Response : a693c520-940d-478a-8aed-7c06c3a707c2: No path found	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
Private key is not available. Failing the push	Trying to push certificates without a keyfile.	Please ensure the certificate to be pushed has a private key file Or if key file exists in device please select privateKeyInDevice option.

Troubleshooting Imperva WAF

- Overview
- Issues in Communicating to Imperva
- Issues in Config Fetch
- Issue in Discovery
- Issue in Push and Rollback

Overview

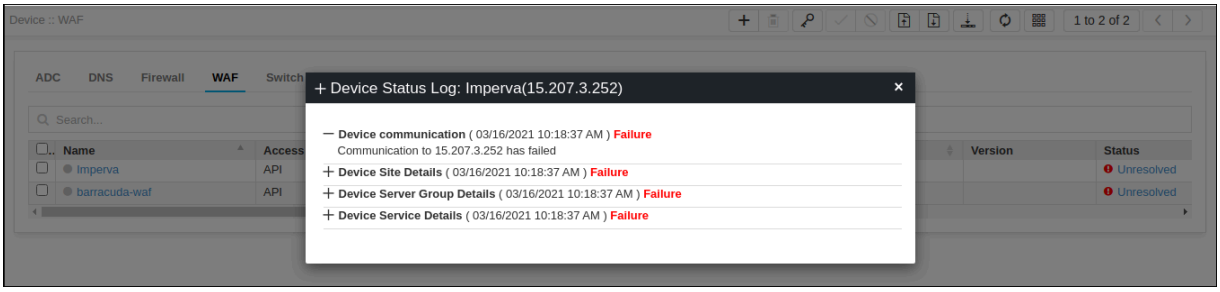
This section will guide you to overcome the various issues faced by you during the use of Imperva WAF and its various functionalities.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Communicating to Imperva

Issues in the Communicating to Imperva

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Error Messages

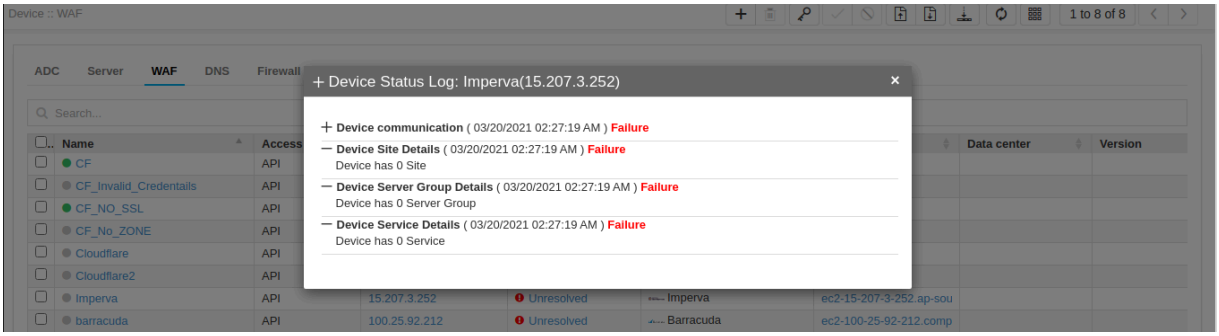
Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if the correct Imperva credentials are provided. Please login to the SecureSphere console to check if Imperva is running.
Connection timeout	Internet / Proxy connection is not provided from AppViewX node. Firewall settings blocking the REST API request	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **WAF** Tab.
5. Select the **Device**, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if a correct Imperva credentials are provided Please login to the SecureSphere to check if Imperva is running.
Device has 0 sites.	No sites configured in Imperva.	Please login to the SecureSphere to check if Sites are configured.
Device has 0 Server Group	No Server Groups configured in Imperva.	Please login to the SecureSphere to check if Server Groups are configured.
Device has 0 Services	No Services configured in Imperva	Please login to the SecureSphere to check if Services are configured.

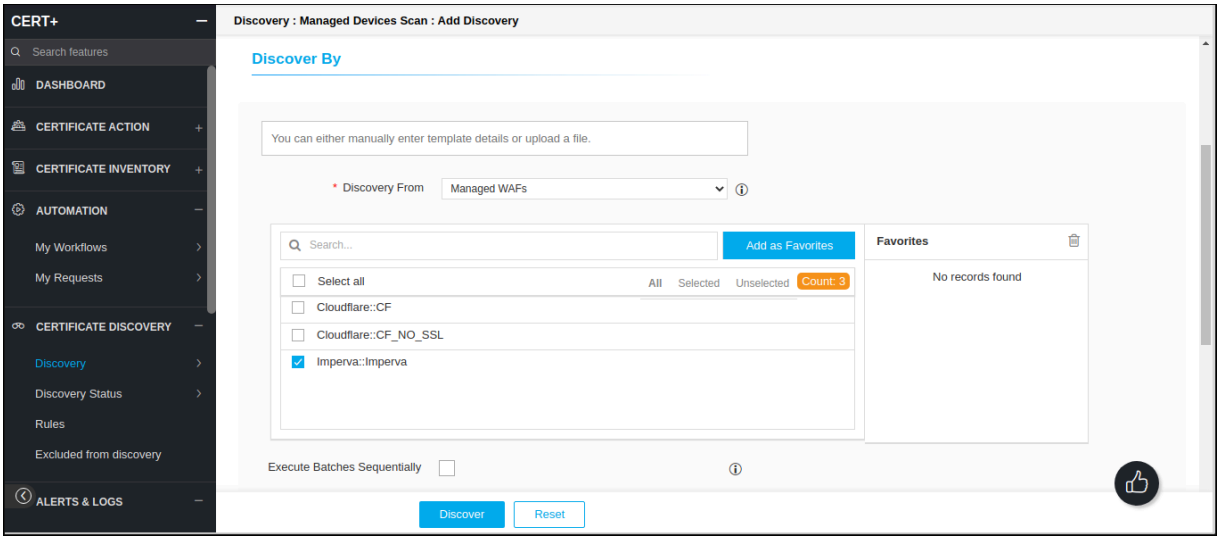
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a devices	No WAF account is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Discovery Status Failed	Check if internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
No Certificates discovered from Imperva WAF	SSL Certificates are not discovered from Imperva due to API restrictions. Imperva Rest API doesn't allow the public Certificate String in the API responses. Only Certificate attributes like common name, signature, Expiry date and Issuer details are captured.	Check with AppViewX PM team / SME for more details

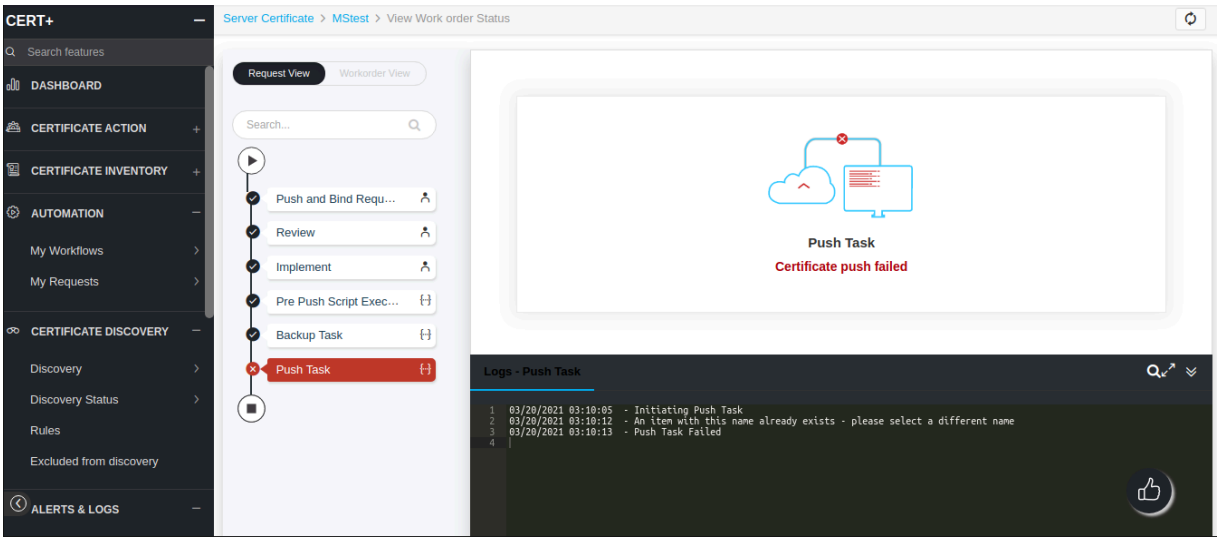
Issue in Push and Rollback

Issue in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **WAF**. The **Server Certificate** page is displayed.
4. Click any **server**. A holistic view of the **Certificate** will be displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



Error Messages

Error Message	Possible Cause	Possible Solution
An item with this name already exists - please select a different name	SSLKeyName should be unique.	Kindly ensure to provide a unique name in “Certificate File Name” field on Connector page.
Site not found	Unable to find the site to push the certificate	Please login to SecureSphere to check if the Site is available.
Server Group not found	Unable to find the Server Group to push the certificate	Please login to SecureSphere to check if the Server Group is available.
Services not found	Unable to find the Service to push the certificate	Please login to SecureSphere to check if the Service is available.

Troubleshooting Linux JBoss Server

- Introduction
- Issues in Linux JBoss Server Addition using AppViewX UI
- Issues in Communicating to Linux JBoss Server
- Issues in Accessing Server

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Credential List
• Issues in Managed Server
• Issues in Unmanaged Server
• Issues in Import Server
• Issues in Export Server
• Issues in Config Fetch
• Issues in Certificate Discovery
• Issues in CSR generation
• Issues in Push and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities.This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux JBoss server.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

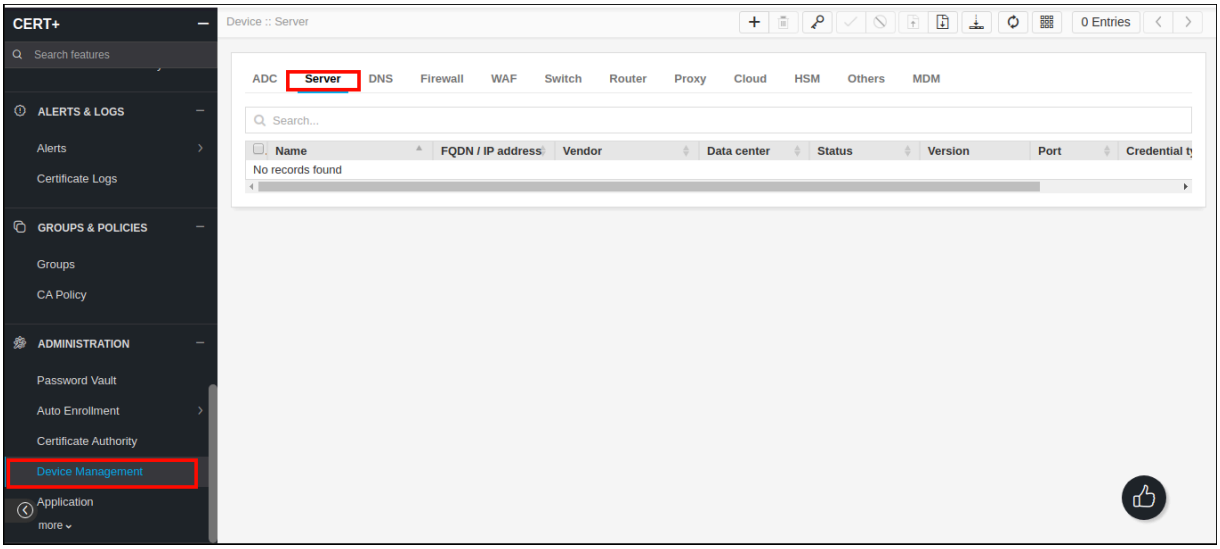
Issues in Linux JBoss Server Addition using AppViewX UI

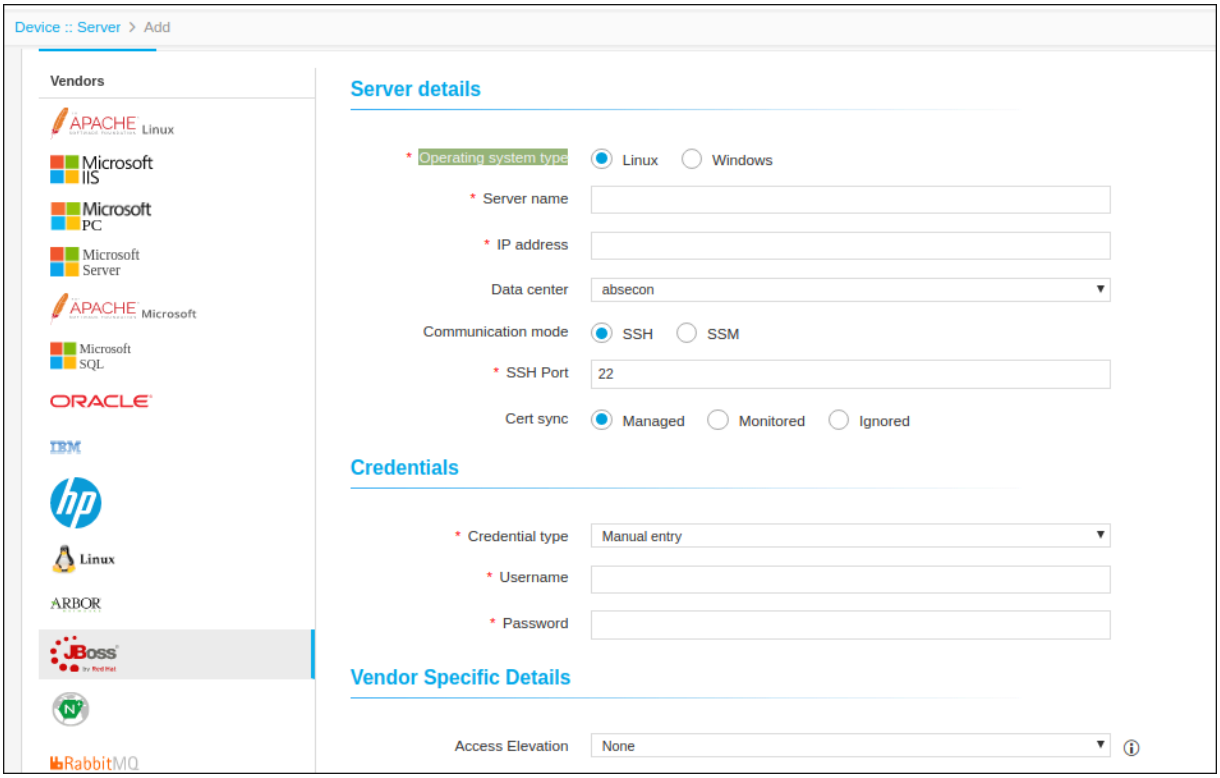
Issues in Linux JBoss Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **JBoss**.
7. Select **Operating System** as **Linux**.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

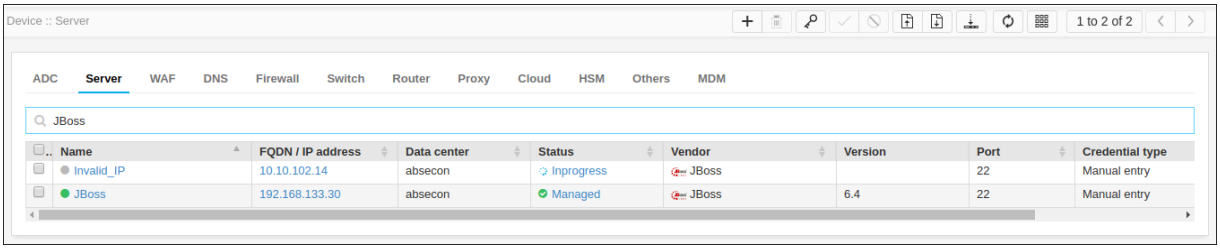
Error Messages

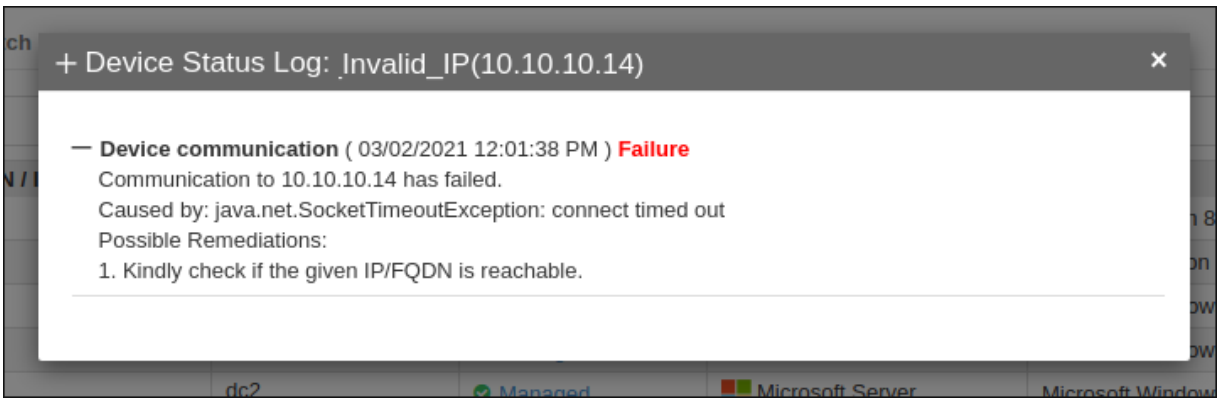
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Linux JBoss Server

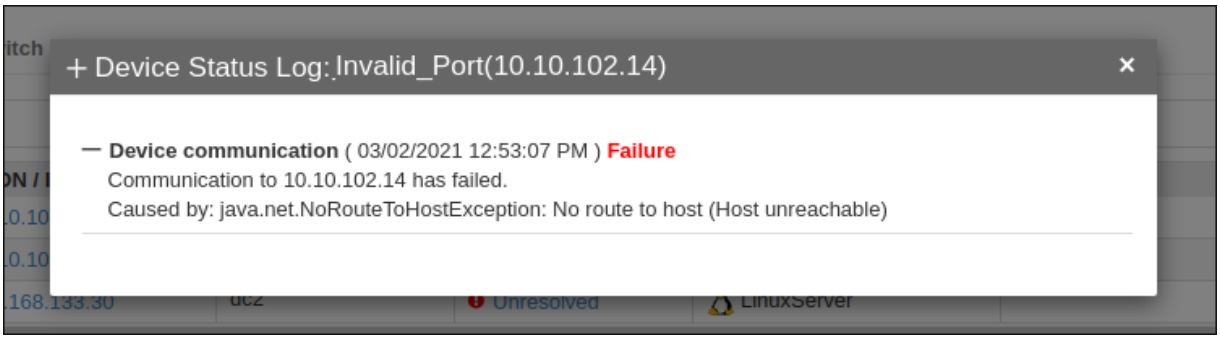
Issues in the Communicating to Linux JBoss Server

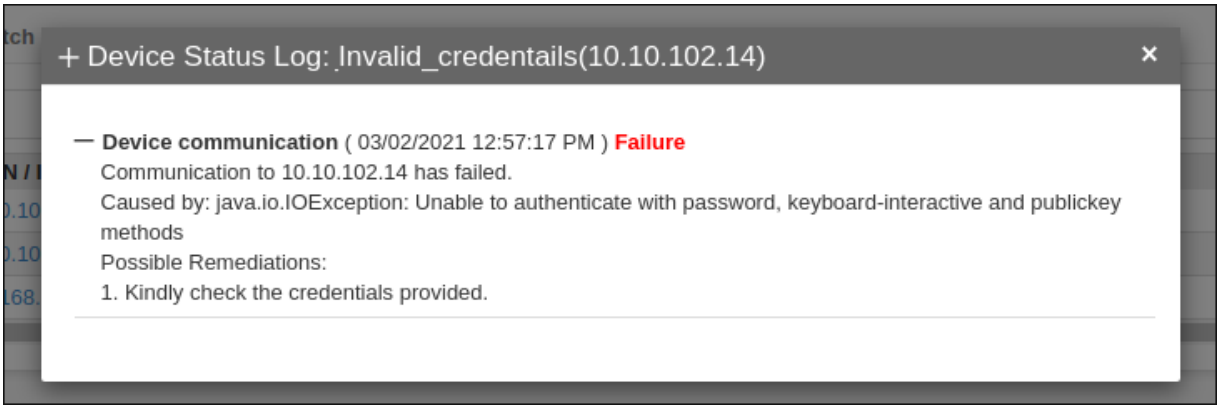
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

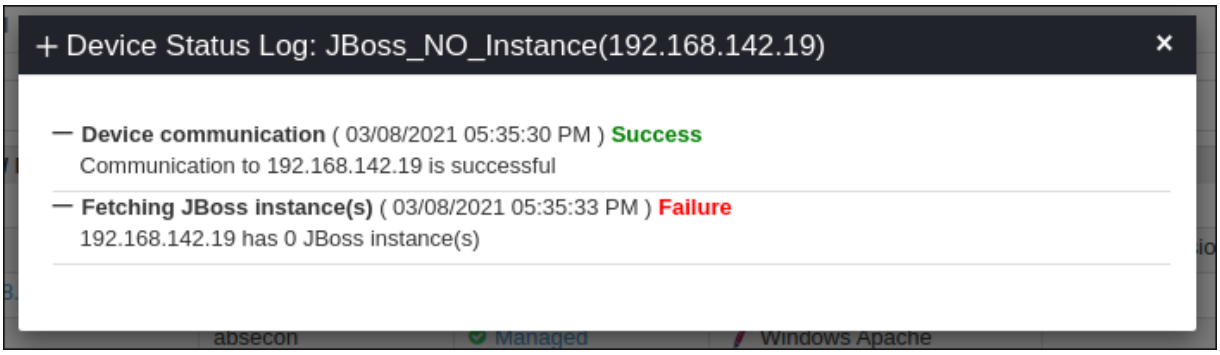




Copyright © 2024 AppViewX, Inc. All Rights Reserved.







Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is either null or empty.	Provide device name as it is a mandatory field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations:	Problem with port configuration	Check if the configured port in the device addition page is correct.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings		
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMACs configured in the target device and ensure AppViewX SSH-plugin supports the same
<IP/FQDN> has 0 JBoss instance(s)	No JBoss server running in the target device,	Login via SSH to the target device and execute the below command to check the status of the JBoss server “ps -ef | grep jboss”.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/ location.	File might not be present in the avx environment.	Check whether someone deleted the file from AppViewX environment. Verify if read permission is given for the location.

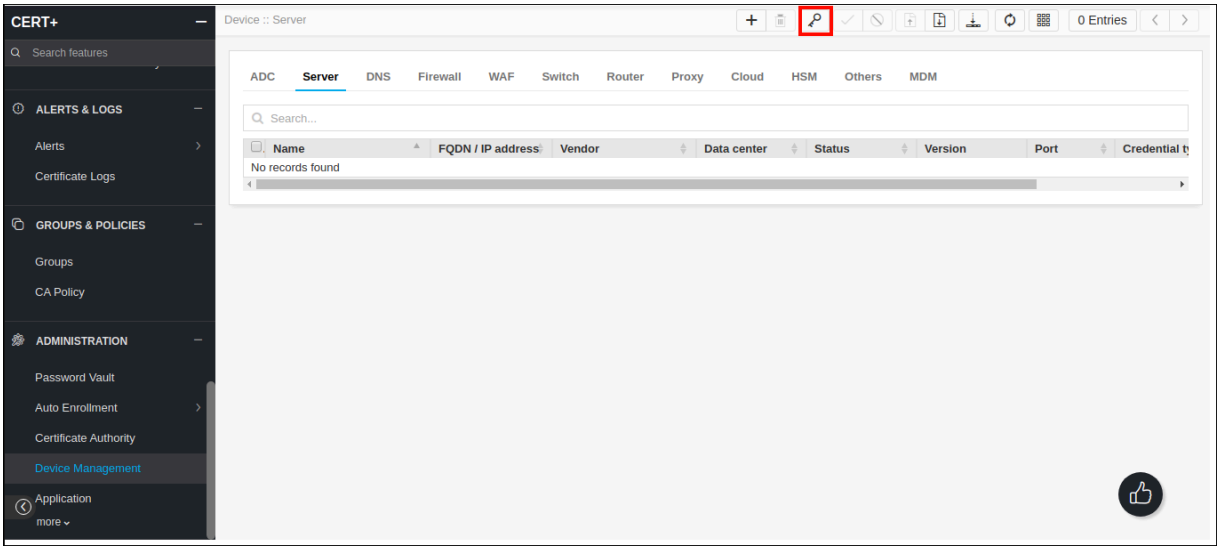
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	User might not have permission to read in the given source location. Device communication might not be established when service has started.	Verify the device connection and restart the service.

Issues in Credential List

Issues in Credential List

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Credentials**. The **Credential List** page is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

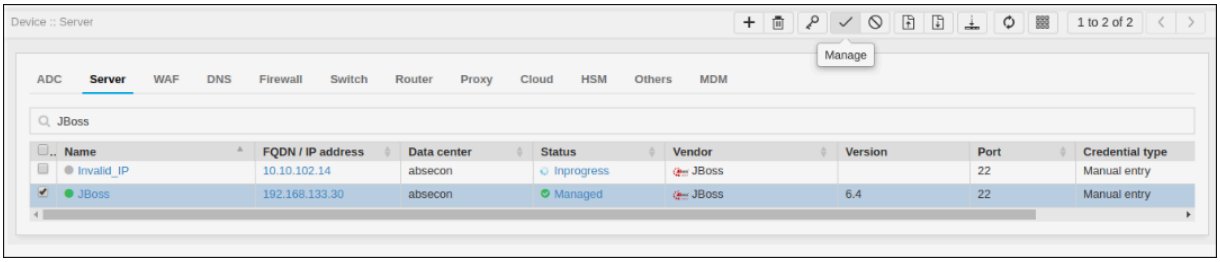
Error Messages

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Issues in Managed Server

Issues in the Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.



Error Messages

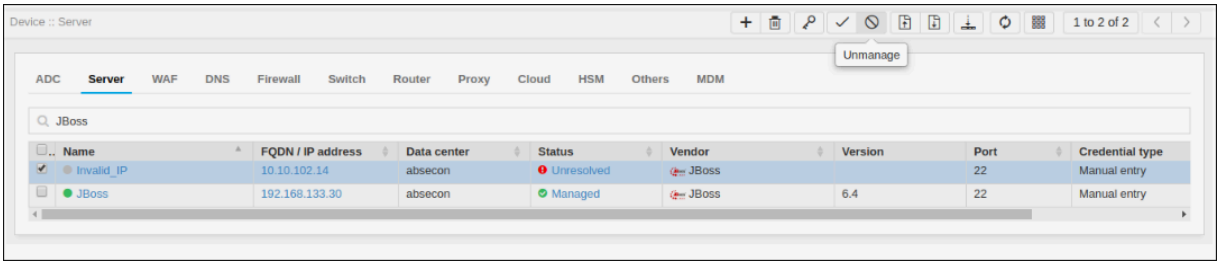
Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Unmanaged Server

Issues in the Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

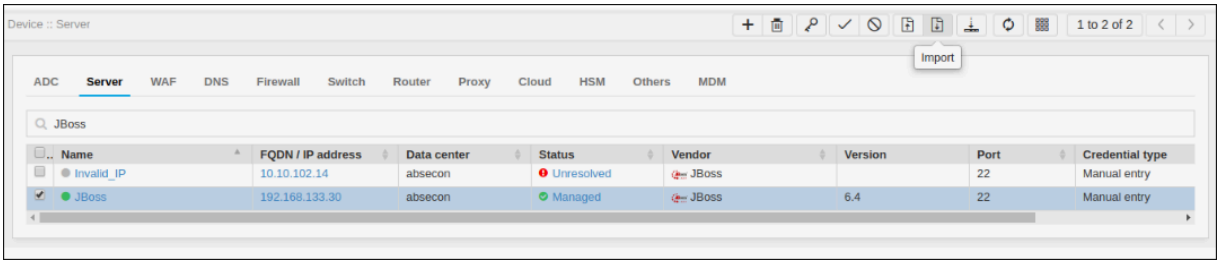
Issues in Import Server

Issues in the Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



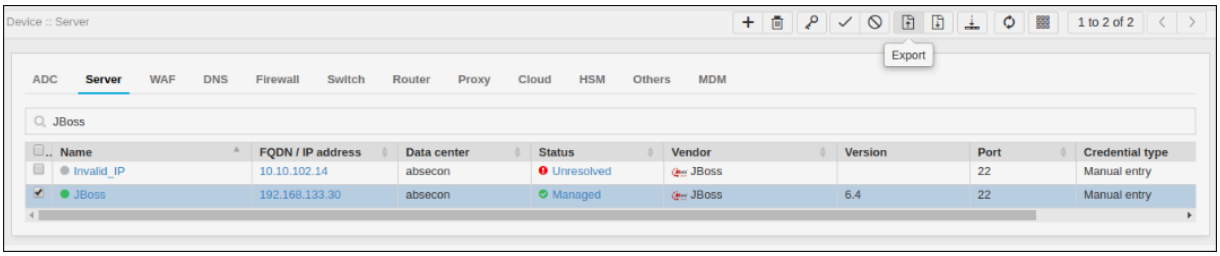
Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are CSV/Xls/xlsx only. Check for the extension of the uploaded file.
Maximum five files allowed, please delete any completed file.	Maximum of 5 files can be maintained in file history of import page.	Delete any of the parsed/completed files to upload a new one.

Issues in Export Server

Issues in the Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Export**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

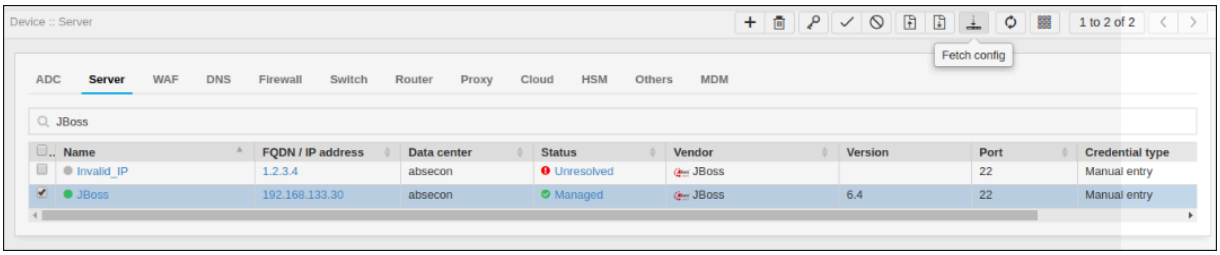
Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue. Unable to fetch device list from the database.	Provide access to be able to create the file on the local system. (e.g. check the directory where it is trying to export and give access to AppViewX for that directory) Make sure the database is running and has correct data.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	Verify the input details and check device status error messages Issues in Communicating to Linux JBoss Server

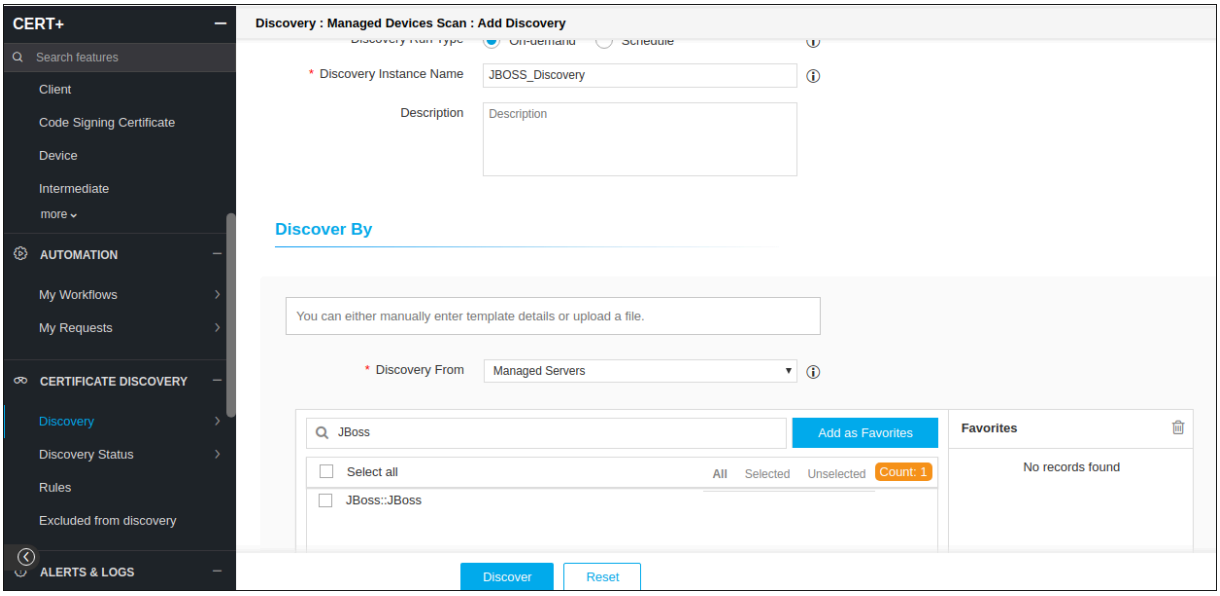
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

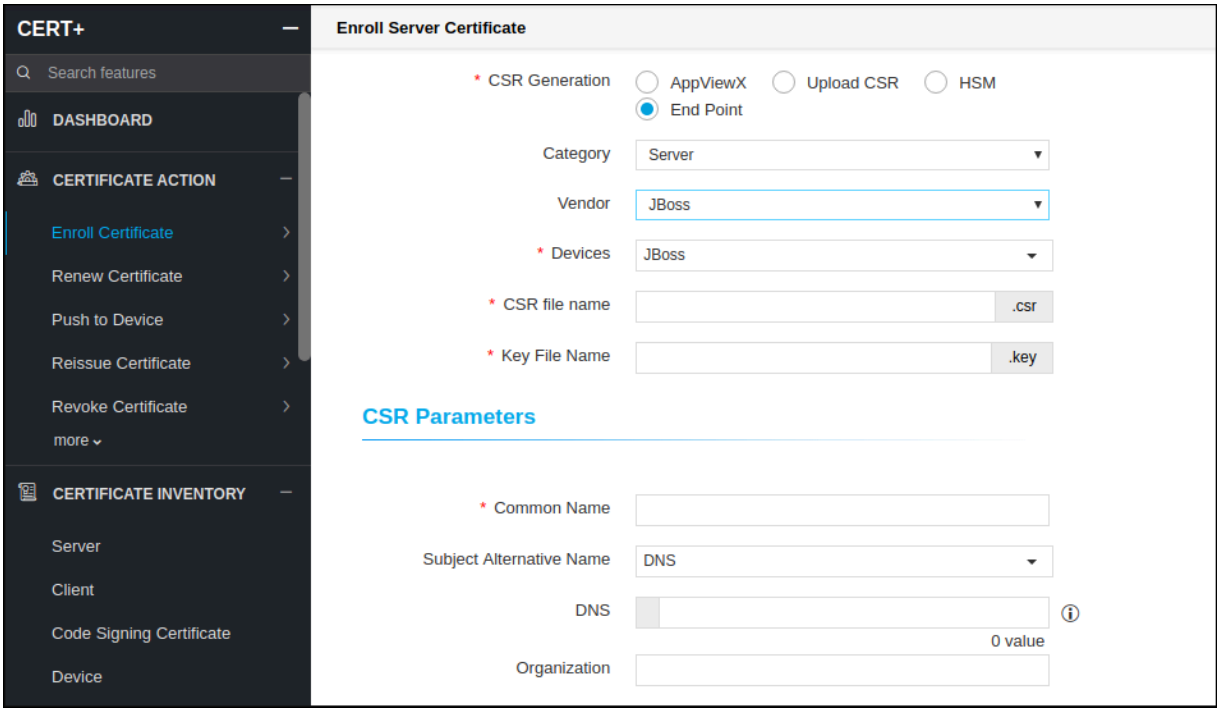
Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category.**
7. From the **Vendor** dropdown, click **JBoss**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.

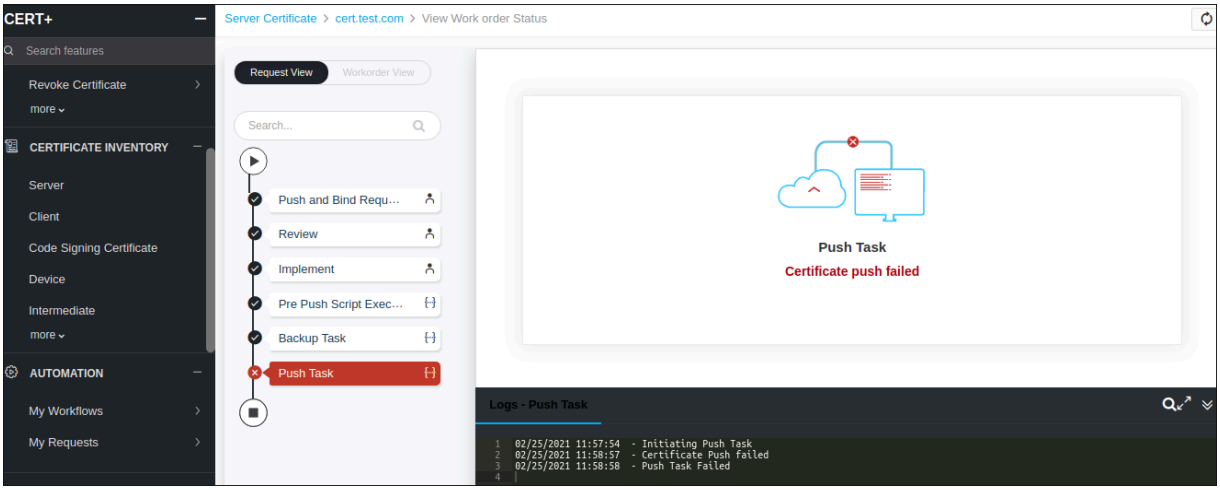
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have the required permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **JBoss server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct “connectorId” if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR generate option from Device.

Troubleshooting Microsoft Enterprise CA

Overview

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Enterprise.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

- Issues in Configuring Microsoft Enterprise CA and Fetch CAs
- Issues in the Certificate Lifecycle Management of a Microsoft Enterprise CA Certificate
- Issues in Revoking Microsoft Enterprise certificate
- Issues in Suspending Microsoft Enterprise certificate
- Issues in Reinstating Microsoft Enterprise certificate
- Issues in Discovering Microsoft Enterprise certificates

Issues in Configuring Microsoft Enterprise CA and Fetch CAs

Configuring Microsoft Enterprise CA

For instructions on configuring Microsoft Enterprise CA using the AppViewX user interface, click here.

Error Messages and Resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already	Check the CA Setting name, it should be unique.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	exists in inventory.	
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with the format	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn –s http/machinename domain\username. • Please note this will work in environments where Kerberos Authentication is set up and there is an AD Domain Setup

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	HTTP/ <SERVER> is not configured for the target.	• If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) **OR** **Error Code 0x80070005 - Access is denied**	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "`Enable-PSRemoting -force`". 4. Execute "`netsh winhttp show proxy`" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		• Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig". • Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests. 5. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. 6. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	The Remote Procedure Call Service is not responding.	Navigate to the target machine and start RPC service if it has stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		• Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached.	• Windows Gateway is not reachable from AppViewX. • Windows Gateway service is down.
Html response : Access is denied	Access is denied.	• In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		have intermediate certificates only. • Client certificate used in AppViewX is not imported in Target machine's Local computer store.

More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator
		1. Check existing config winrm get winrm/config.
		2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		.

Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. **This user is allowed a maximum number of 4 concurrent shells, which has been exceeded.** **Close existing shells or raise the quota for this user.**	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution

		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		
		.

Client Certificate gives Permission Denied 403 error. **This can happen in certain environment and its intermittent**	CA Store mismatch or invalid client certificate used.	Check if the Client certificate is installed correctly by checking the chain in the Personal Store. • Root of the client certificate should be available in the Trusted Root Certification Store of the Server. • Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. • If all the above looks good then go to the agent server and do the following steps 1. MMC. 2. Add “Add/Remove SnapIn. 3. select certificates. 4. select “LocalMachine”. 5. Navigate to the Personal Store and click on the client certificate. 6. Navigate to Chain.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		7. Export the Root certificate and save it as Root.cer in a location. 8. Import the “Root.cer” into trusted Root back again. 9. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. 10. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. 11. Take a backup of such certificates and move it to respective stores. 12. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
The permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.	Check if the credentials are valid.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
• **There is not enough space on the disk** • **The WSMan service could not launch a host process to process the given**	There is not enough	Ensure that your hard disk has enough free space.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
request. Make sure the WSMan provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. • **Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fail within the expected range.**	space on the disk.	
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		configured username is part of the administrator group. • or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Issues in the Certificate Lifecycle Management of a Microsoft Enterprise CA Certificate

Managing Microsoft Enterprise CA Certificates

For instructions on enrolling a Microsoft Enterprise CA certificate, click here.

For instructions on renewing a Microsoft Enterprise CA certificate, click here.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

For instructions on regenerating a Microsoft Enterprise CA certificate, click here.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn’t have access	Please give access to the user.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	to the template.	
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it and select

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec). 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add “Add/Remove SnapIn.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save it as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected template/CA's Policy.	Supply valid CSR values accepted by template or CA policy.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Issues in Revoking Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Revoke Certificate** submenu.
4. Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
5. From the menu bar at the top of the page, click **List**.
6. Click any **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
7. From the dropdown menu next to the **Certificate**, click **Revoke**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Issues in Suspending Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Suspend**.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Enterprise certificate

Issues in the Microsoft Enterprise Certificate

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and Click **Server/Client/Code Signing Certificate**. The **Server Certificate/Client Certificate/Code Signing Certificate** page is displayed.
4. From the menu bar at the top of the page, click **List**.
5. Click any suspended **Microsoft Enterprise certificate**. A holistic view of **Server Certificate** with the **Certificate number** will be displayed.
6. From the dropdown menu next to the **Certificate**, click **Reinstate.**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Issues in Discovering Microsoft Enterprise certificates

Issues in the Microsoft Enterprise Certificates

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery** and select **Discovery**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Certificate Authority Scan**. The **Discovery: Certificate Authority Scan: Add Discovery** page is displayed.
5. Select **CA** as **Microsoft Enterprise**.
6. Click **Discover** at the bottom of the page.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting Microsoft Tomcat

• Overview
• Issues in Microsoft Tomcat Server Addition using AppViewX UI
• Issues in Communicating to Tomcat Server
• Issues in Accessing Server

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Config Fetch
• Issues in Certificate Discovery
• Issues in CSR generation
• Issues in Push and Rollback

Overview

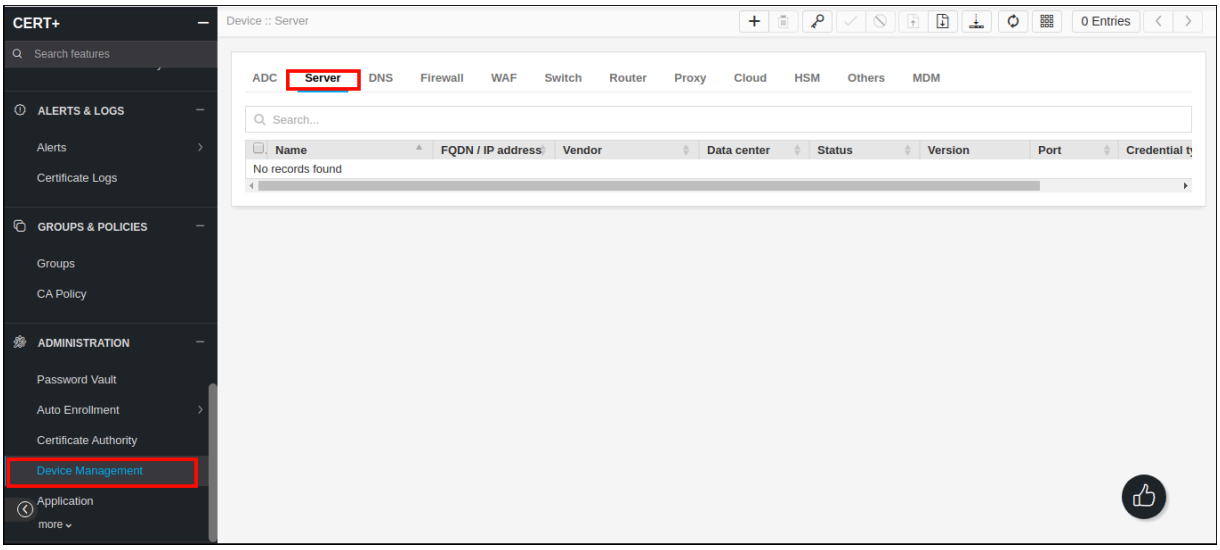
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Microsoft Tomcat server.

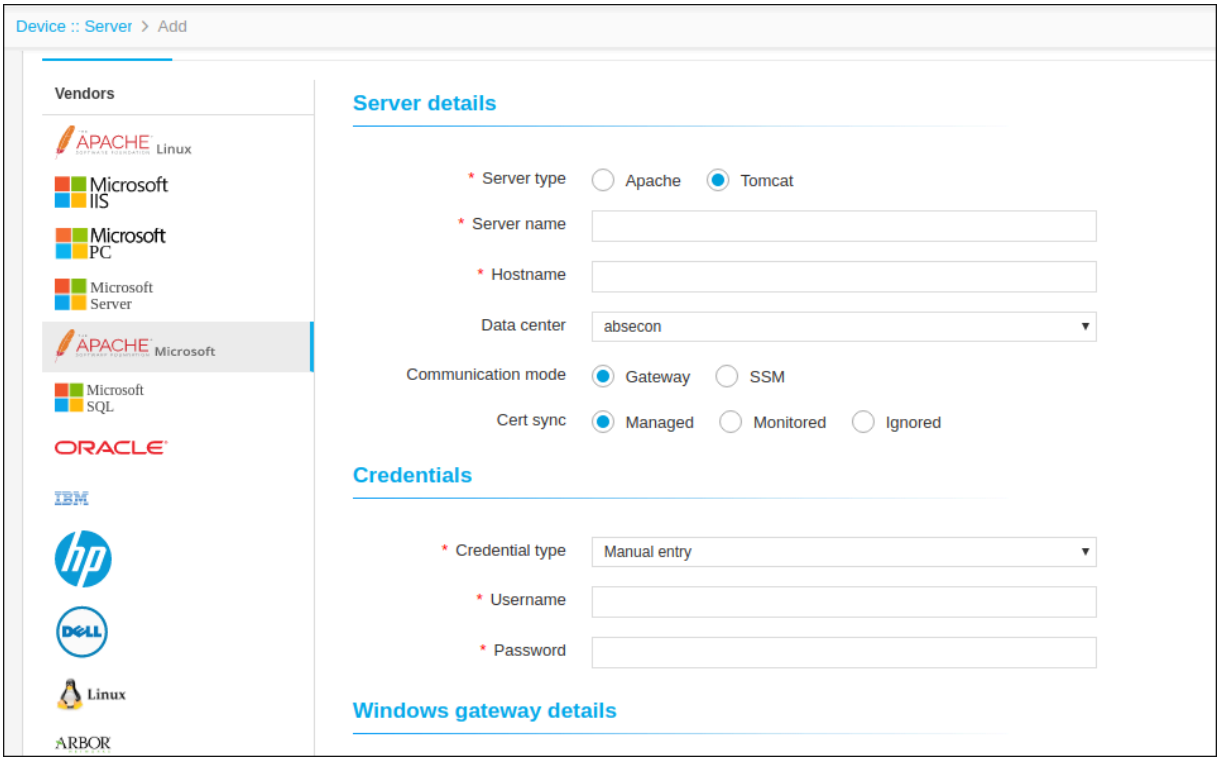
Issues in Microsoft Tomcat Server Addition using AppViewX UI

Issues in the Microsoft Tomcat Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **APACHE Microsoft**, **server type Tomcat**.
7. Fill in the appropriate details.
8. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name exists in inventory.	Check the Device name, it should be unique.

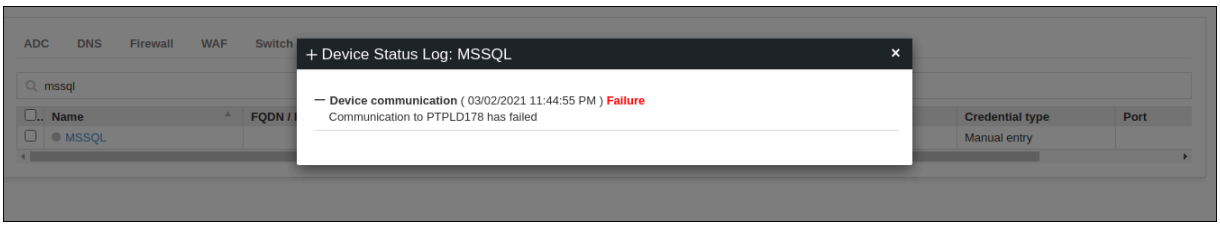
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

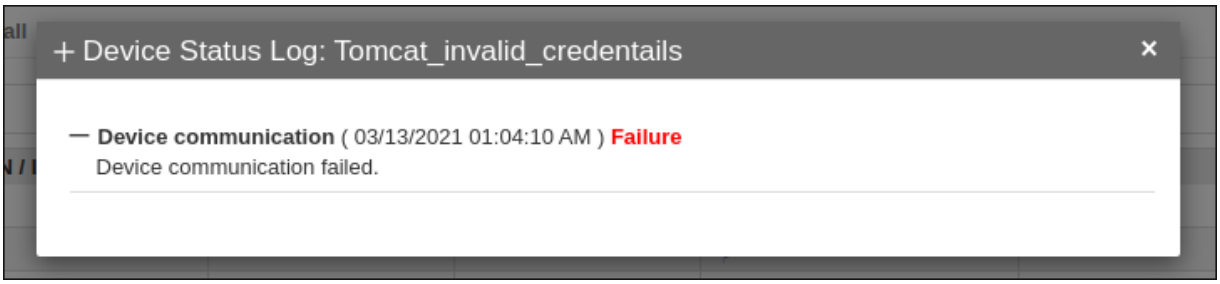
Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Tomcat Server

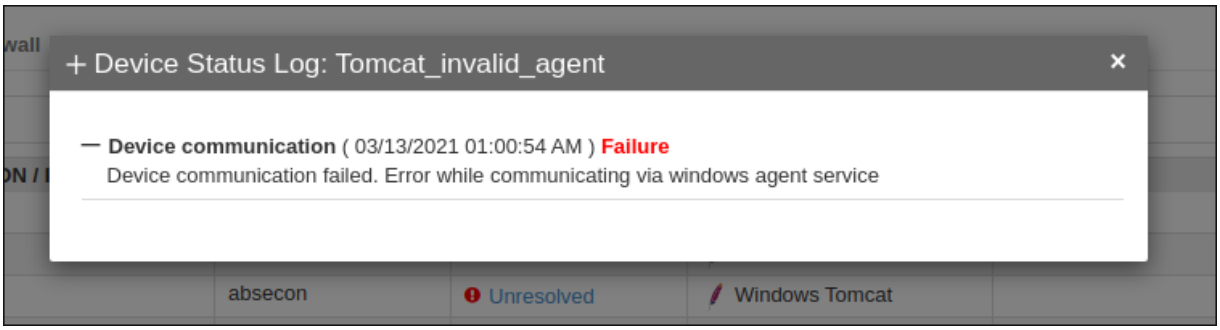
Issues in the Communicating to Tomcat Server

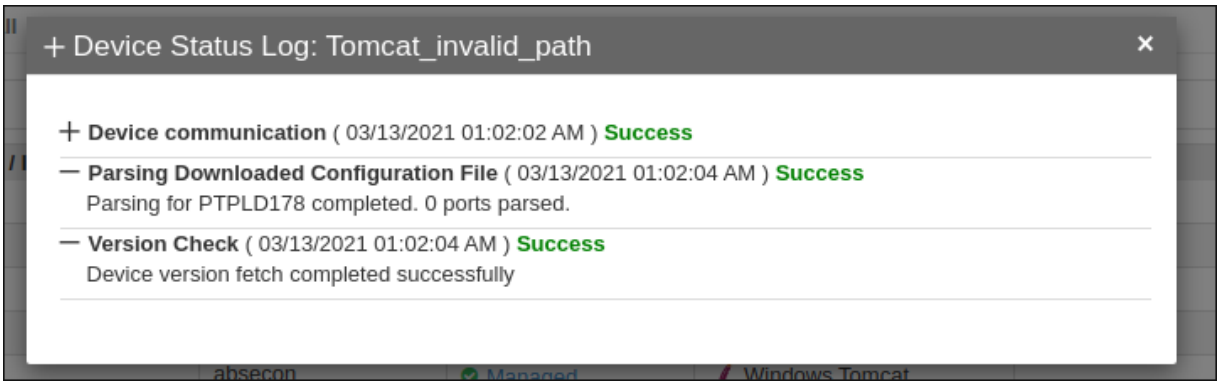
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added	Click on the device name in the Inventory Page. Update the correct details and click Save.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	might be wrong.	
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Parsing for PTPLD178 completed. 0 ports parsed.	Invalid Tomcat Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page
Error on fetching Tomcat instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location.

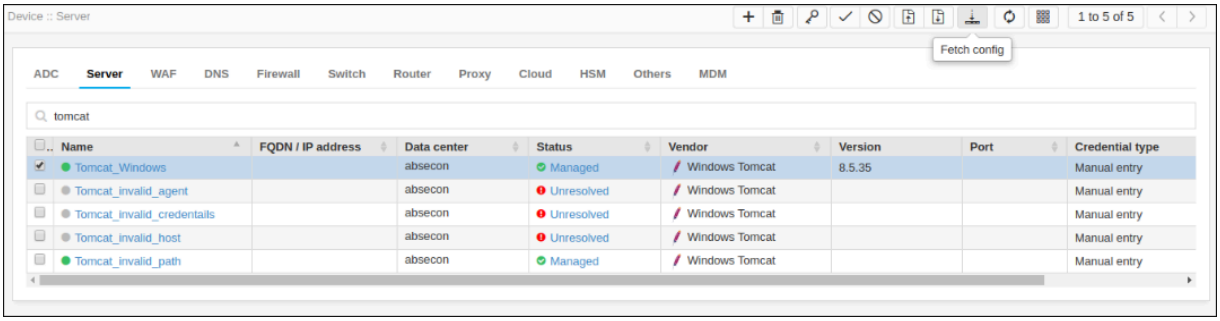
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	3.Device communication might not be established when service has started.	3.Verify the device connection and restart the service.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	1.Verify the input details and check for device status error messages Issues in Communicating to Tomcat Server

Issues in Certificate Discovery

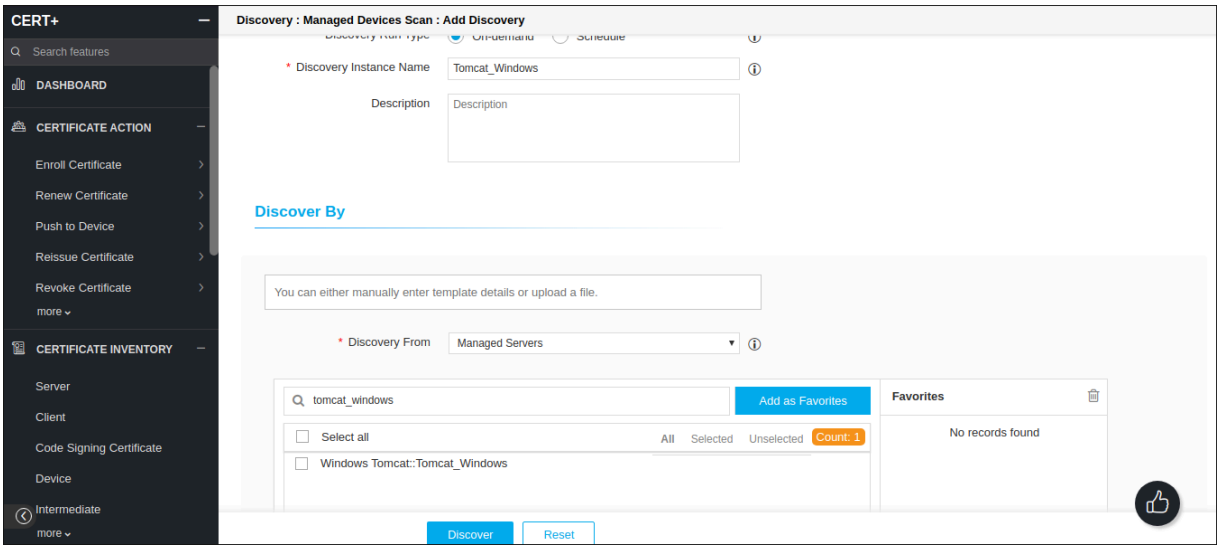
Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

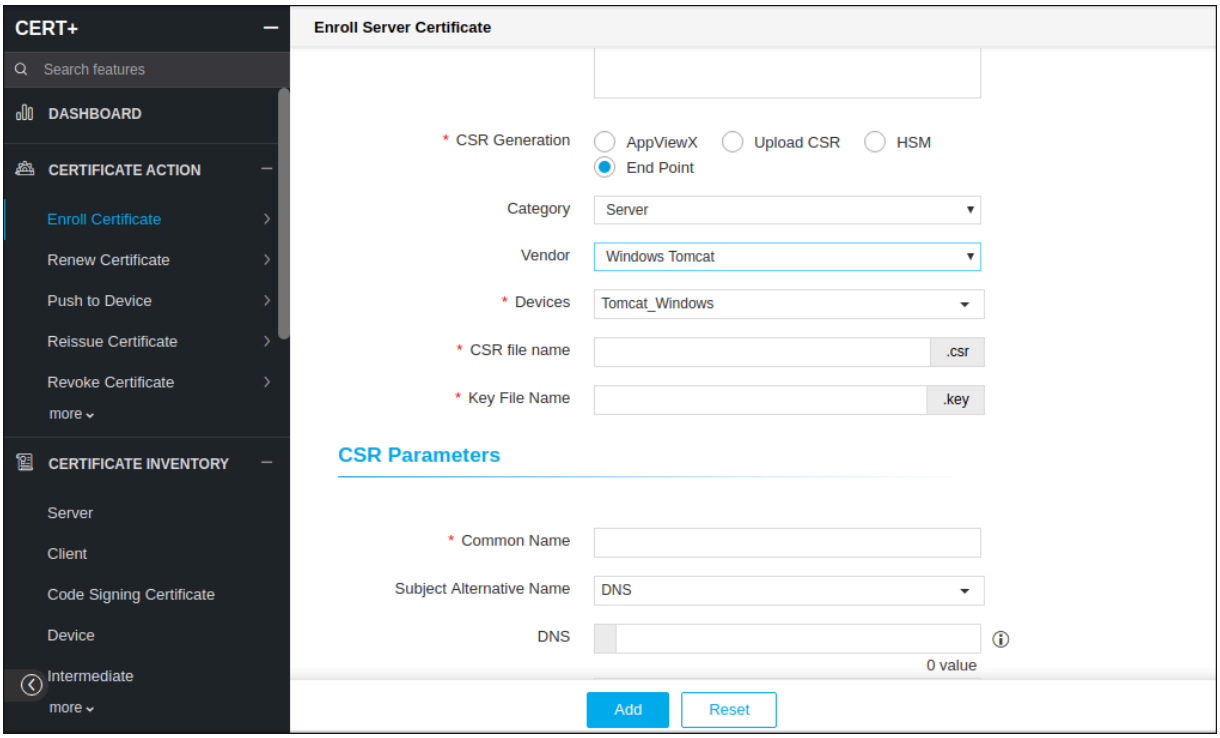
Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Windows Tomcat**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.

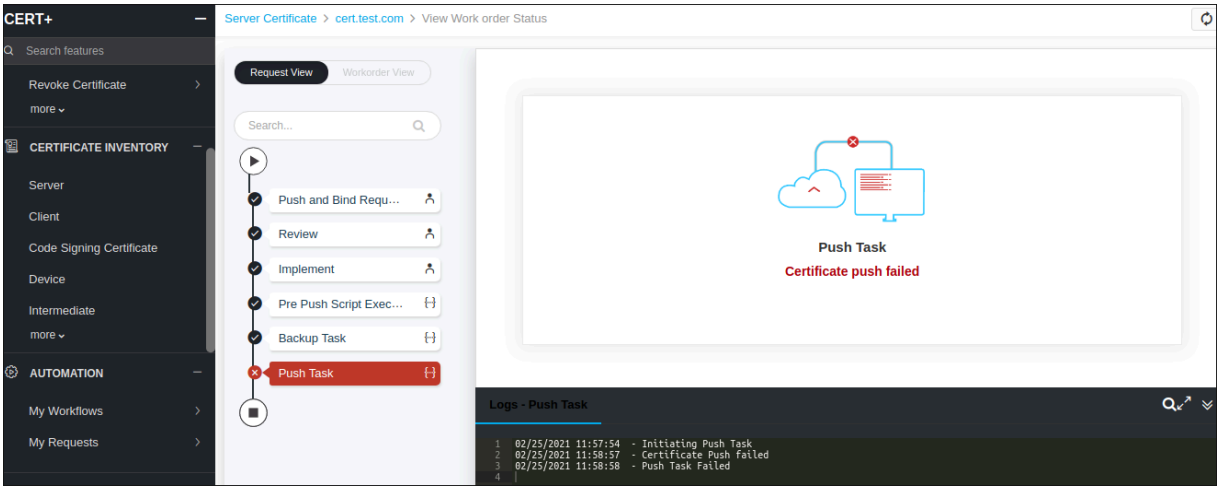
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

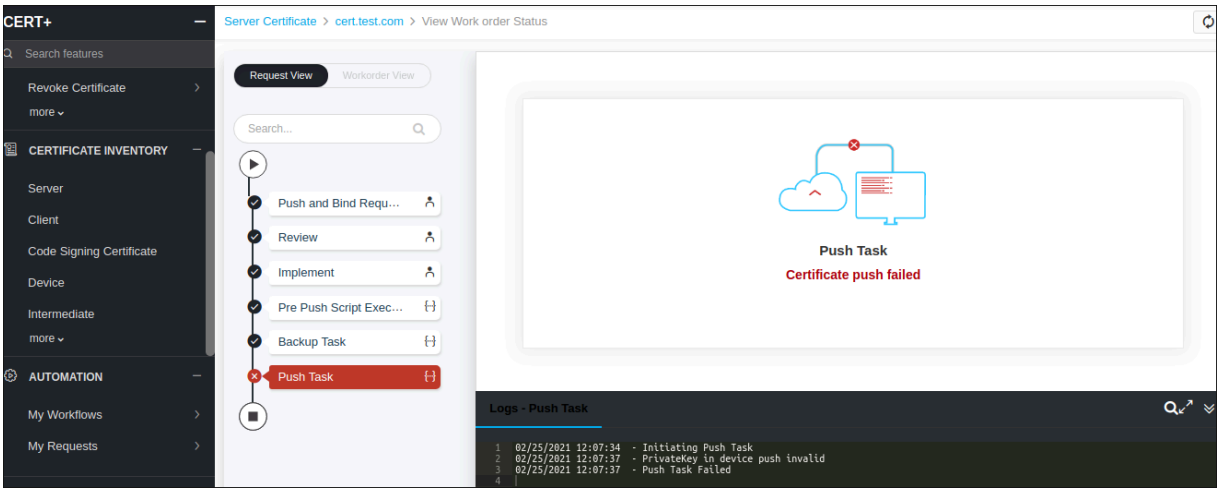
Issues in Push and Rollback

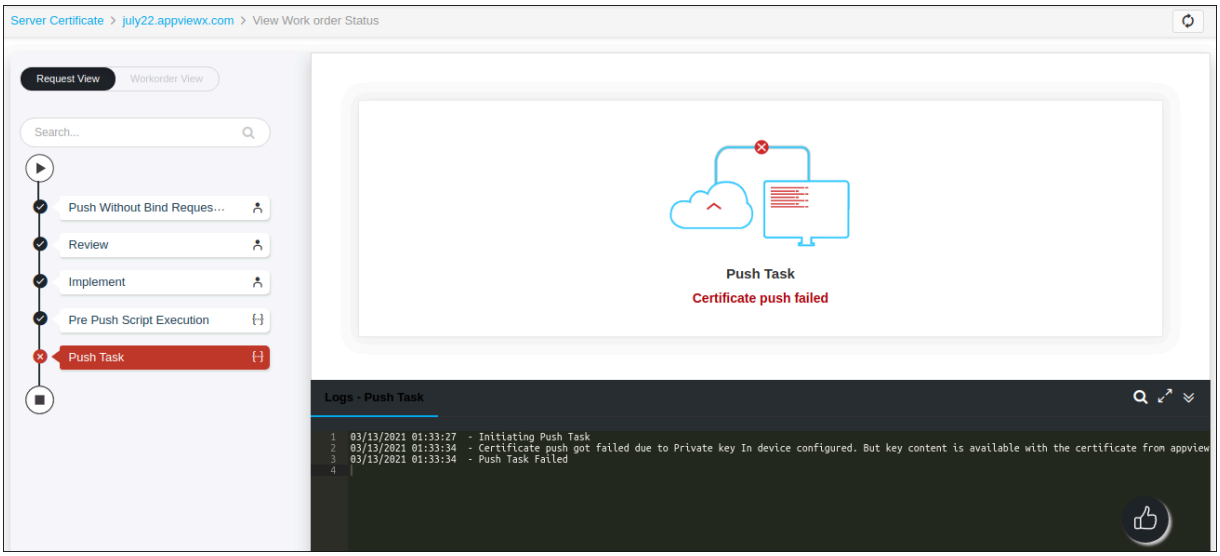
Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Windows Tomcat server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is	Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	unavailable, i.e. in a new state.	
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	“Private key in Device” is enabled in application connector and also private key is available in the certificate	Ensure “Private key in Device” attribute in application connector is unchecked.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting MQServer Linux

- Overview
- Issues in Device communication
- Issues in Certificate Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

This section will guide you to overcome the various issues faced by you during the use of MQServer Linux and its various functionalities.

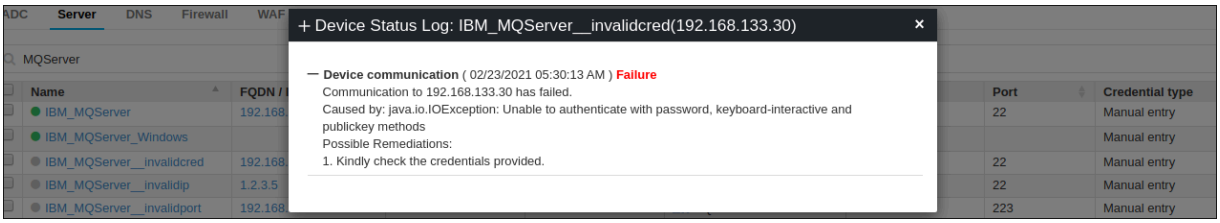
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

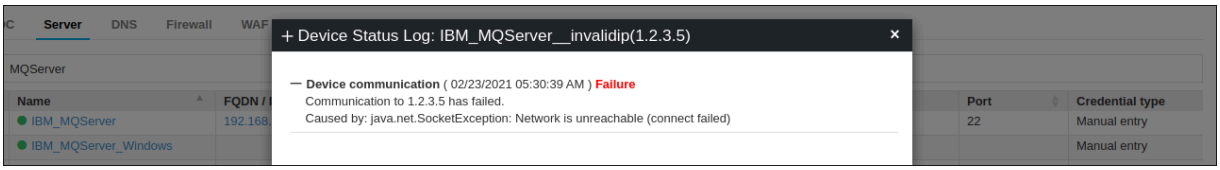
Issues in Device communication

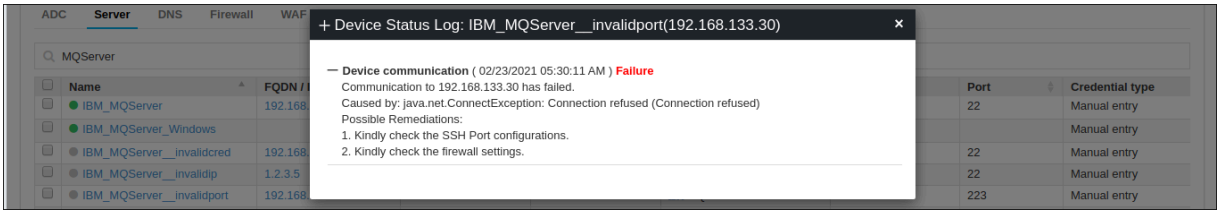
Issues in the Device communication

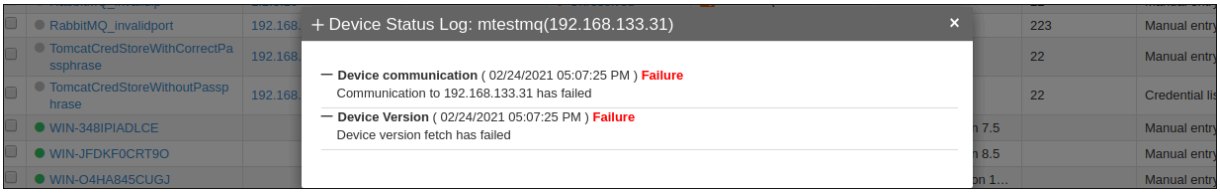
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.











Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added could be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.
Device communication (02/24/2021 05:07:25 PM) Failure	MQ is not configured in the target device	Check if MQ server is configured in the target device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to 192.168.133.31 has failed Device Version (02/24/2021 05:07:25 PM) Failure Device version fetch has failed		Check MQ toolkit is installed in the target device
Device communication (02/24/2021 06:12:50 PM) Failure Communication to 192.168.133.30 has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same

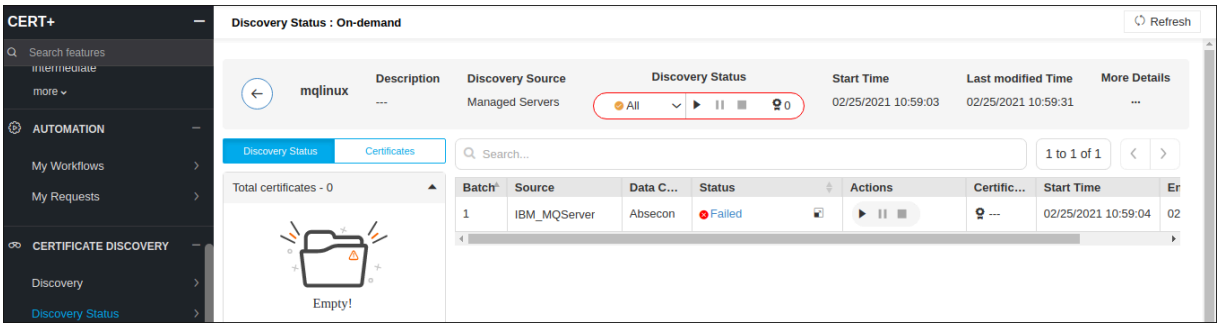
Issues in Certificate Discovery

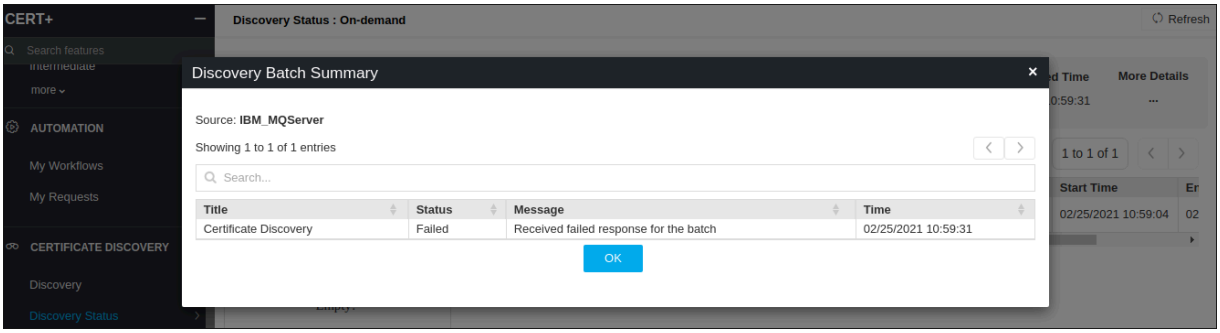
Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

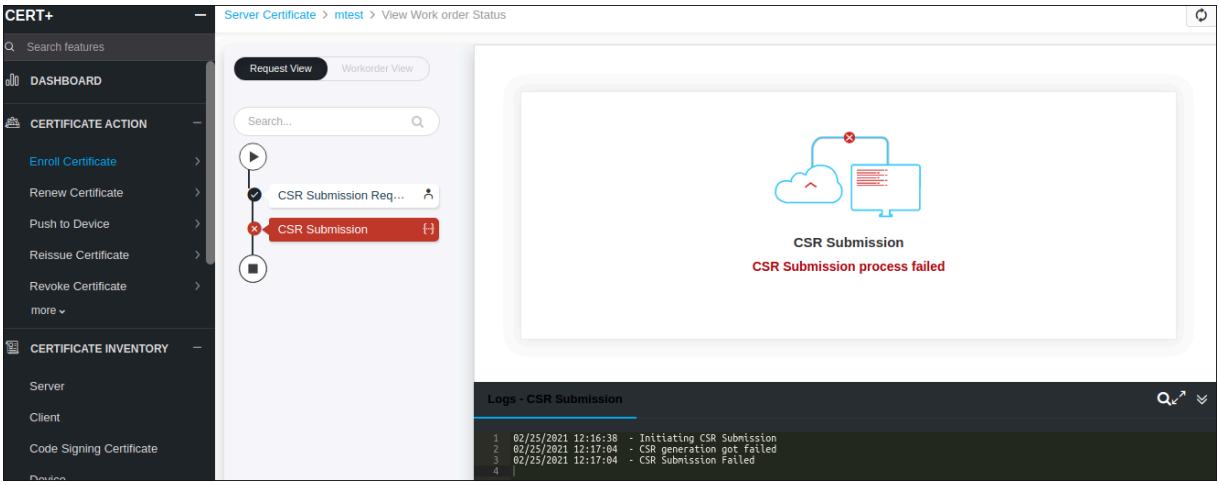
Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command: `strmqm <qname>`
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path: `echo "DIS QMGR SSLKEYR" | runmqsc`

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **MQServer**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

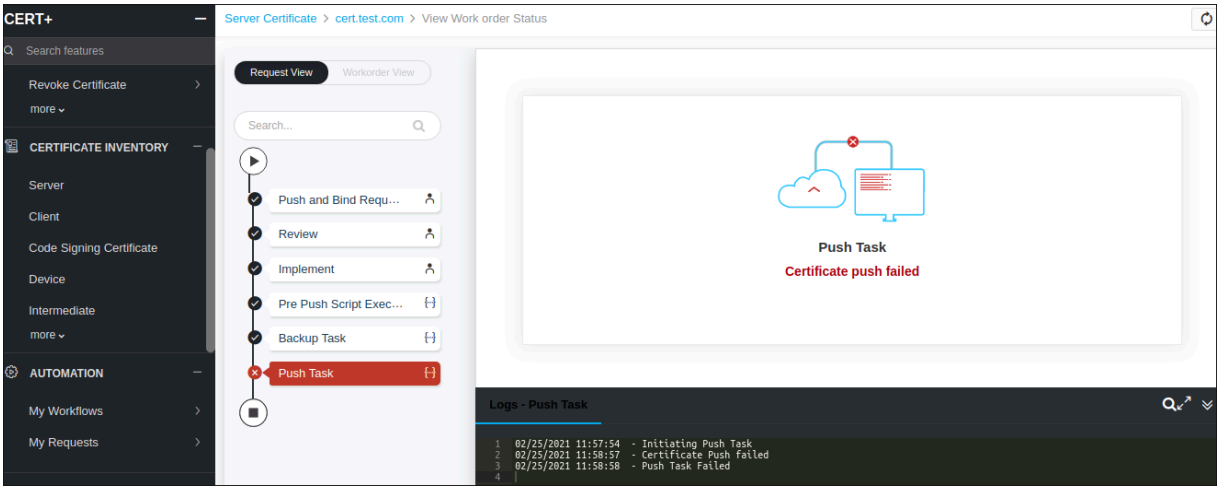
Issues in Certificate Push

Issues in the Certificate Push

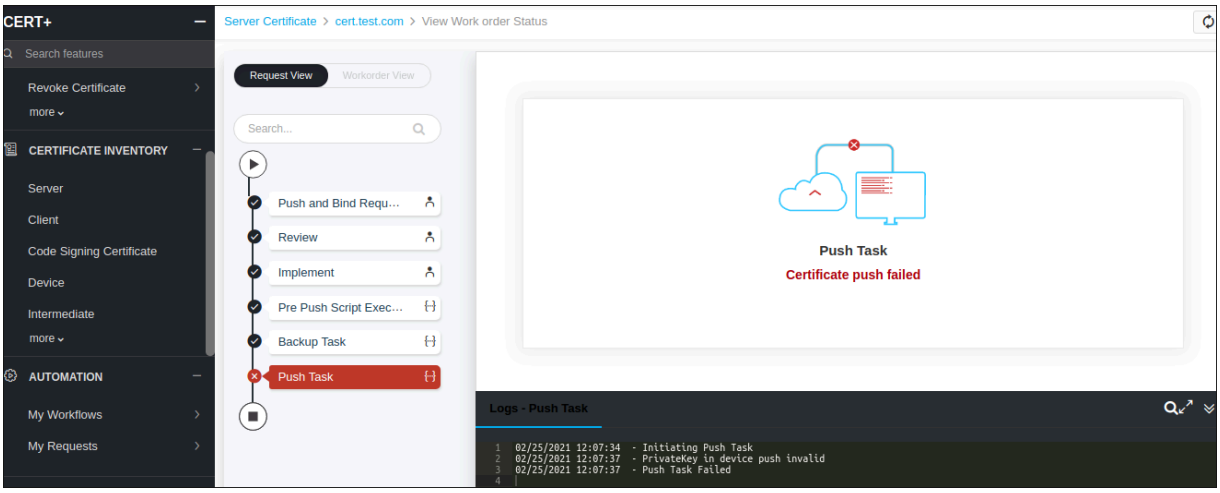
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

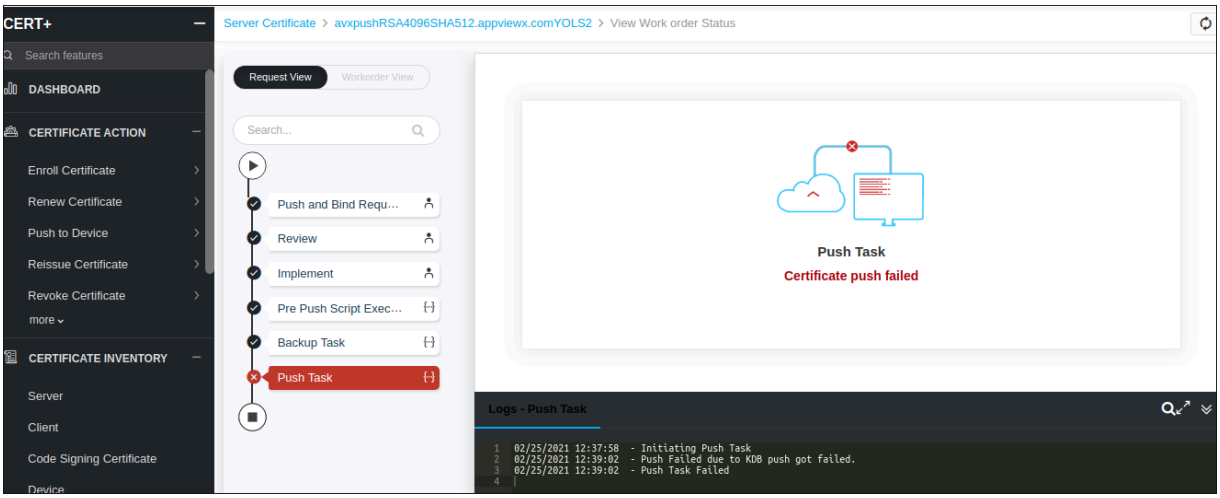
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Linux server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with "**Create KDB**" profile, click **Add App Connector.**
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Troubleshooting MQServer Windows

• Overview

• Issues in Device communication

• Issue in Discovery

• Issues in CSR generation at Endpoint

• Issues in Certificate Push

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with MQServer Windows.

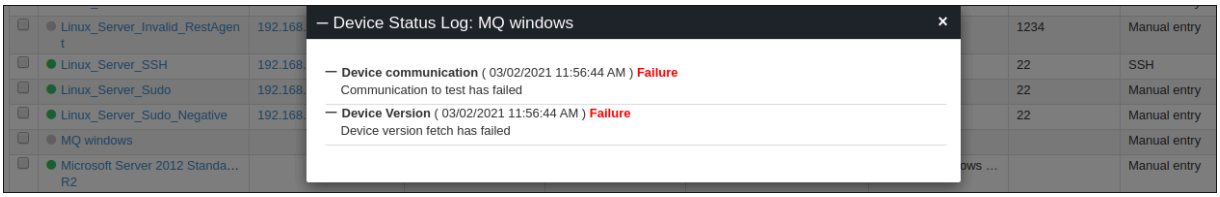
Issues in Device communication

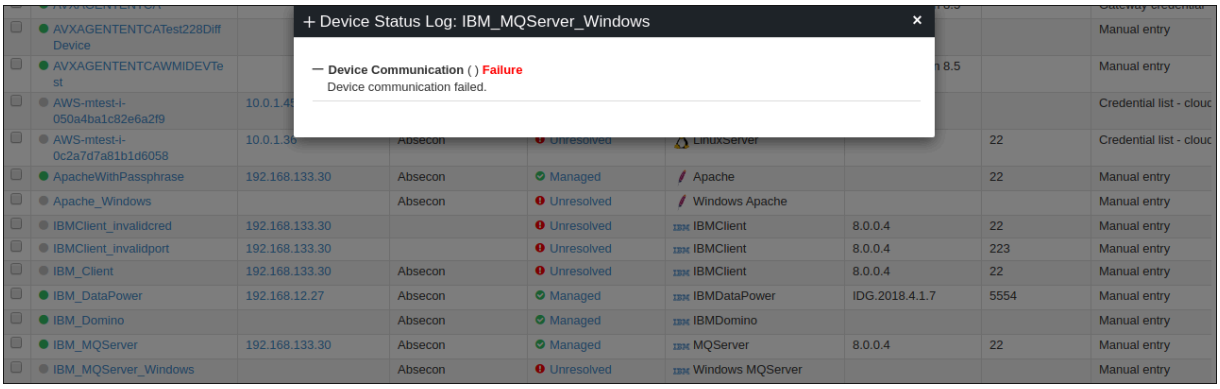
Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Issue in Discovery

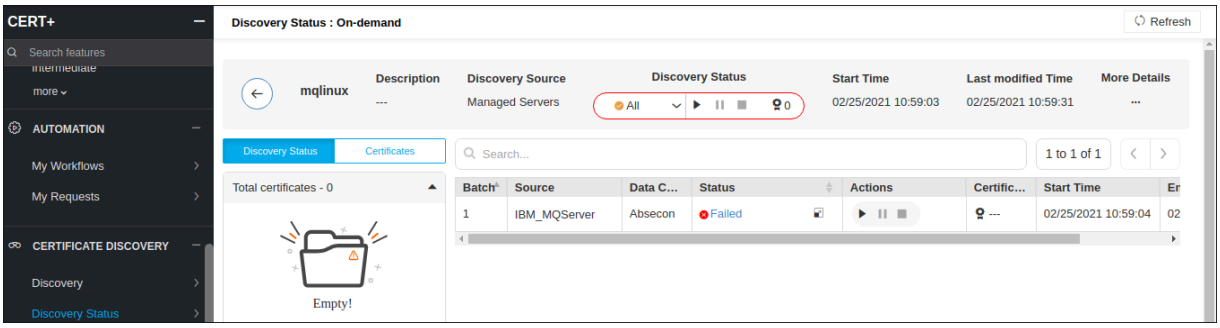
Issue in the Certificate Discovery

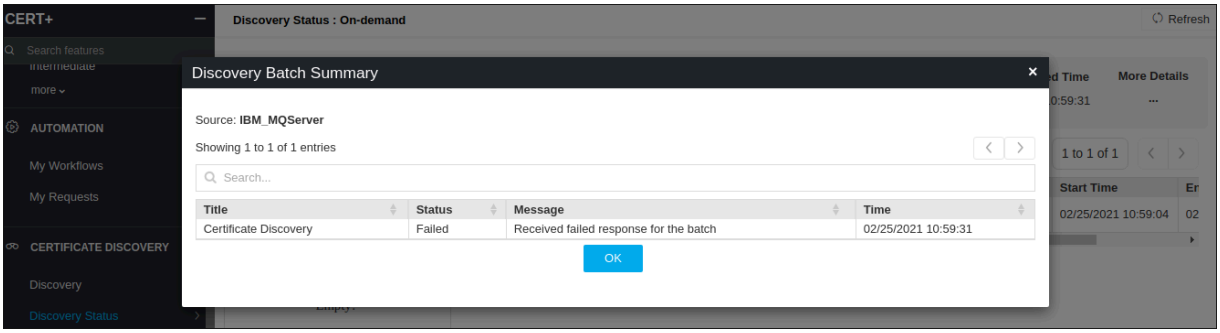
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command:

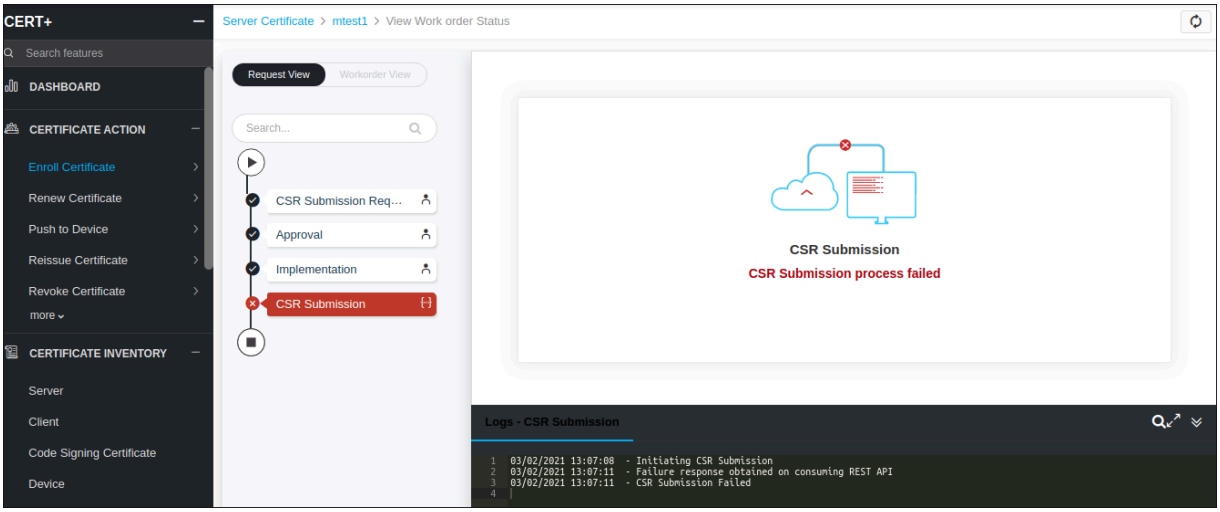
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		strmqm <qname>
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path: echo "DIS QMGR SSLKEYR" | runmqsc.

Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, Click correct **Category**.
7. From the **Vendor** dropdown, click **Windows MQServer**. A list of devices will be generated in the **Devices dropdown**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Mesages

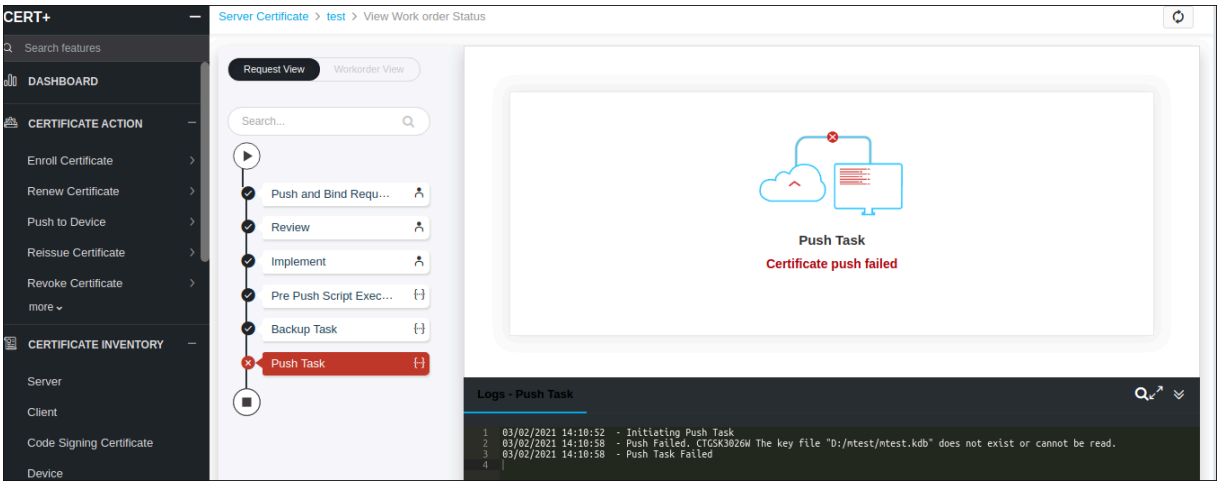
Error Message	Possible Cause	Possible Solution
Failure response obtained on consuming REST API. CSR submission failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

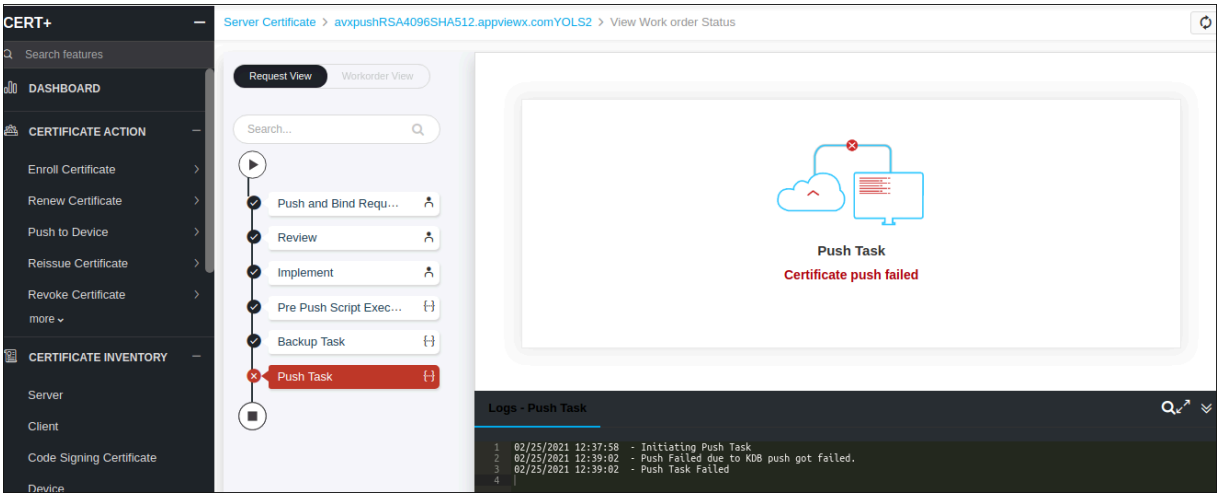
Issues in Certificate Push

Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Linux server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions** with “**Create KDB**” profile, select **Add App Connector.**
6. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read.	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting MS SQL Windows

- Overview
- Issues in Communicating to MS SQL
- Issues in Config Fetch
- Issue in Discovery
- Issue in CSR generation
- Issue in Push and Rollback

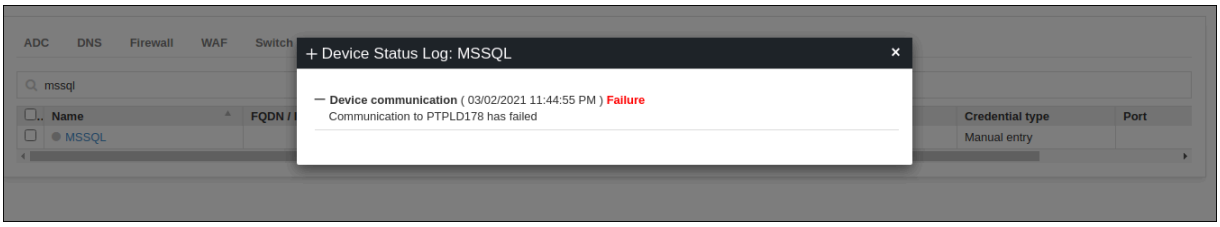
Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback and other actions associated with MS SQL Windows.

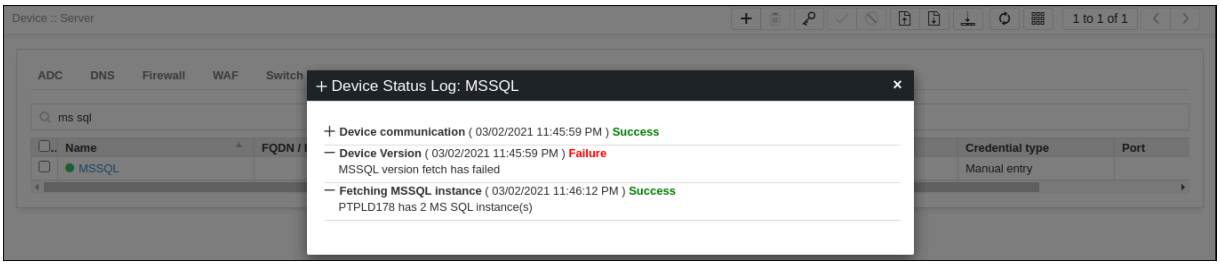
Issues in Communicating to MS SQL

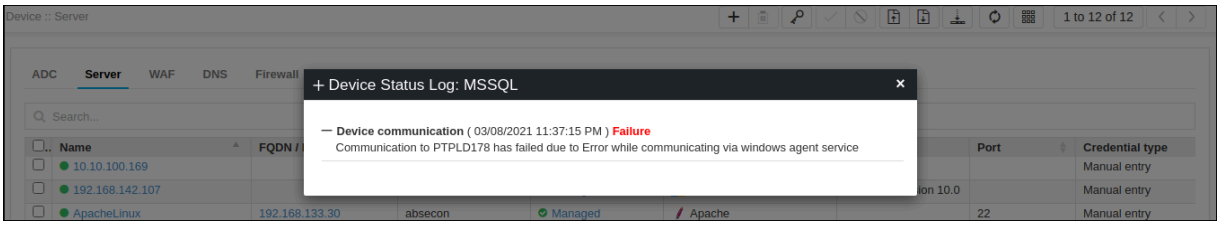
Issues in the Communicating to MS SQL

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> has failed	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.
Device version fetch has failed.	MSSQLSERVER service instance is down	Restart the MSSQLSERVER instance
Device version fetch has failed.	Command not supported by MS SQL version	Execute the version command SQLCMD -Q 'SELECT @@VERSION;' -t 3 in the CLI of the device to check if it returns version response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.

Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
PTPLD178 has 0 instances.	No installed MS SQL instances. Installed instances are not up and running.	Execute (get-itemproperty 'HKLM:\\SOFTWARE\\Microsoft\ \Microsoft SQL Server').InstalledInstances in the device as a powershell script and check if it returns the MS SQL instances

Issue in Discovery

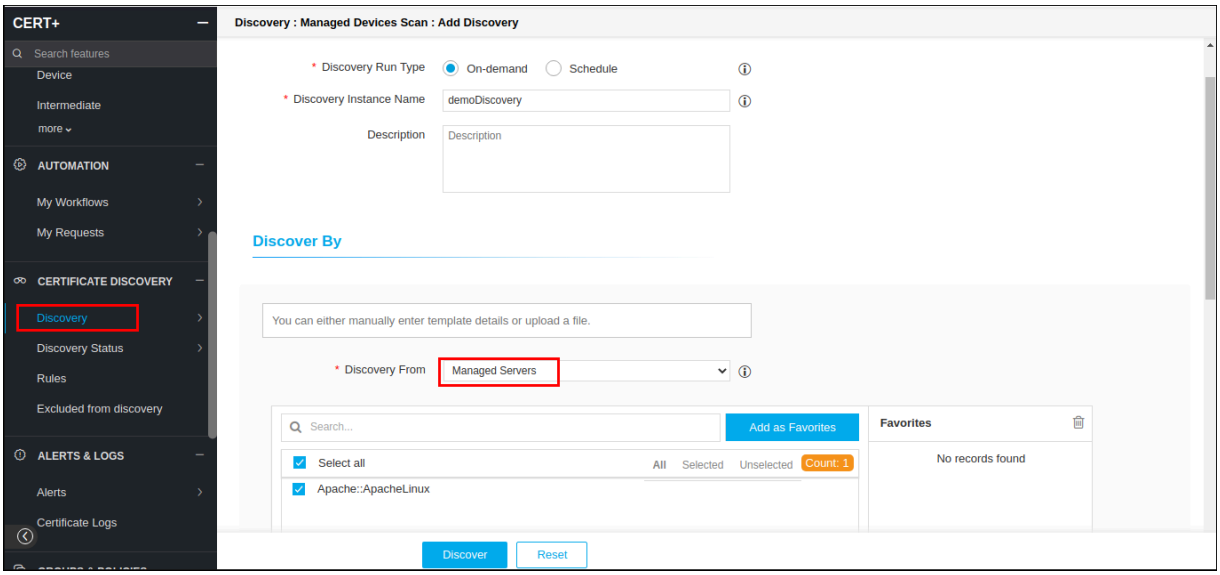
Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid certificates in store that are binded to the MS SQL instances.	Ensure the certificates are binded to a MS SQL instance.

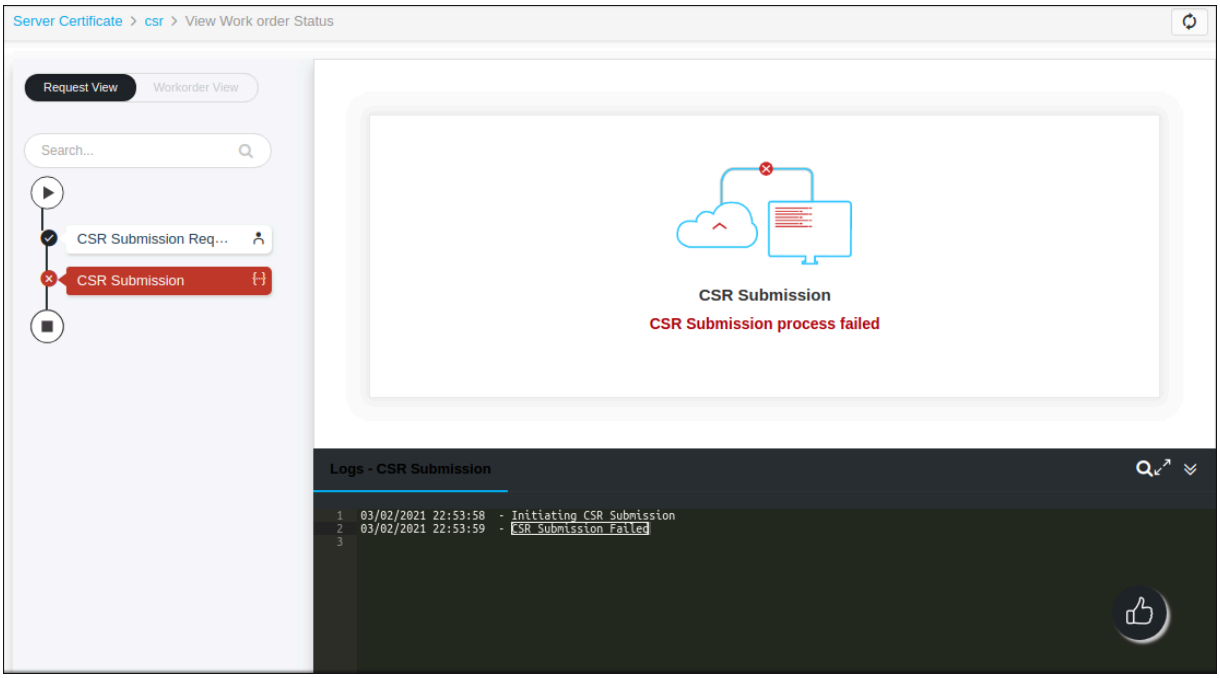
Issue in CSR generation

Issue in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **MS SQL**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

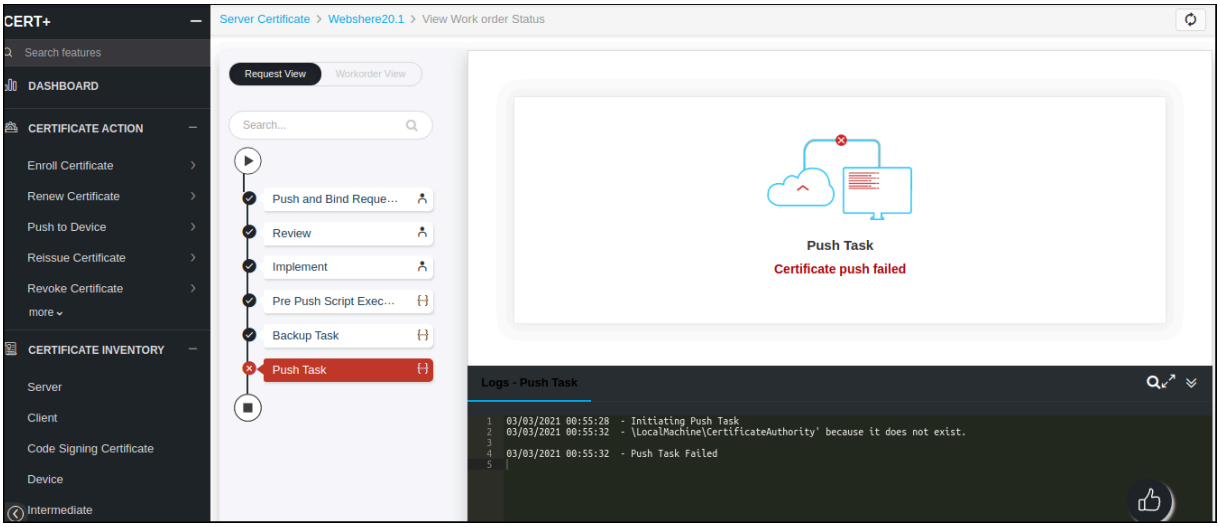
Issue in Push and Rollback

Issue in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Push the certificate to the device.



Error messages

Error Message	Possible Cause	Possible Solution
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key.If privatekey is available in device please select privateKeyInDevice option.
Error: “/LOCAL_MACHINE/ CertificateAuthority” does not exist	CertificateAuthority Store is removed from the Store	Create a CertificateAuthority store.

Troubleshooting Nginx Server

- Overview
- Issues in Device communication
- Issue in Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

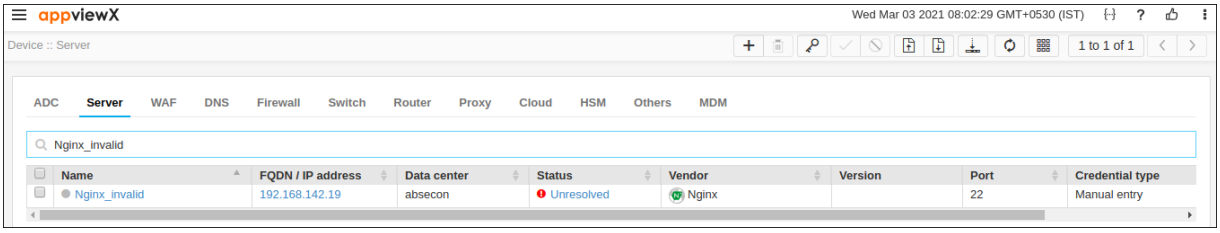
This section helps you troubleshoot the common problems that you might encounter when using certificate Nginx Server functionalities.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Nginx** Device, click **Status**. The **Device Communication Status** is displayed.





Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	1. Given credentials are incorrect. 2. Given IP may be incorrect.	1. Check and input the correct credential. 2. Check and input the correct IP

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

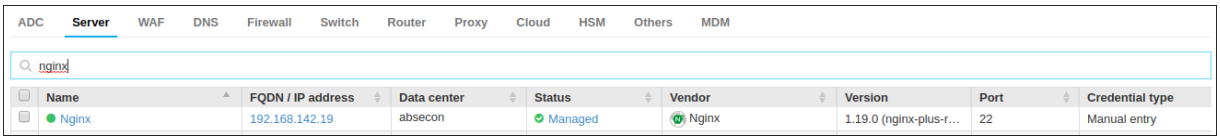
Error Message	Possible Cause	Possible Solution
	3. Device not reachable	3. Ensure device is up and accessible

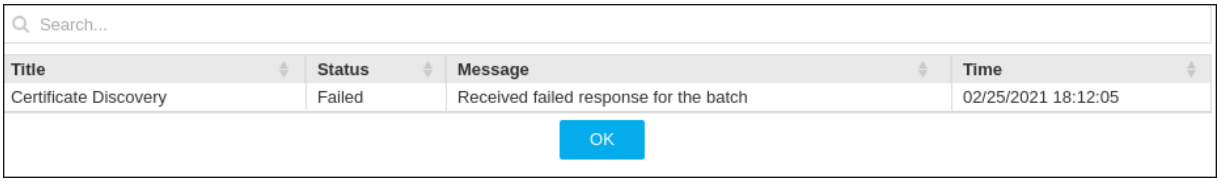
Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





Error Messages

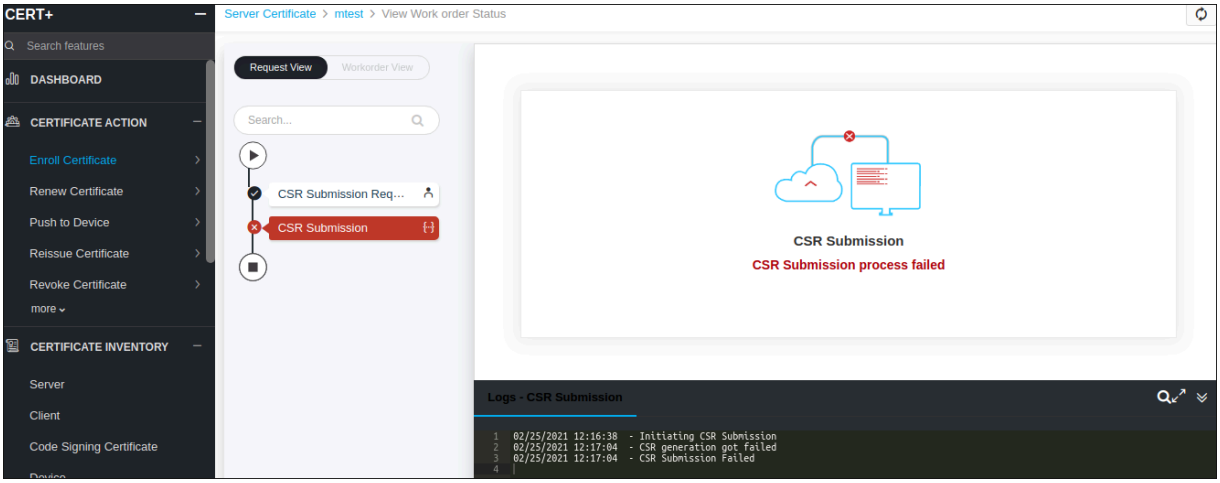
Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Nginx** device. A list of devices will be generated in the **Devices dropdown**.



Error Messages

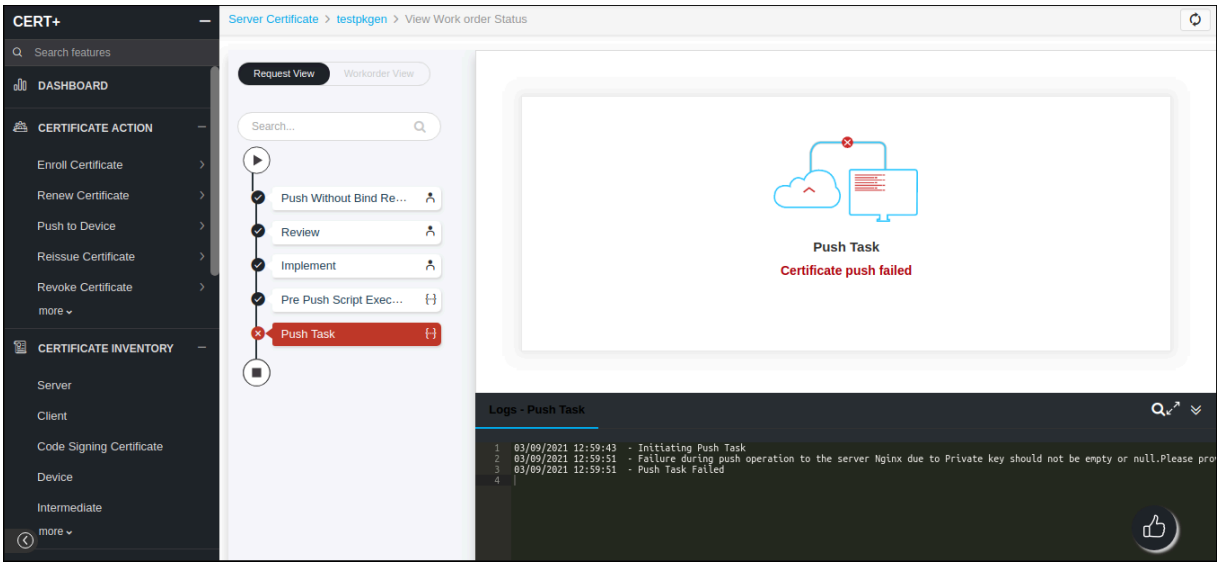
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1.Kindly ensure the user configured for device addition has read/write access to the path configured. 2. For sudo user, Please check the access elevation configured in device addition

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

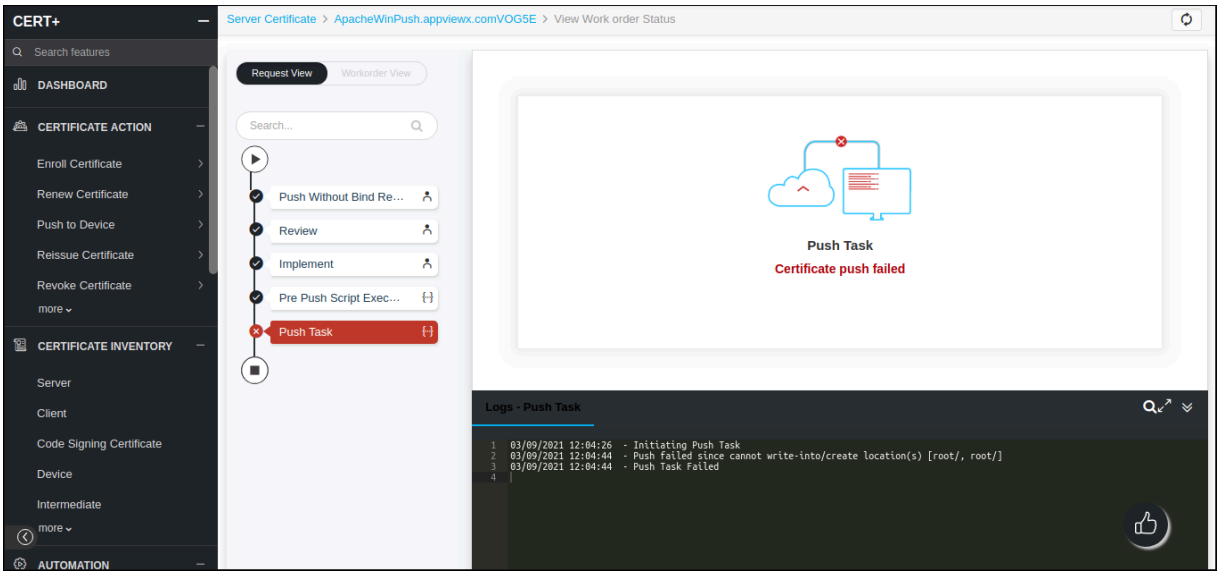
Issues in Certificate Push

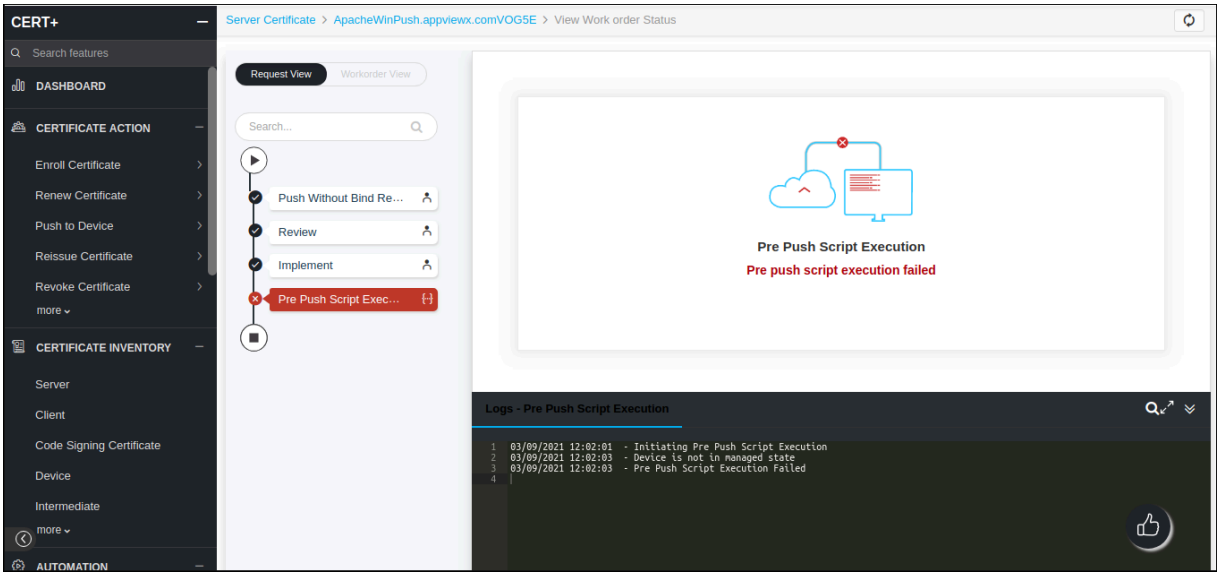
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Nginx server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Failure during push operation to the server Nginx due to Private key should not be empty or null.Please provide valid key to proceed push.	Private key not available in push request certificate	Please ensure the private key is available in request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Pivatekey In device configured. But key content is available with the certificate from AppViewX.. So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting NginxPlus ADC

- Overview
- Issue in Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with NginxPlus ADC.

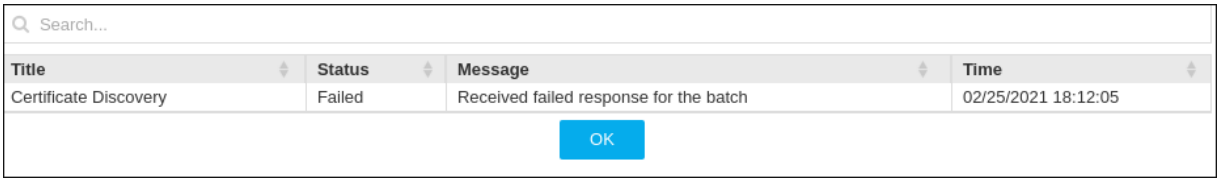
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

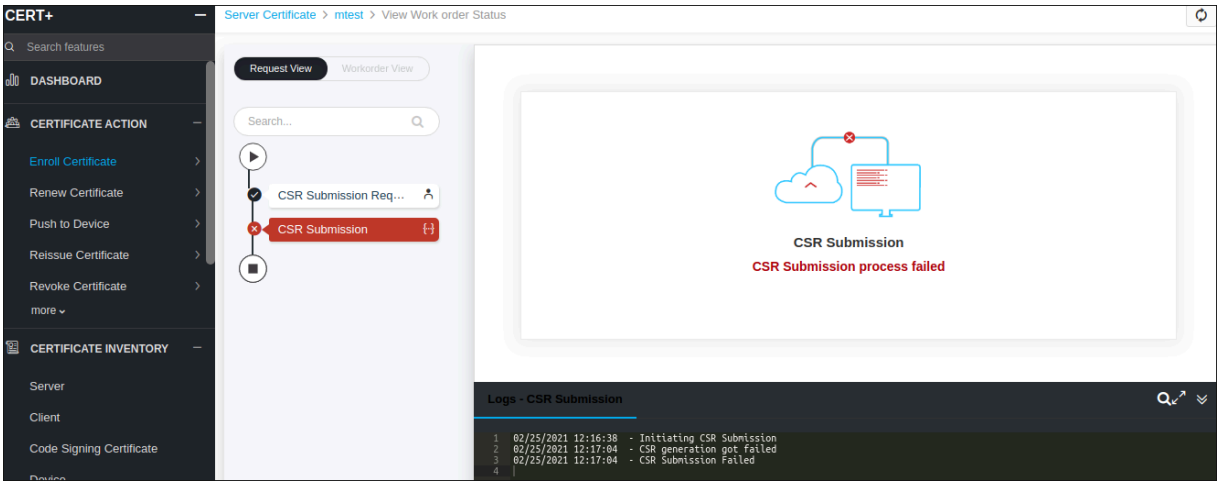
Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **NginxPlus**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

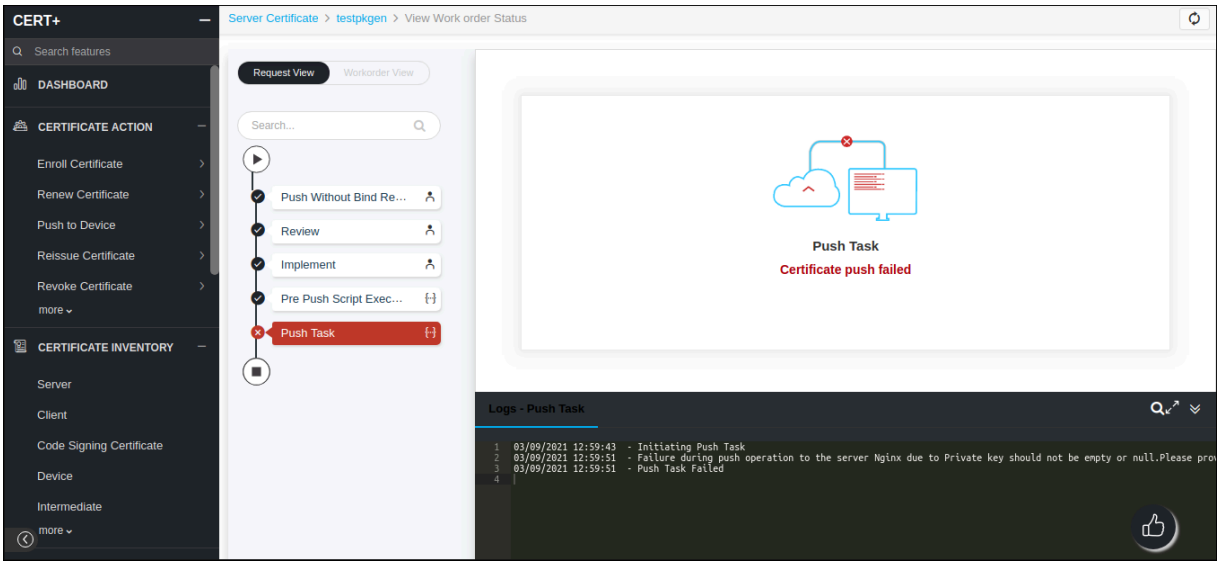
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

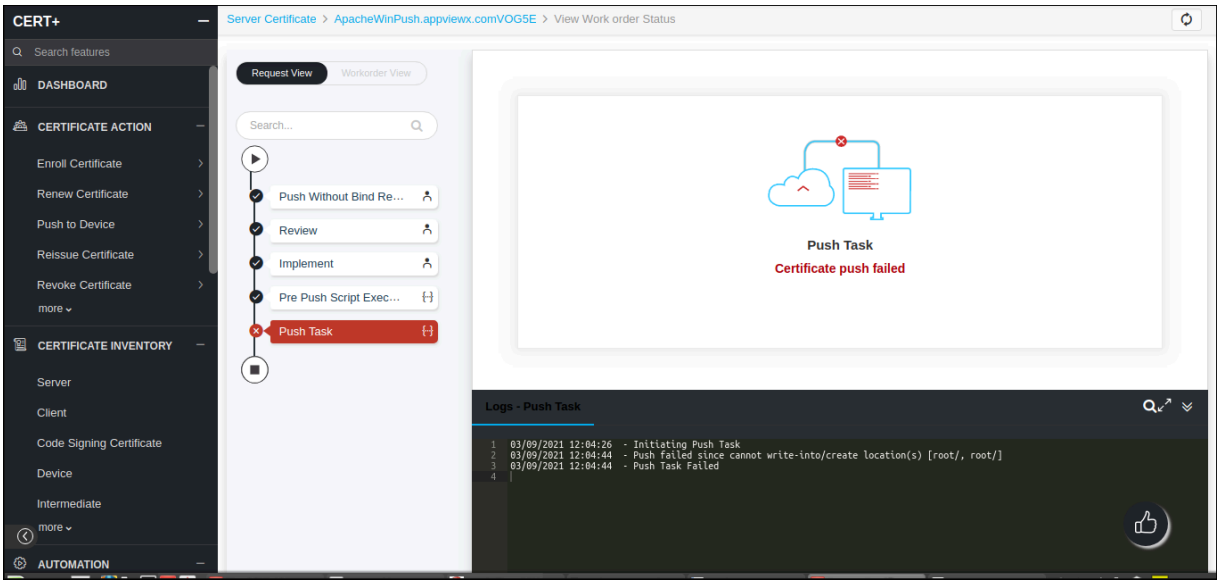
Issues in the Certificate Push

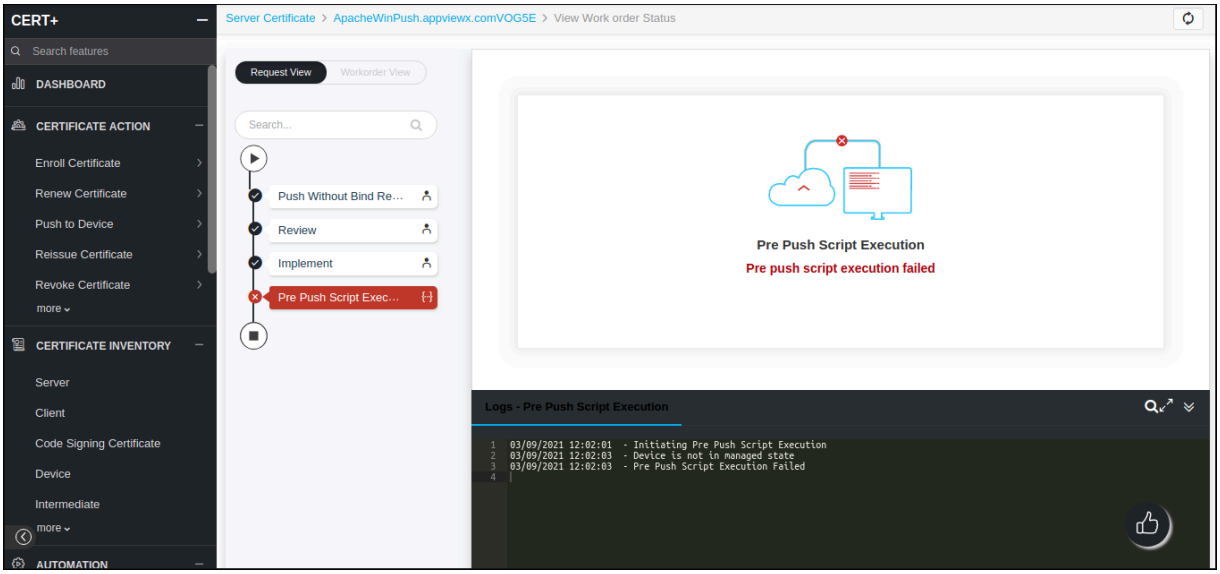
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **NginxPlus** device. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Private key should not be empty or null.	Private key not available in push request certificate	Please ensure the private key is available in request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Pivate key In device configured. But key content is available with the certificate from AppViewX.So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	Ensure the user has permission.
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Paloalto Firewall

- Introduction
- Issues in Fetch Config
- Issues in CSR Generation
- Issue in Discovery
- Issue in Backup, Push, Bind and Rollback

Introduction

Overview

This section helps you troubleshoot the common problems that you might encounter while using Paloalto firewall functionalities. This guide will give more troubleshooting processes on Paloalto firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Paloalto firewall.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in CSR Generation

Issues in the CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall**.
7. Click Paloalto as Vendor from the dropdown. A list of devices will be generated in the **Devices dropdown**.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Invalid parameter for number of bits Csr generation is device failed	Selected EC bit length may not be supported by Paloalto.	Please select valid bit length supported.

Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name not given or length less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issue in Backup, Push, Bind and Rollback

Issue in the Certificate Actions

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with the private key to bind with the profile.
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
certificate is not yet valid	Certificate valid from value is greater than current time.	Only valid certificates can be pushed.

Troubleshooting Panorama Firewall

- Introduction
- Issues in Fetch Config
- Issues in Panorama Firewall Discovery
- Issues in Panorama Firewall CSR Generation
- Issues in Panorama Firewall Backup, Push, Bind, and Rollback

Introduction

Overview

This document helps you troubleshoot the common problems that you might encounter when using the Panorama firewall functionalities. This guide will give more troubleshooting processes on Panorama firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Panorama firewall.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Firewall** Tab.
5. Select the device, click **Fetch Config**.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall Discovery

Issues in the Panorama Firewall Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall CSR Generation

Issues in the Panorama Firewall CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the **Category** dropdown, click **Firewall**.
7. From the **Vendor dropdown**, click **Panorama**. A list of devices will be generated in the **Devices dropdown**.

Error Messages

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials
Unsupported Key type provided	Unsupported key type is selected	Please select RSA or EC
Csr generation is device failed	CSR generation is failed	CSR generation has failed. Please refer to the error message associated with this
1) Invalid parameter for number of bits 2) Csr generation is device failed	Selected EC bit length may not be supported by panorama	Please select valid bit length supported

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Panorama Firewall Backup, Push, Bind, and Rollback

Issues in Panorama Firewall Certificate Actions

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. At the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with private key to bind with the profile
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than current time.	Currently, valid certificates only can be pushed.

Troubleshooting RabbitMQ Server

- Overview
- Issues in RabbitMQ Server Addition using AppViewX UI
- Issues in Communicating to RabbitMQ Server
- Issues in Accessing Server
- Issues in Config Fetch
- Issues in Certificate Discovery

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in CSR generation
• Issues in Push and Rollback

Overview

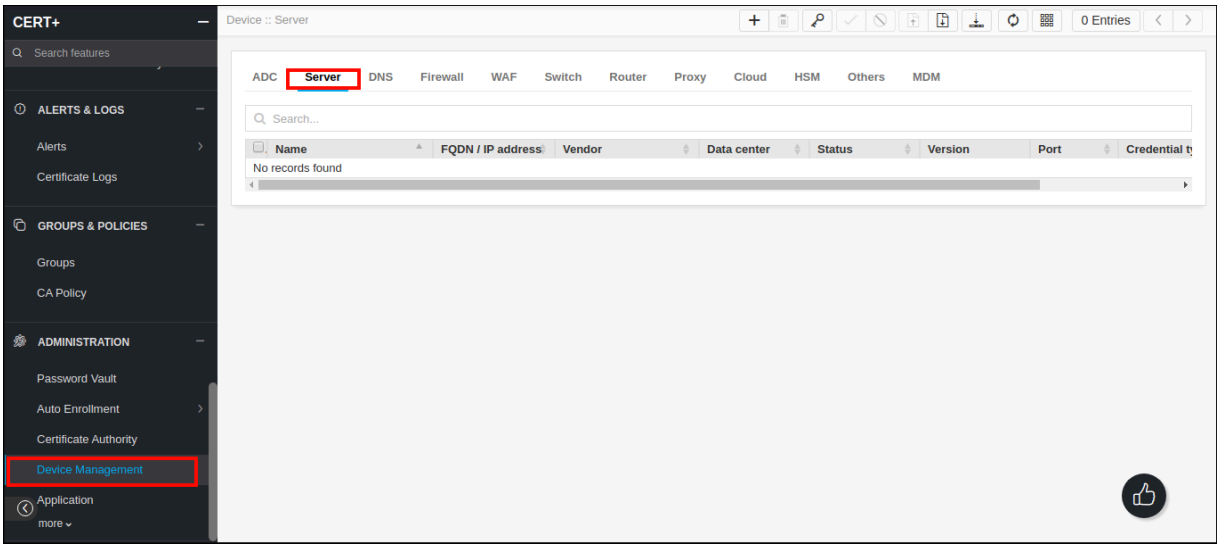
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with RabbitMQ server.

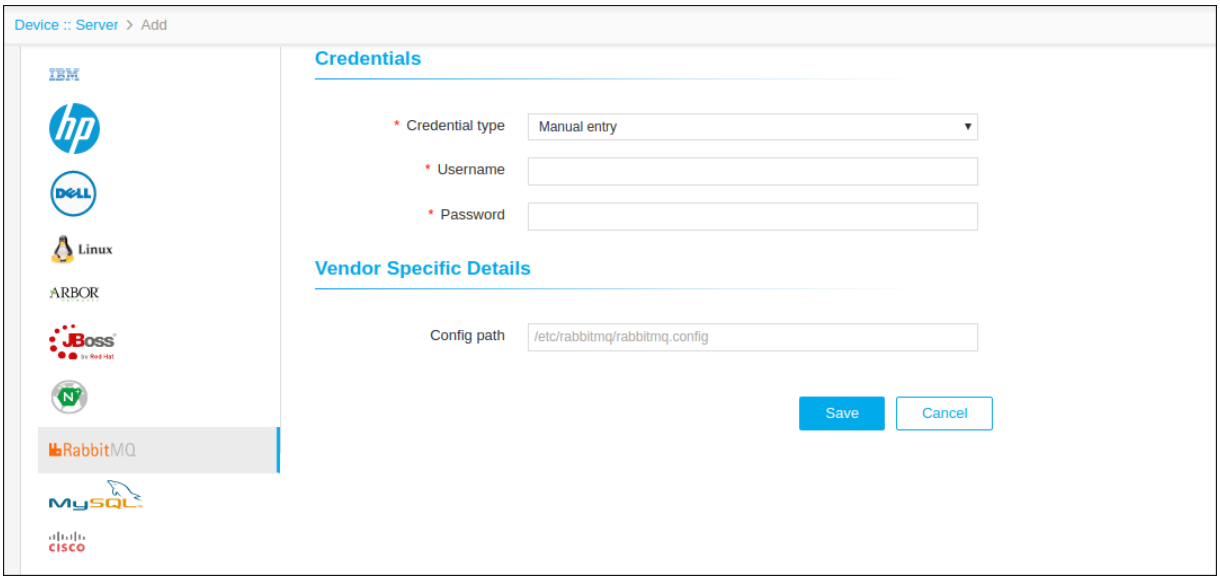
Issues in RabbitMQ Server Addition using AppViewX UI

Issues in the RabbitMQ Server Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **RabbitMQ**.
7. Fill in the appropriate details.
8. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

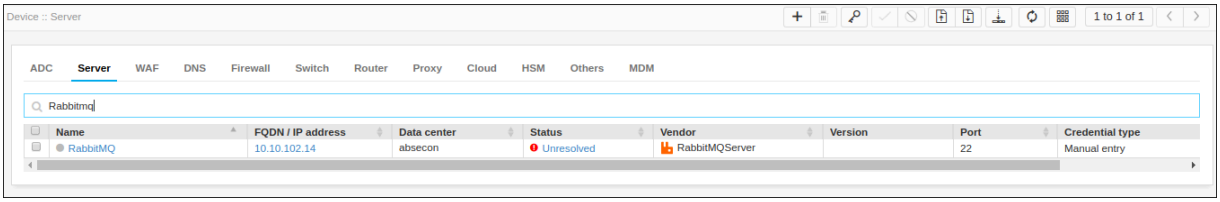
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

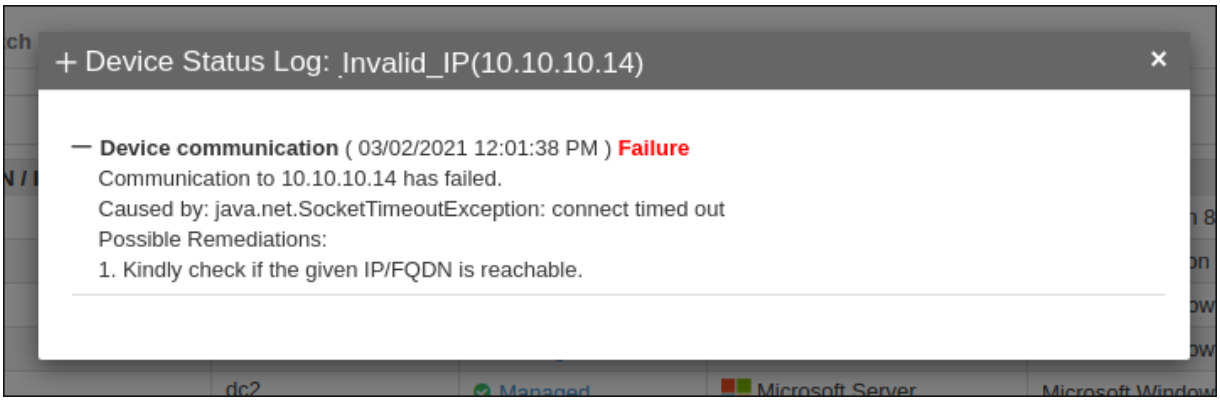
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

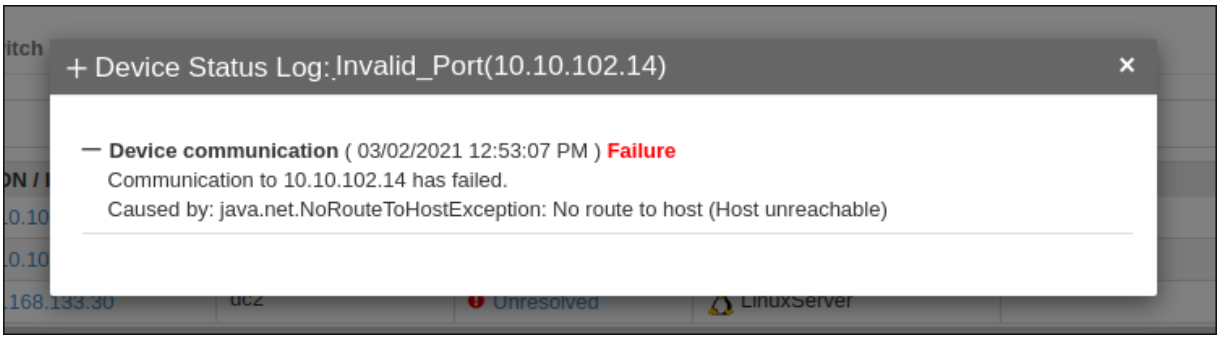
Issues in Communicating to RabbitMQ Server

Issues in the Communicating to RabbitMQ Server

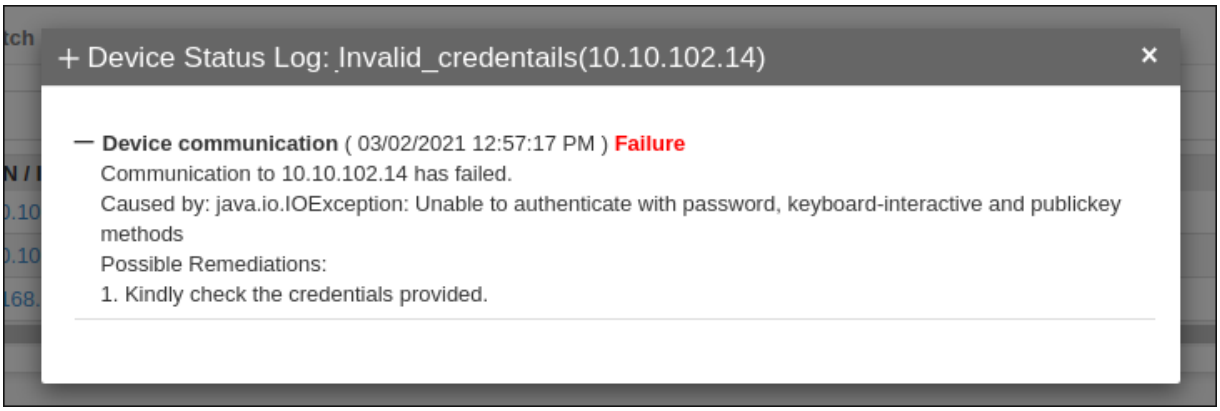
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

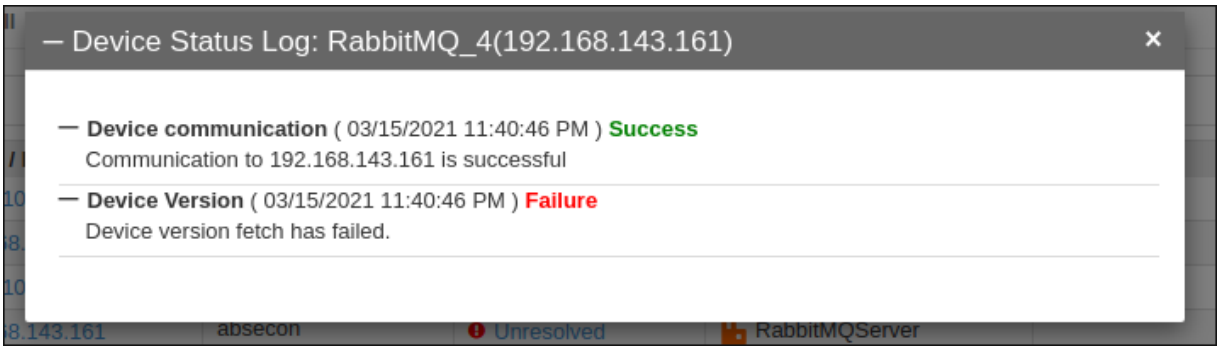






Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.		
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key	Problem with SSH key handshake	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
exchange was not finished, connection is closed.		
Device version fetch has failed.	Config path is incorrect / No RabbitMQ instances running in the target device	Check manually by establishing an SSH session to the target device and check RabbitMQ installations and find a valid configuration path and update the same in the device addition page.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files (/etc/rabbitmq/rabbitmq.config). These errors can be collected either from logs, API responses, or in the status field for the particular server.

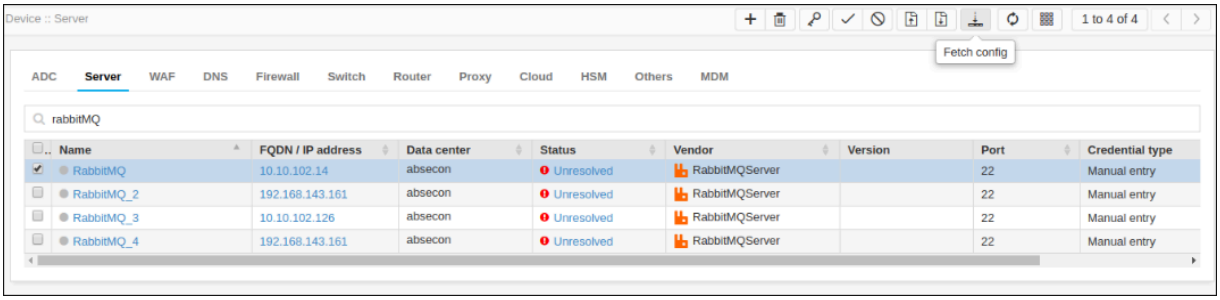
Error Message	Possible Cause	Possible Solution
Custom Config Location	For default installation, The config location path is / etc/rabbitmq/rabbitmq. config, if any custom location is provided check the valid rabbitmq config file exists in that location	Login via SSH to the target device and check the “rabbitmq” installations and valid configuration file location path
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3.Device communication might not be established when service has started.	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <IP/ FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	1.Verify the input details and check device status error messages Issues in Communicating to RabbitMQ Server

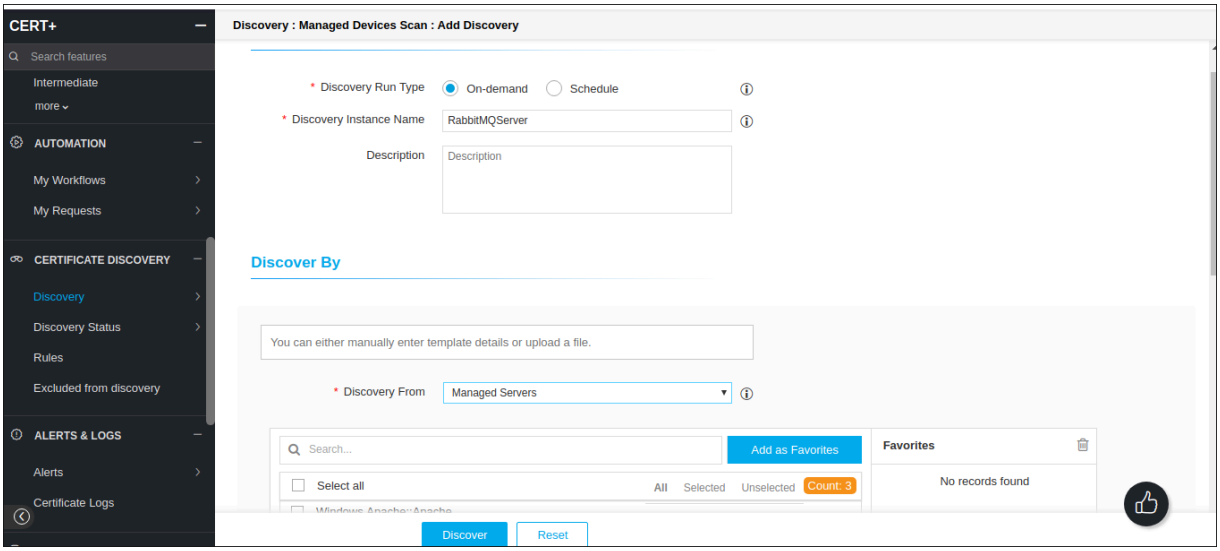
Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

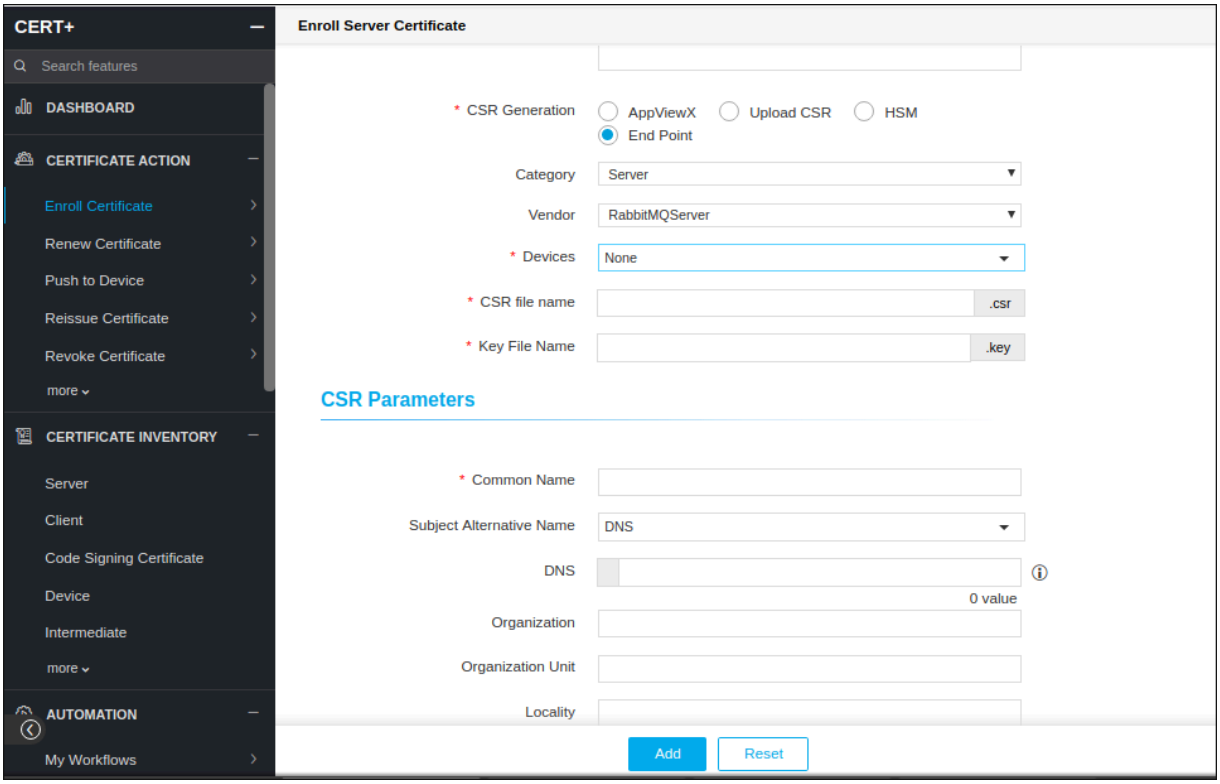
Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category.**
7. From the Vendor dropdown, click **RabbitMQServer**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

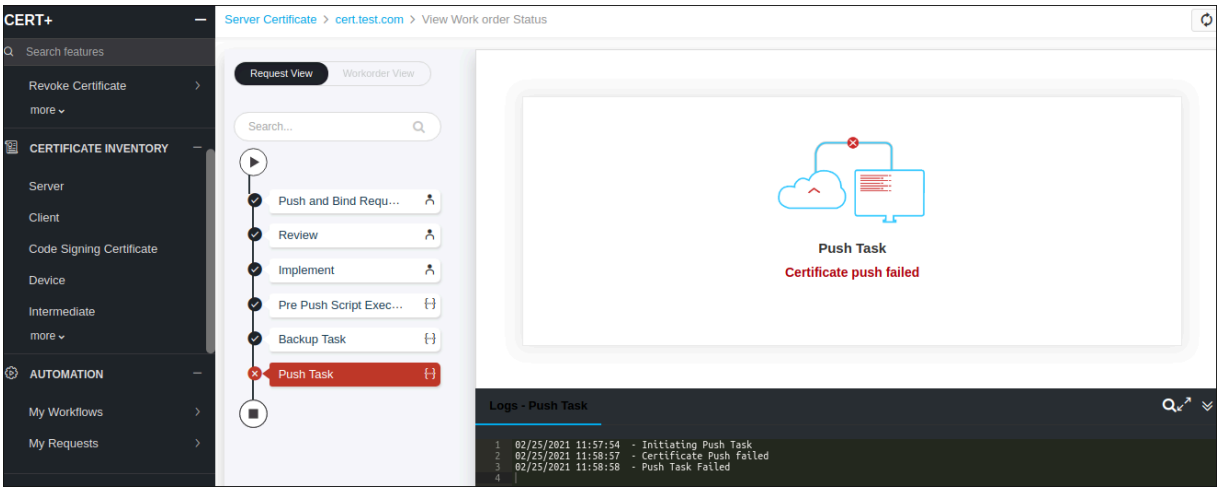
Error Message	Possible Cause	Possible Solution
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

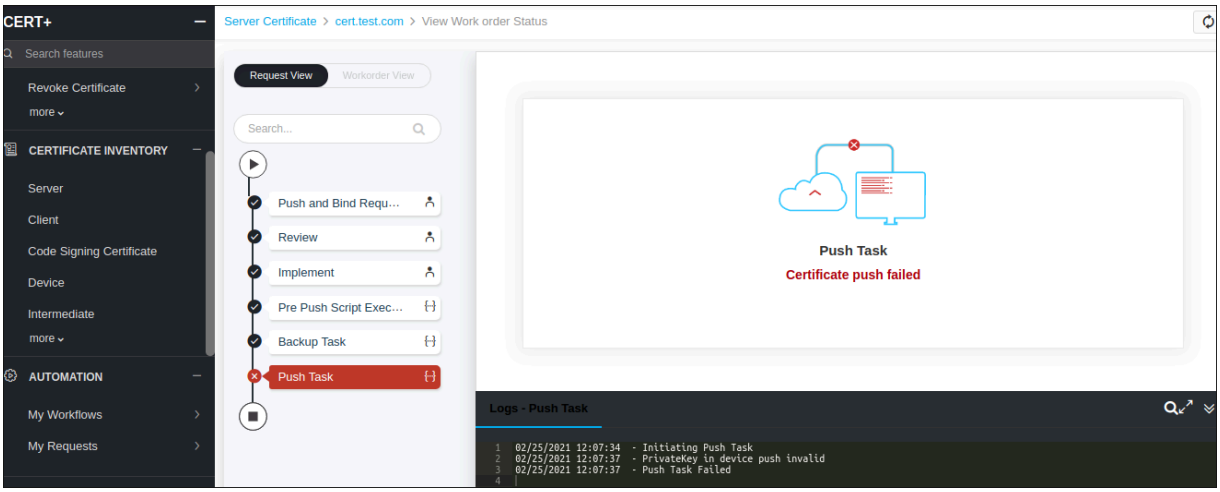
Issues in Push and Rollback

Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **RabbitMQ server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available on device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Rapid SB Server Inventory

- Introduction
- Issues in Accessing Server
- Issues in Credential List
- Issues in Managed Server
- Issues in Unmanaged Server
- Issues in Import Server
- Issues in Export Server
- Issue in Discovery

Introduction

Overview

This document will help you troubleshoot the issues faced during the use of the functionalities of Rapid SB connectors server inventory. It begins by troubleshooting the common functionalities and then goes on to handle the issues peculiar to various Rapid SB connectors Servers.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

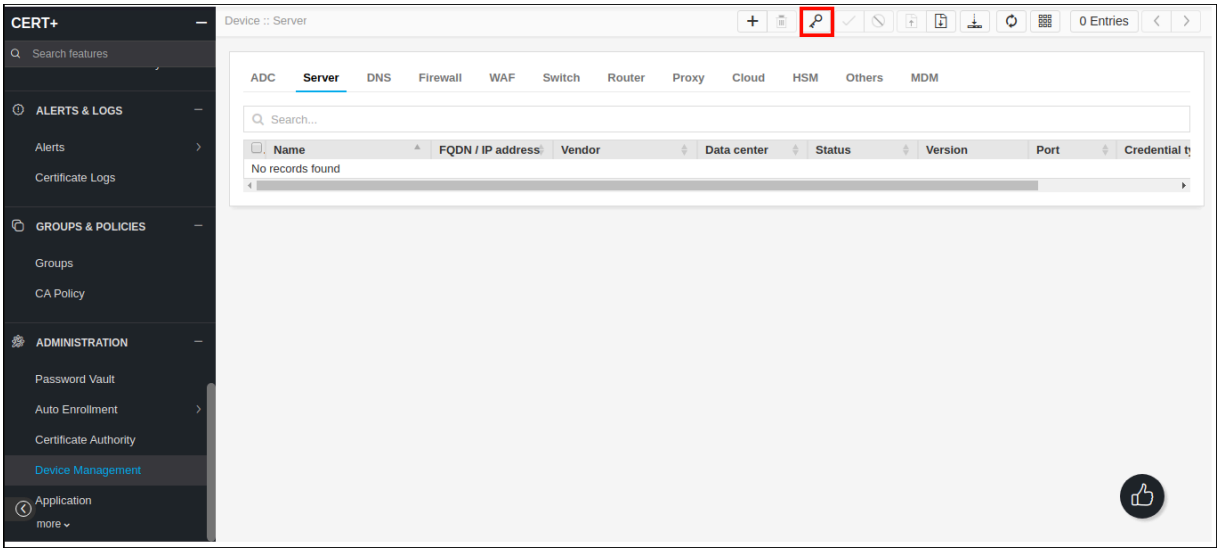
Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3.Device communication might not be established when service has started.	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Credential List

Issues in the Credential List

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Credentials**. The **Credential List**page is displayed.



Error Messages

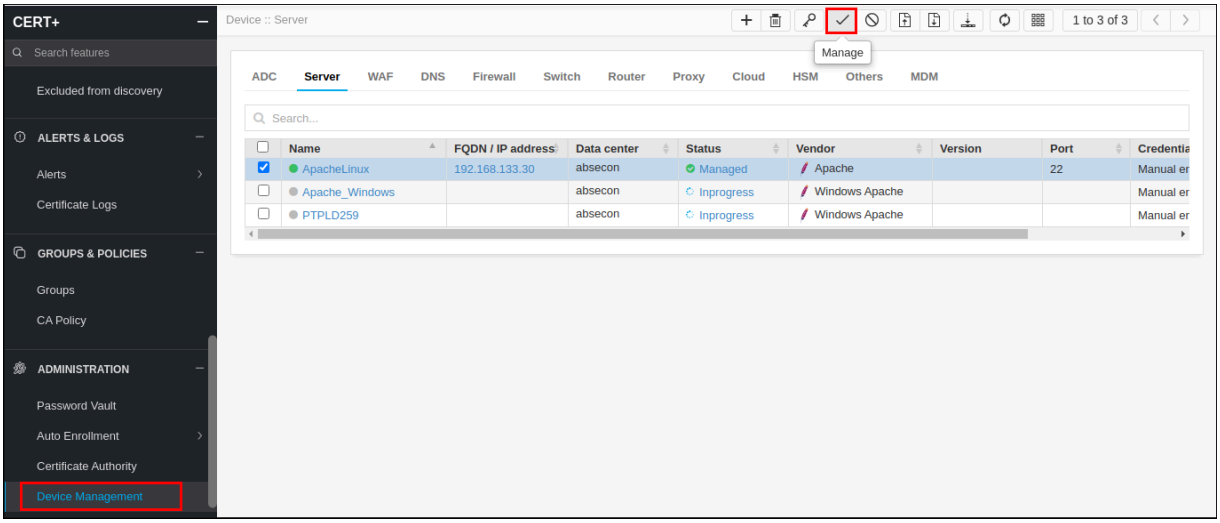
Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Managed Server

Issues in the Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.



Error Messages

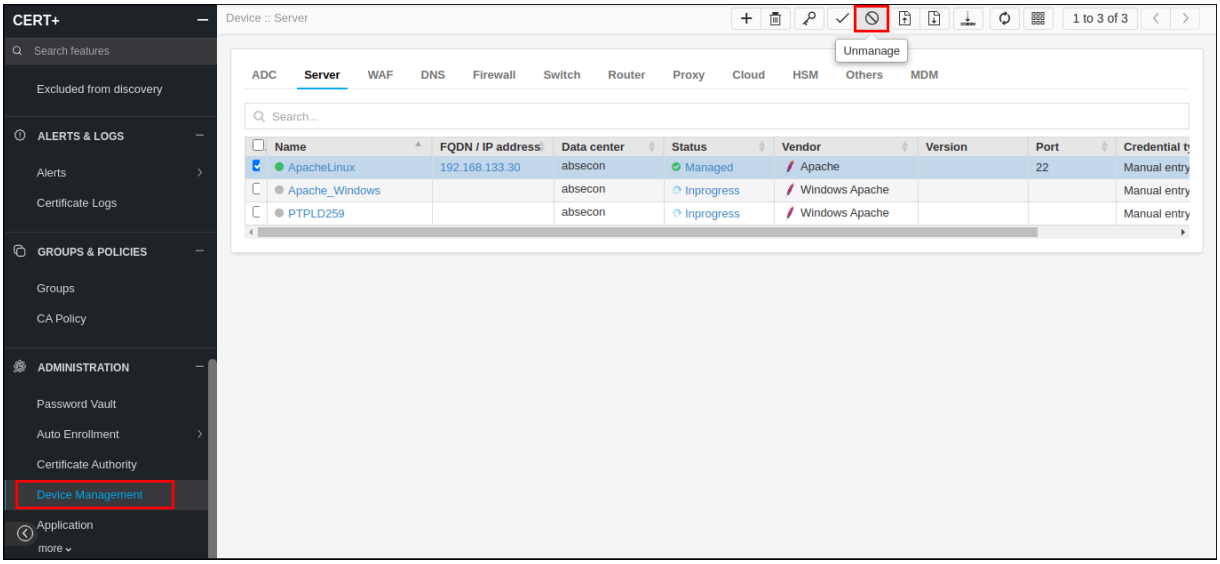
Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Unmanaged Server

Issues in the Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Unmanage**.



Error Messages

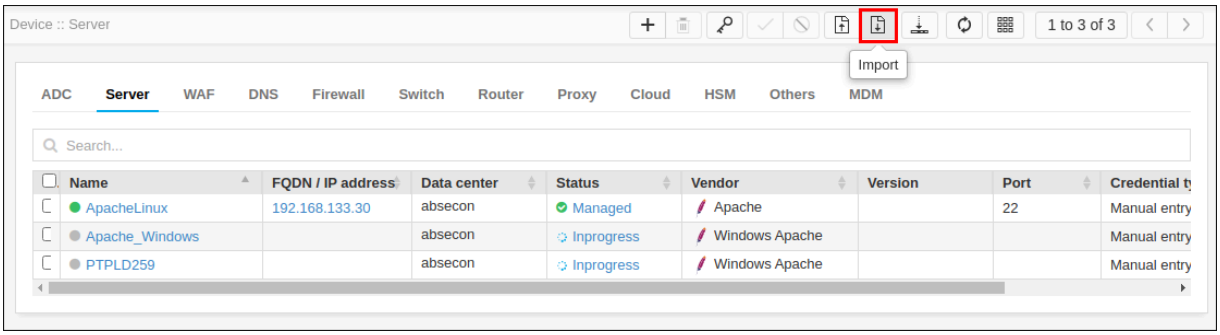
Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Import Server

Issues in the Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Import**.



Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in an expected format.	Supported file types are CSV/Xls/ xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum of 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

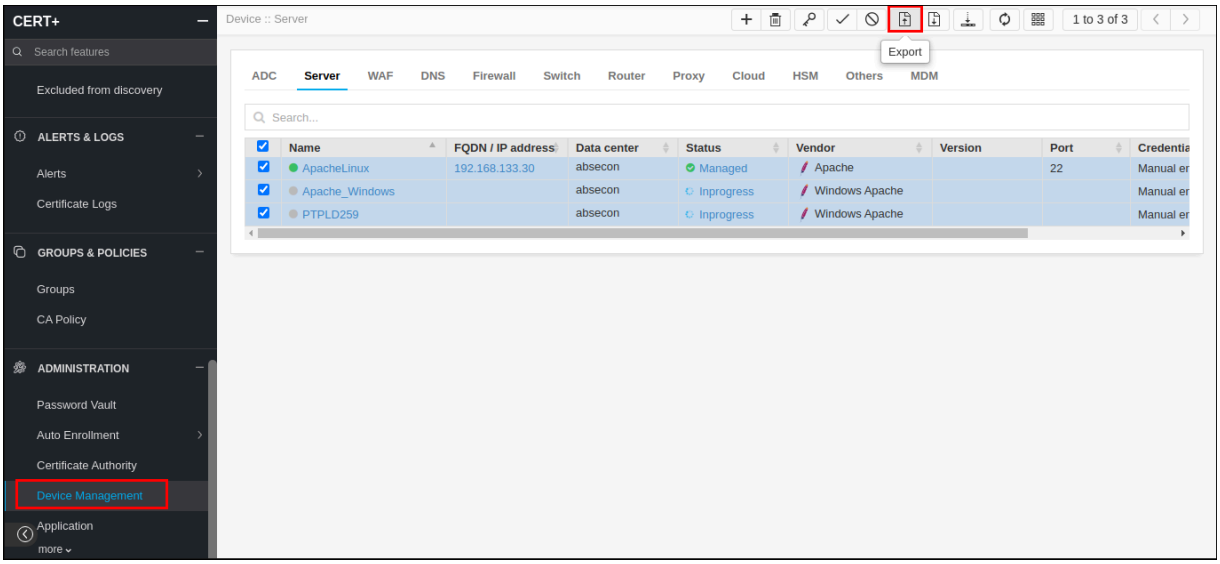
Issues in Export Server

Issues in the Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** Page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. On the **Device Management** Page, click **Server** Tab.
5. Select the device and click **Export**.



Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	1.General failure - Unable to create file on the local system due to permission issue. 2.Unable to fetch device list from the database.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

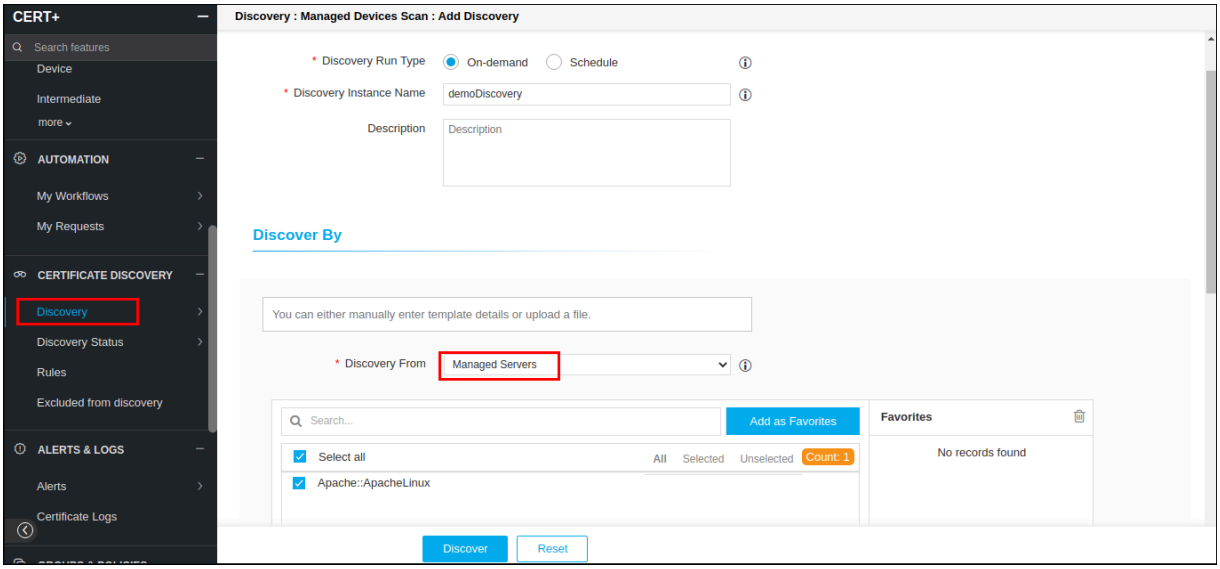
Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “**Discover By**” section.	Select at least one device to discover certificates from.

Troubleshooting Rapid SB Linux Server

- Overview
- Issues in Linux Server Addition using AppViewX GUI
- Issues in Communicating to Linux Server
- Issues in Accessing Server

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Issues in Credential List
• Issues in Managed Server
• Issues in Unmanaged Server
• Issues in Import Server
• Issues in Export Server
• Issues in Config Fetch
• Issues in Certificate Discovery
• Issues in CSR generation
• Issues in Push and Rollback

Overview

Overview

This section helps you troubleshoot the common problems that you might encounter while using certificate server functionalities for Linux servers. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux servers.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

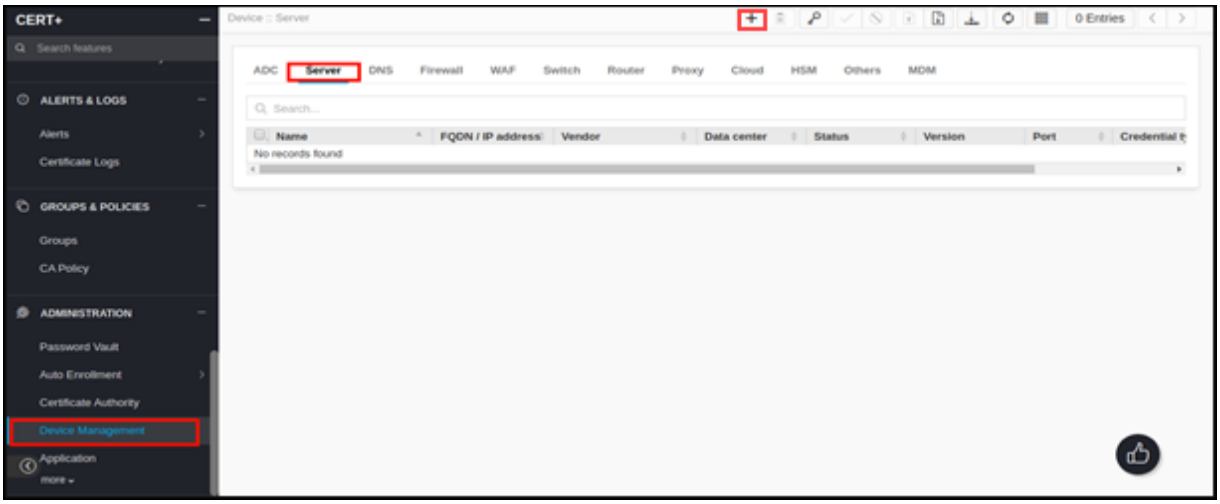
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

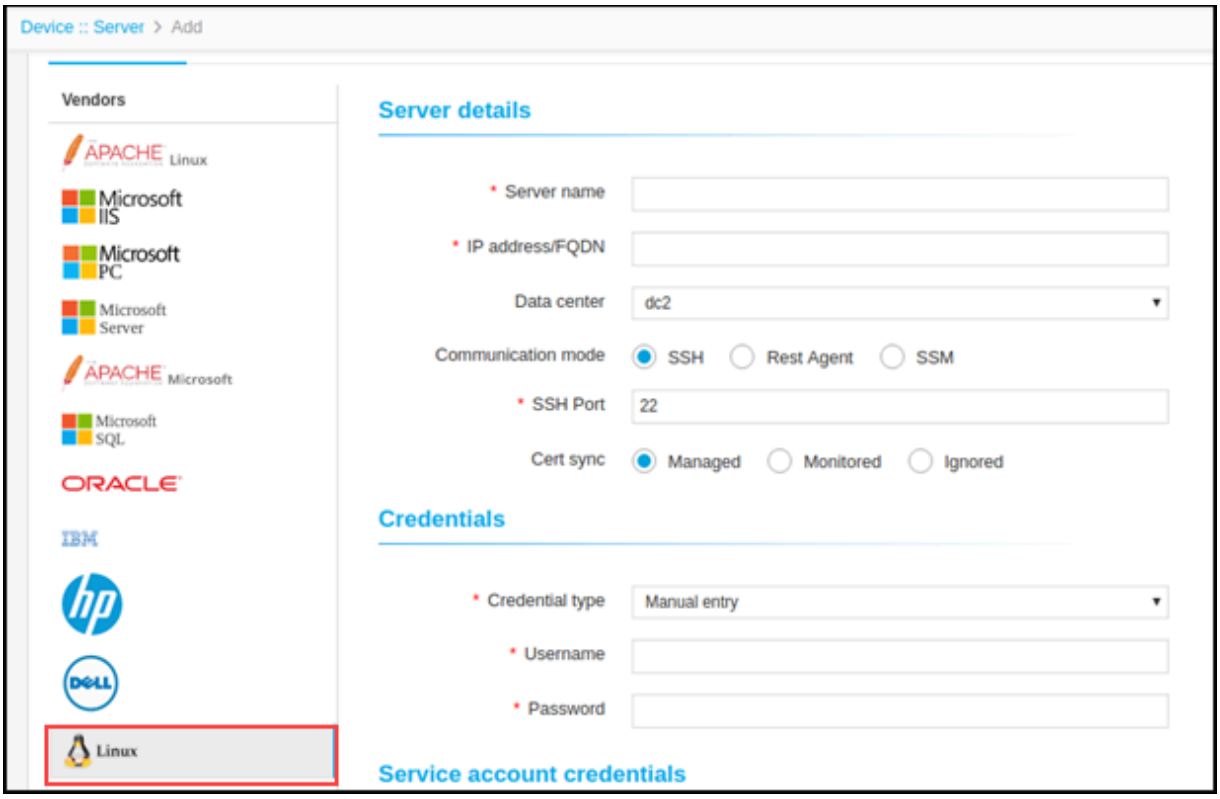
Issues in Linux Server Addition using AppViewX GUI

Issues in Linux Server Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Linux**.
7. Fill in the appropriate details.
8. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.

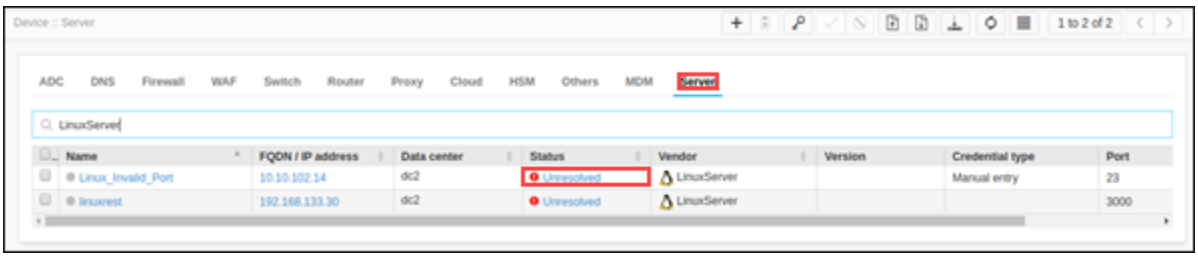
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

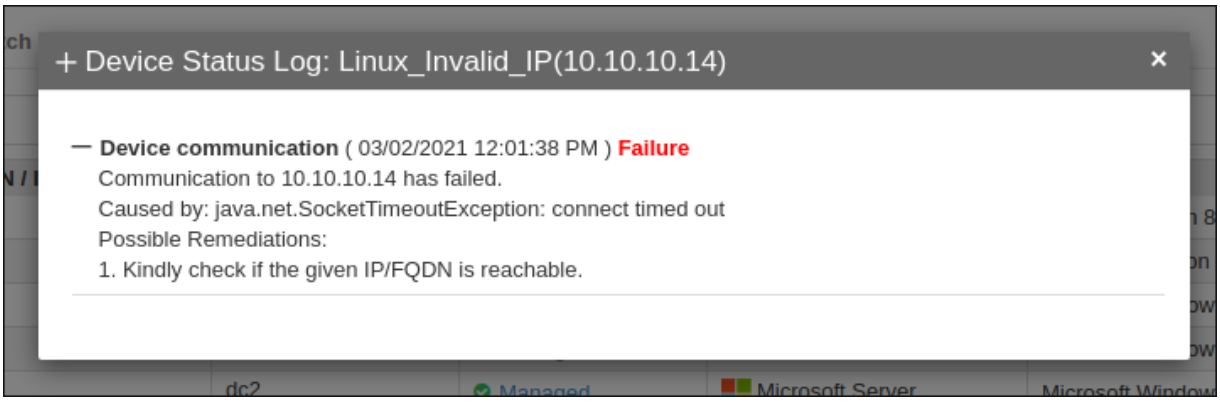
Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Linux Server

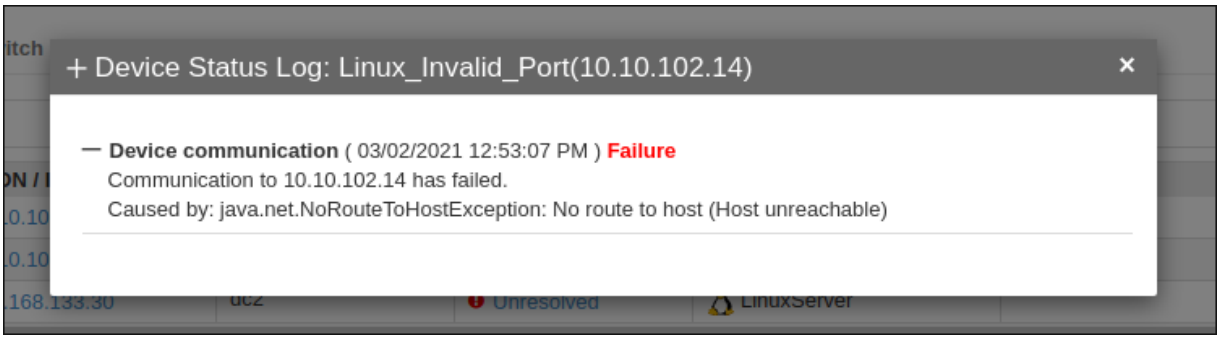
Issues in the Communicating to Linux Server

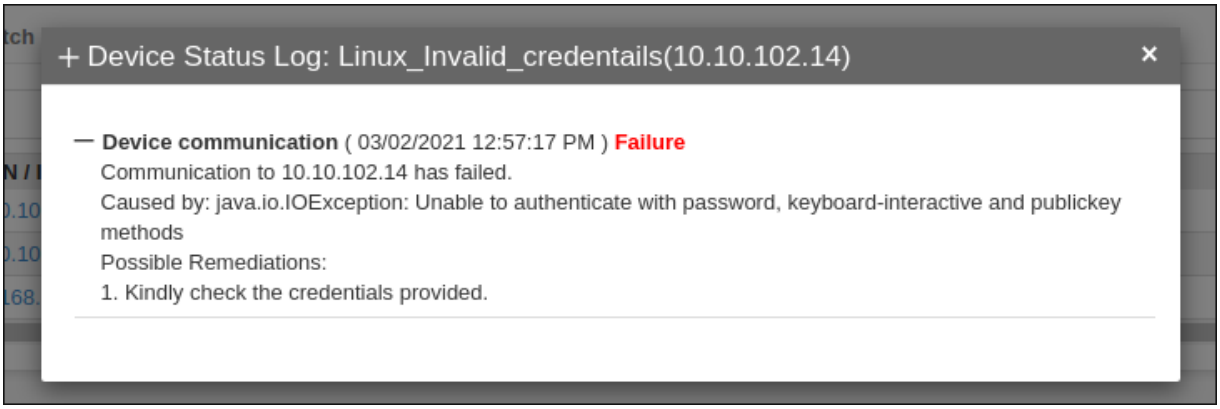
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

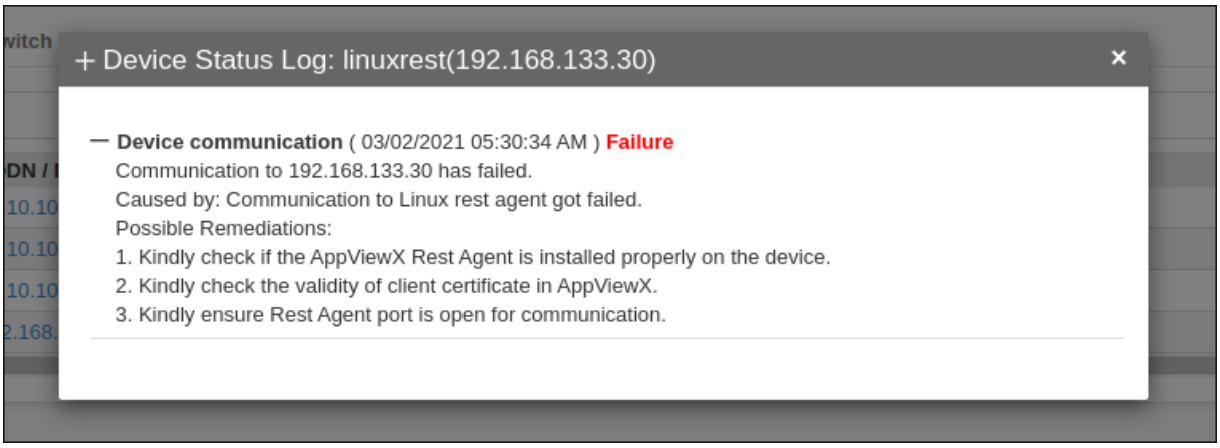




Copyright © 2024 AppViewX, Inc. All Rights Reserved.







Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid device name.	Device Name is not valid.	The Device name can contain only alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable.	Check manually by establishing a SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations:	Problem with port configuration.	Check if the configured port in the device addition page is correct.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings		
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake.	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same.

Issues in Accessing Server

Issues with accessing servers can occur while communicating with servers or discovering or fetching configuration files. These errors can be collected either from logs, API responses or can be seen in the status field for that particular server.

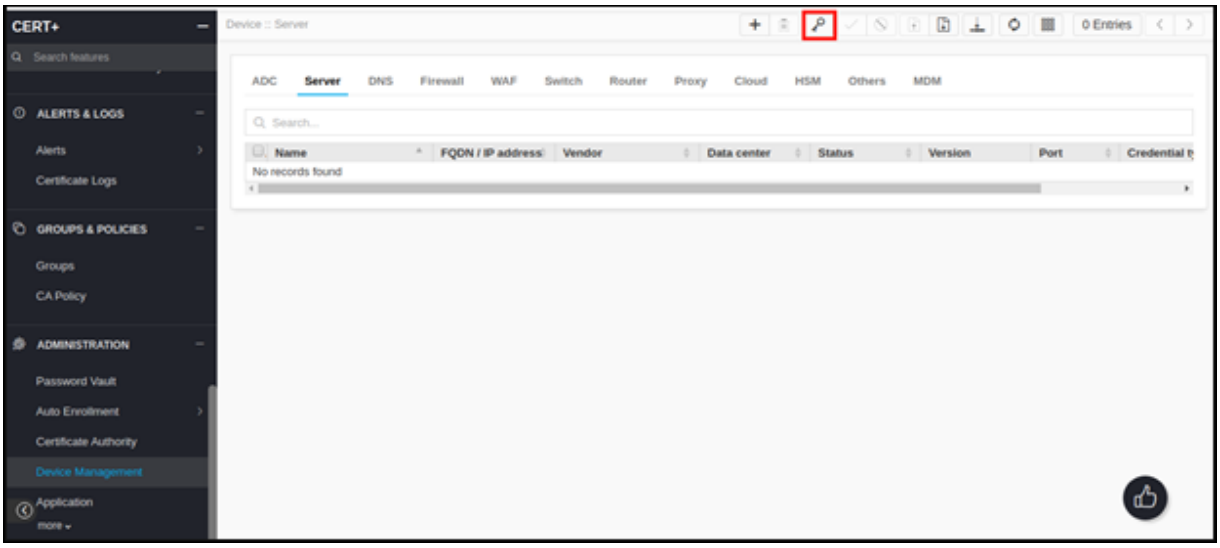
Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Credential List

Issues in the Credential List

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Credentials**. The **Credential List** page is displayed.



Error Messages

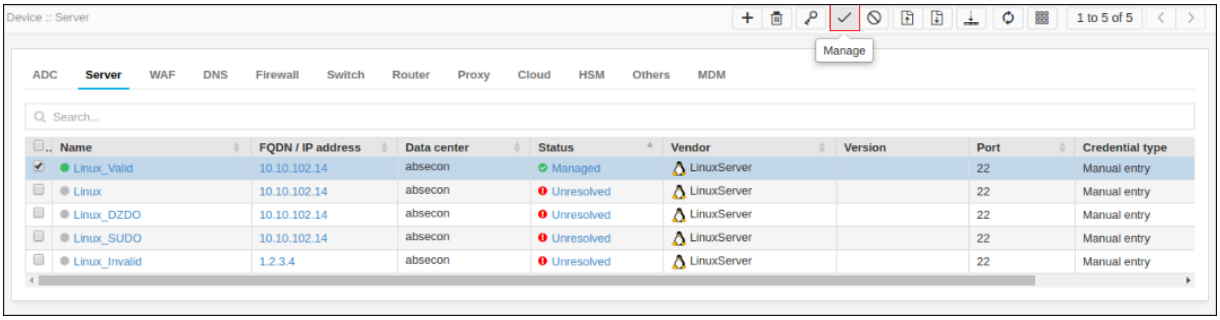
Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded does not have the correct format.	Provide key file with correct format (.pem or .txt)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Managed Server

Issues in the Managed Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Manage**.



Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

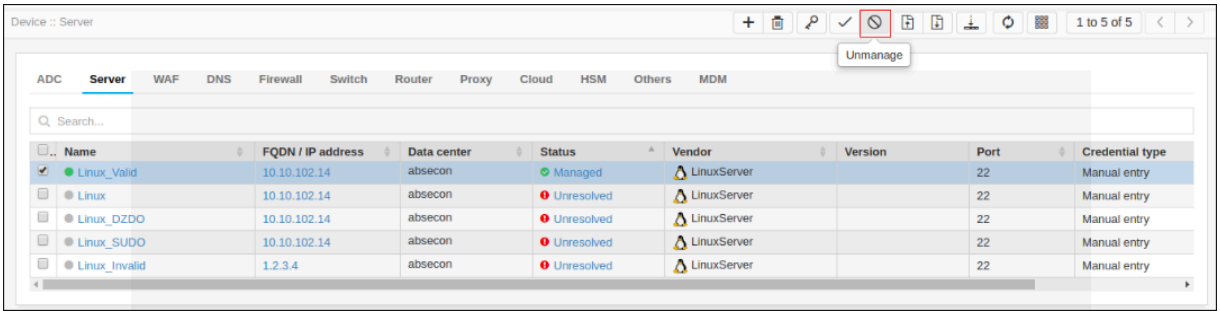
Issues in Unmanaged Server

Issues in the Unmanaged Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device and click **Unmanage**.



Error Messages

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) that is in unmanaged state before unmanaging it again.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) that is in an unmanaged/inprogress state before unmanaging it again.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an inprogress state.	Wait for the device to be resolved to a state before performing action.

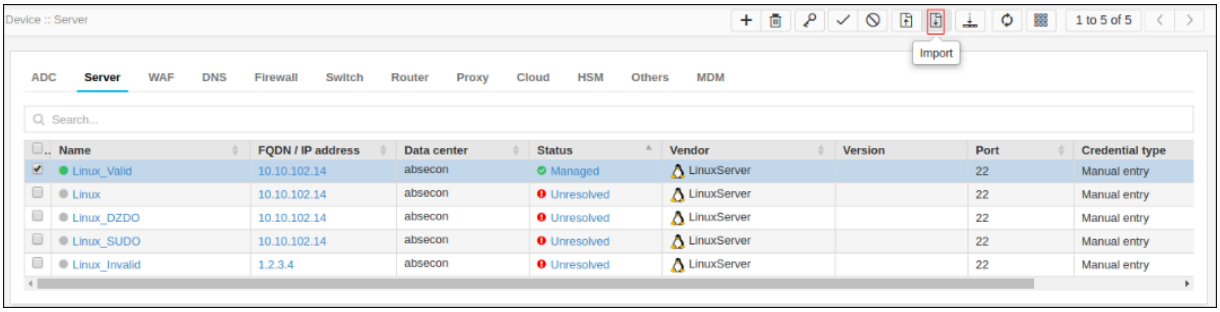
Issues in Import Server

Issues in the Import Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device and click **Import**.



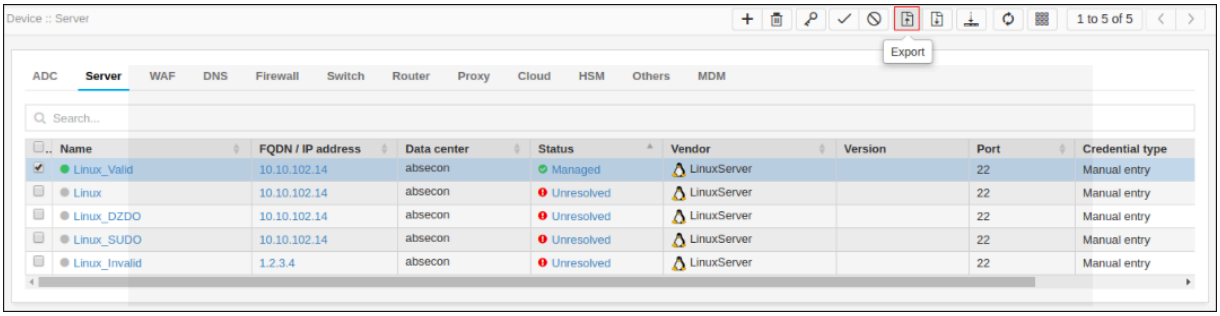
Error Messages

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In file history of import page maximum 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

Issues in Export Server

Issues in the Export Server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device and click **Export**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

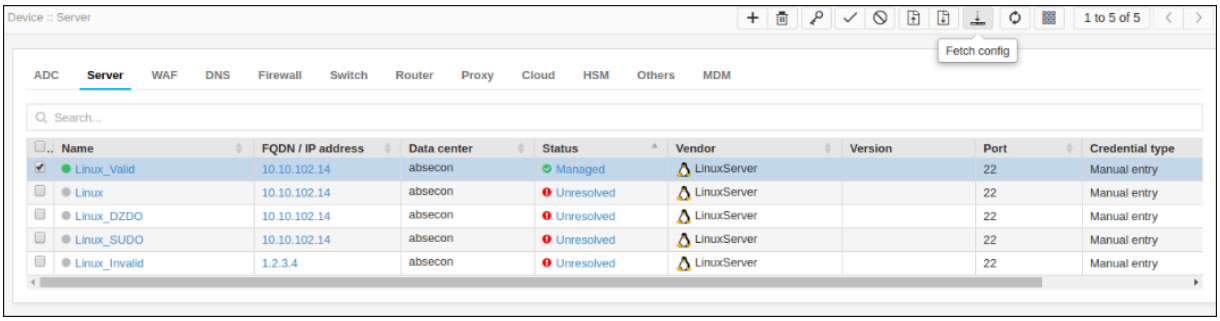
Error Messages

Error Message	Possible Cause	Possible Solution
Exception while exporting	1. General failure - Unable to create file on the local system due to permission issue. 2. Unable to fetch device list from the database.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Fetch Config**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

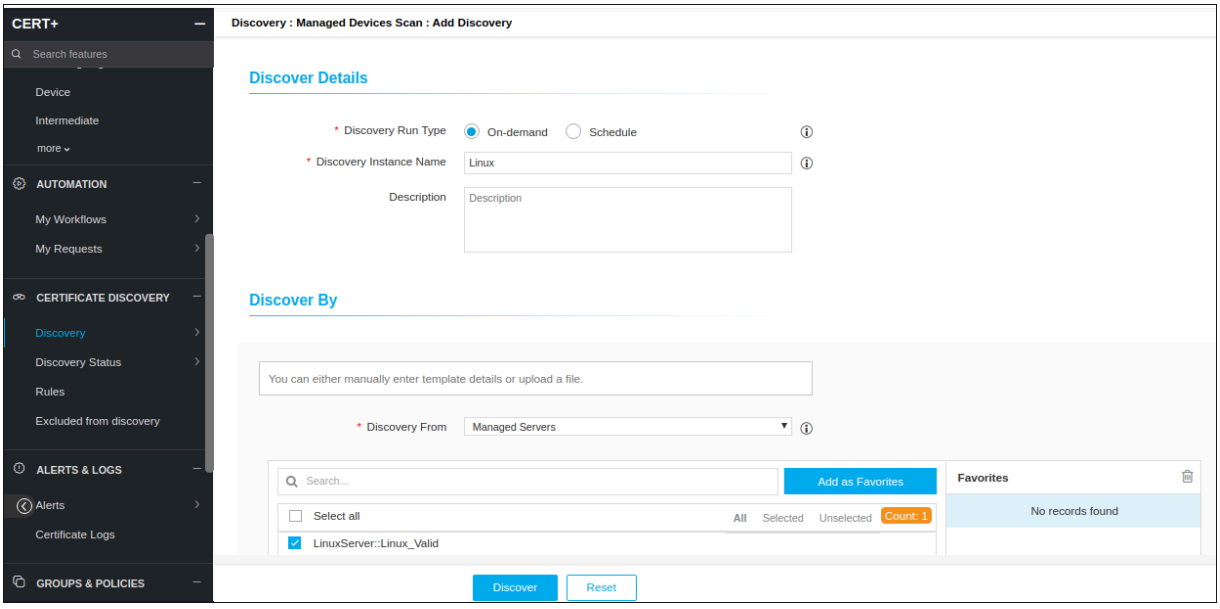
Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due invalid credentials / SSH Port.	Verify the input details and check device status error messages in Issues in Communicating to Linux Server

Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

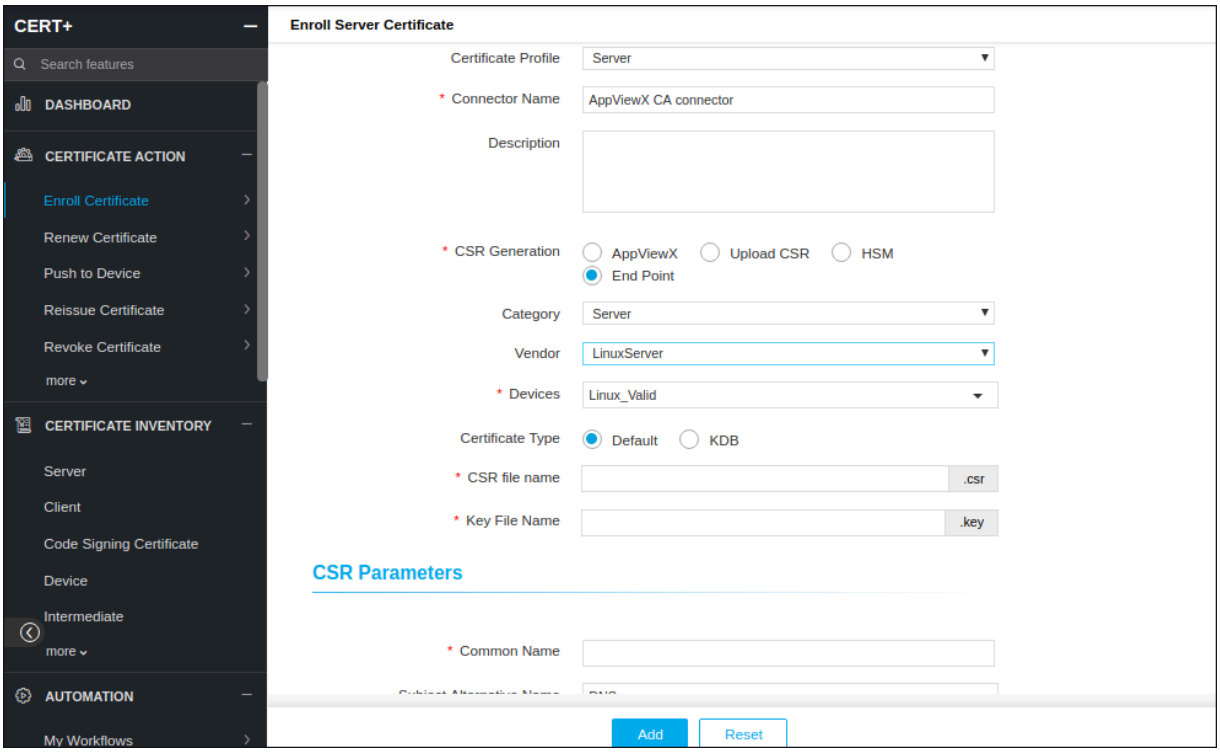
Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click correct **Category** from the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **Linux Server.** A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

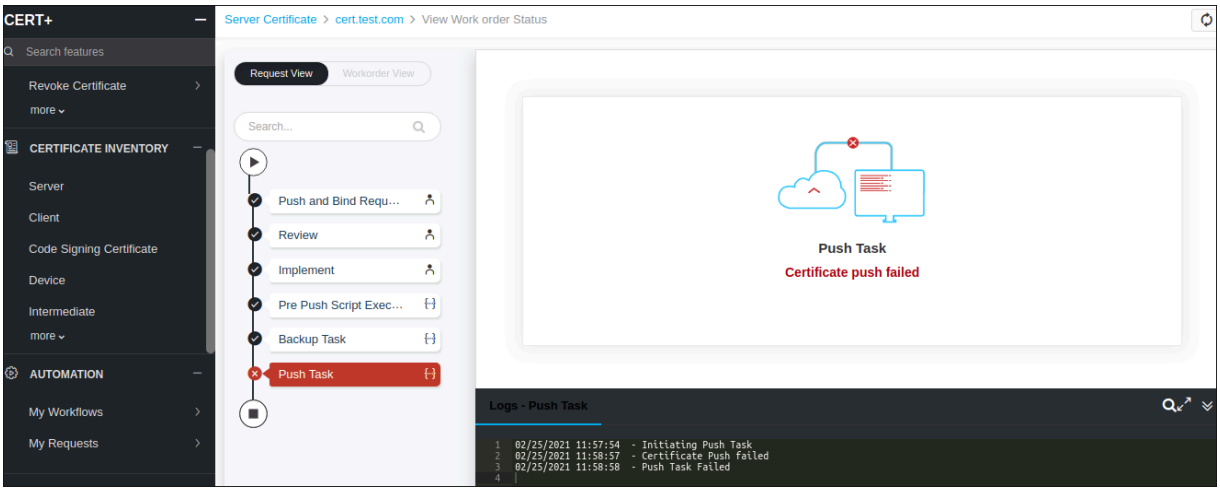
Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

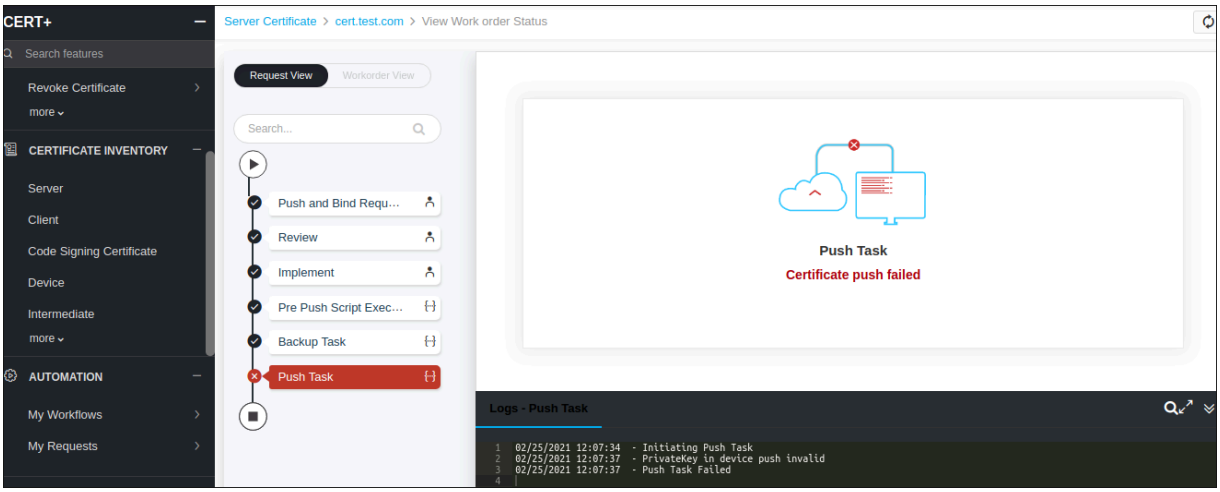
Issues in Push and Rollback

Issues in the Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Linux server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Tomcat Linux

- Overview
- Issues in Device Addition using AppViewX GUI
- Issues in Communicating to the server
- Issues in CSR Generation
- Issue in Access
- Issues in Fetch Config
- Issue in Discovery
- Issues in Push and Rollback

Overview

This document helps you troubleshoot the common problems that you might encounter when using Tomcat Linux functionalities. This guide will give more troubleshooting processes on issues related to the Tomcat Linux server. The issues are device addition, communication to the server, CSR generation, access to the server, fetch configuration, discovery along with push and rollback.

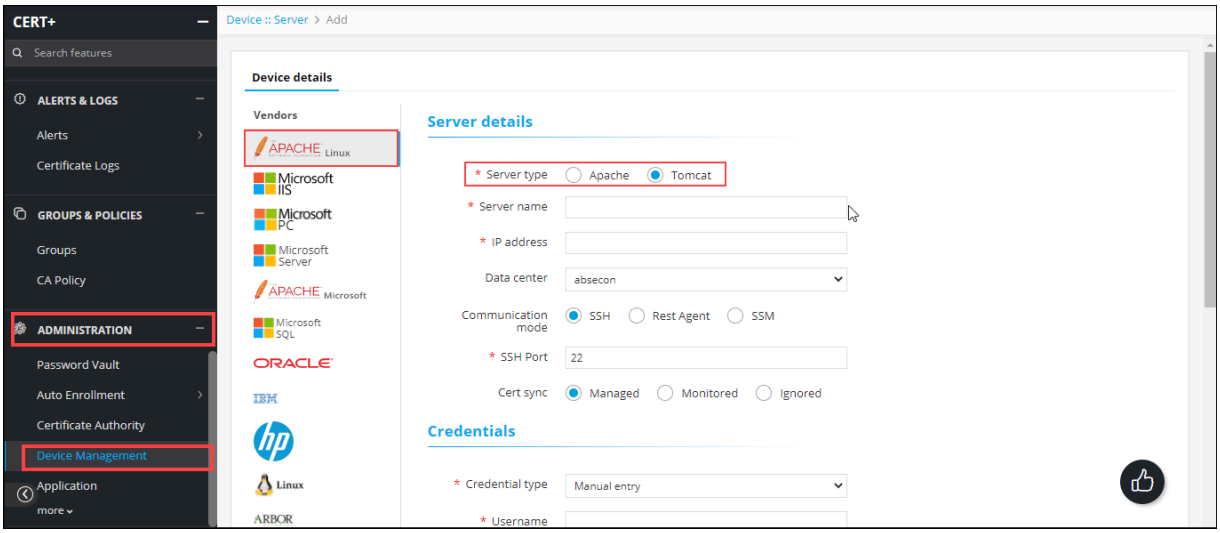
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Device Addition using AppViewX GUI

Issues in the Device Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details section** on the left, Click **Apache Linux**.
7. Click **Server type** as **Tomcat**.
8. Fill in the appropriate details.
9. Click **Add**.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

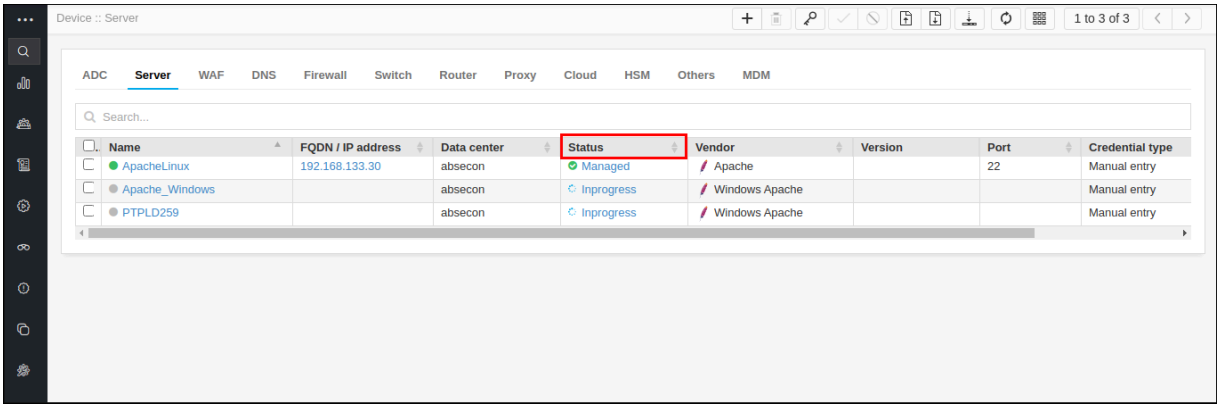
Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Device name accepts '-' , '_' , '.' , '*' , '|' , '!' and space only, with min 2 and max 64 characters.	Server name is not valid.	Provide a server name with min 2 and max 64 characters with only the allowed characters.

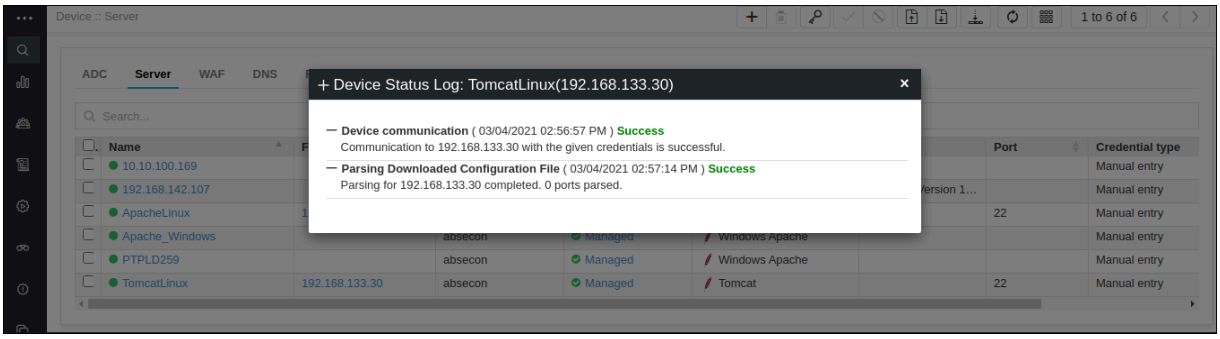
Issues in Communicating to the server

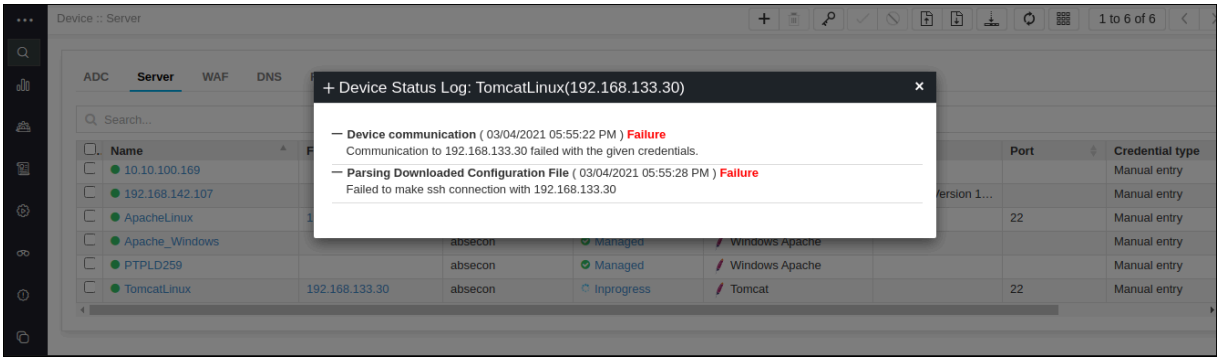
Issues in the Communicating to the server

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Failed to make the ssh connection with the given IP.	Given IP may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure given IP is connected to the network.
	SFTP port is not open for SSH communication.	Open given port for the SSH communication.
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

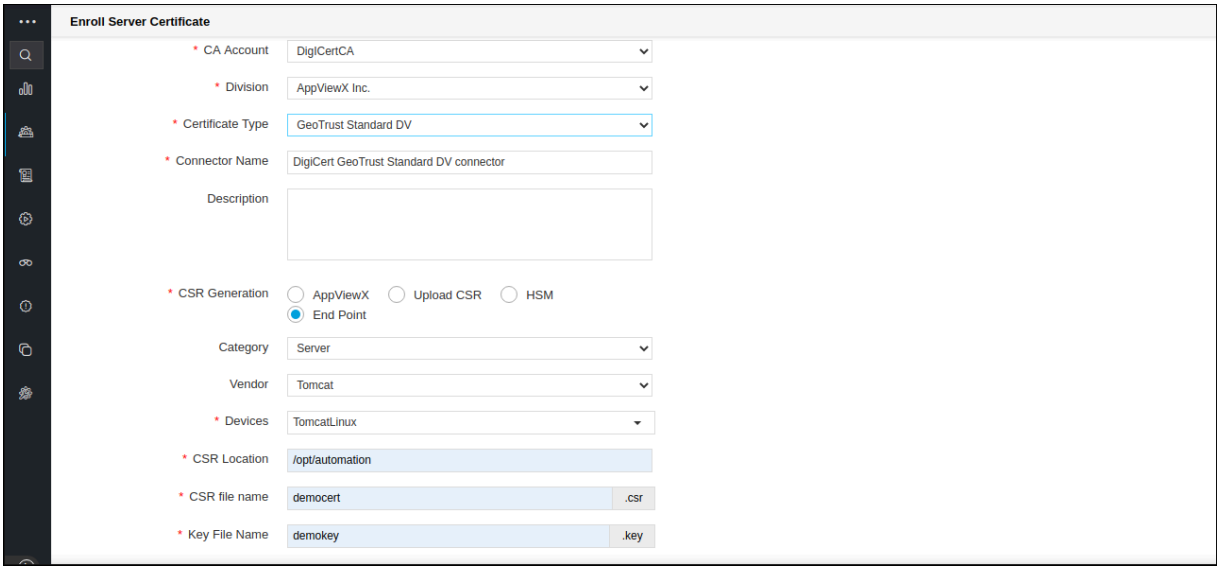
Error Message	Possible Cause	Possible Solution
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Device does not belong to Tomcat Server.	Device does not have any running tomcat instances.	Start any tomcat server in the device.
Failed to make ssh connection.	Target device may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure the target device is connected to the network.
	The User may not have permission to execute the command.	Provide permission for the user to execute \"ps -ef\" command.
Linux rest agent communication failed	Rest agent installed in the device might not be running.	Install AppViewX Rest agent in device.
	The Client certificate installed in AppViewX might not be valid.	Install valid client certificate in AppViewX.
	Rest agent port might not be open for communication.	Ensure port is open for communication.
Error while decrypting password.	Password invalid for decryption key.	Check if the password matches with the decryption key.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in CSR Generation

Issues in the CSR Generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click correct **Category** from the dropdown.
7. Click correct **Vendor** from the dropdown. A list of devices will be generated in the **Devices dropdown**.
8. For generating CSR, select **Apache** device.
9. Click **Add**.



Error Messages

Error Message	Possible Cause	Possible Solution
CSR Generation Failed.	Given CSR Location is not available in device.	Provide a valid path to store CSR and key.
	User does not have read/write permission for the location.	Ensure the user has read/write permission to the given location.
	“Openssl” package is not installed	Install “Openssl” package in the device

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	The User does not have permission to execute “Openssl” commands.	Provide permission for user to execute “Openssl” commands

Issue in Access

Access Issues might occur when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
File Download Failed.	User or User group does not have read/write permission for server.xml in device.	Provide read/write permission for user in device

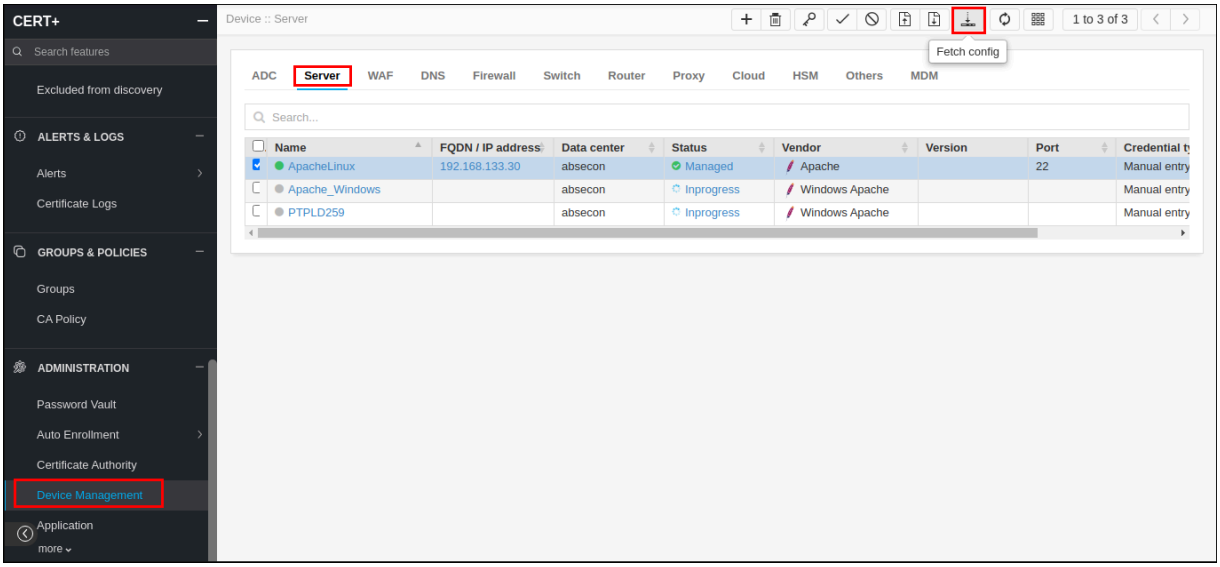
Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
XML Parsing Failure	FileName provided might not be a valid XML file.	Ensure the provided filename is a valid XML file.
File Download Failed.	server.xml is not found in the specified directory.	Ensure server.xml is present in the conf directory.

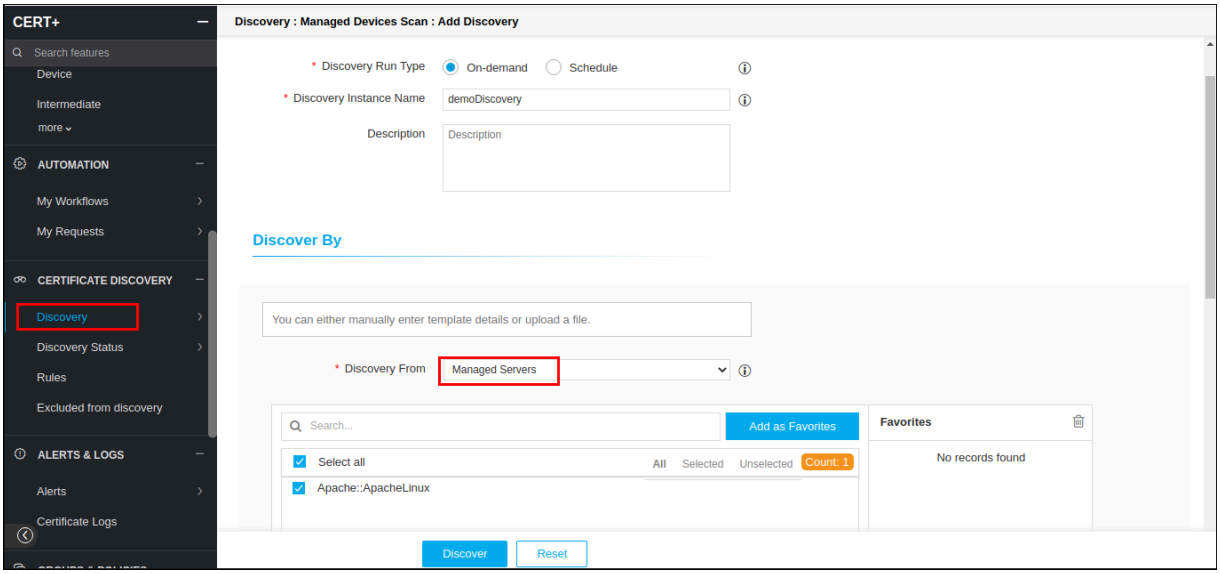
Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

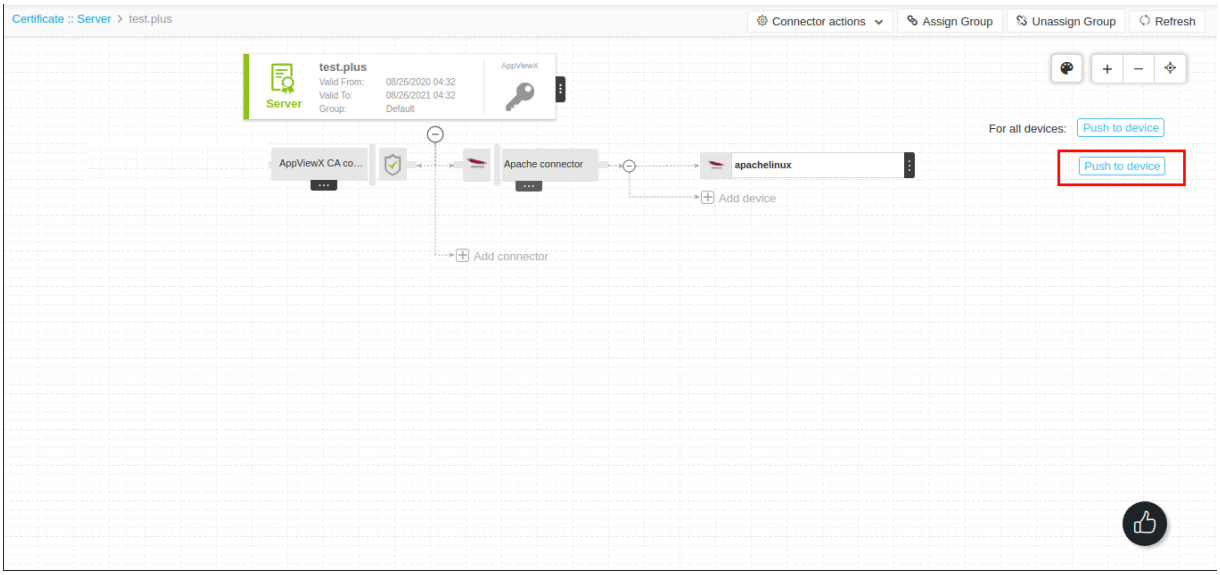
Error Message	Possible Cause	Possible Solution
File Not Found	server.xml is not present in the specified directory.	Ensure server.xml is present in the conf directory.
	SSL certificate or key file parsed from configuration file is not present in the specified directory.	Ensure parsed certificate or key file is present in the directory specified in server.xml
JKS Parsing Failure	Password for Keystore file may not be present in server.xml	Password given in server.xml might be incorrect.

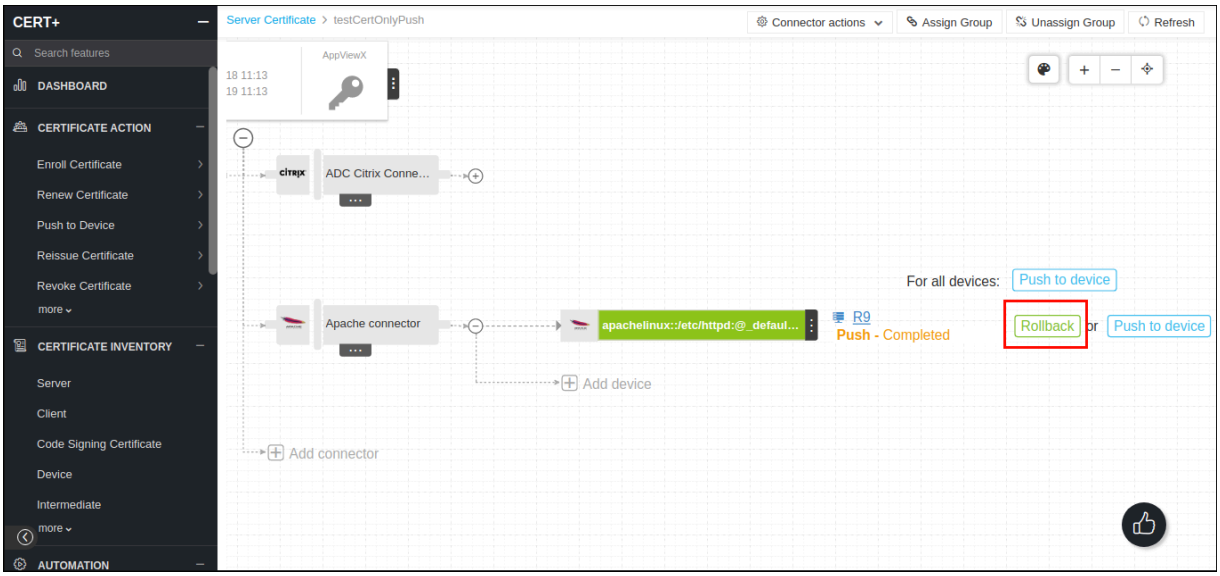
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Issues in Push and Rollback

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory**, select **Server**.
4. On the top right corner of the page, click **List**. The **Server Certificate** page is displayed.
5. Click the certificate to be pushed or rolled back.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Push failed.	Creating local certificate files failed while Backup.	Provide required access to AppViewX to create local files
Certificate Push Failure	Invalid certificate, key, or trust location is given.	Provide the valid certificate, key, or trust location while adding an application connector.
Bind Failed as the SSL is disabled for the port	SSL is disabled for the given port on the server.	Kindly enable SSL for the port on the server.
KeyStore creation failed	Unable to create the Keystore locally.	Provide required access to AppViewX to create local files

Troubleshooting Weblogic Linux

- Overview
- Issues in Device Addition using AppViewX UI
- Issues in Communicating to Weblogic Linux
- Issues in Fetch Config
- Issue in Discovery
- Issues in CSR generation
- Issues in Push and Rollback

Overview

This section helps you troubleshoot the common problems that you might encounter when using Weblogic Linux functionalities. This guide will give more troubleshooting processes on issues related to Weblogic Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

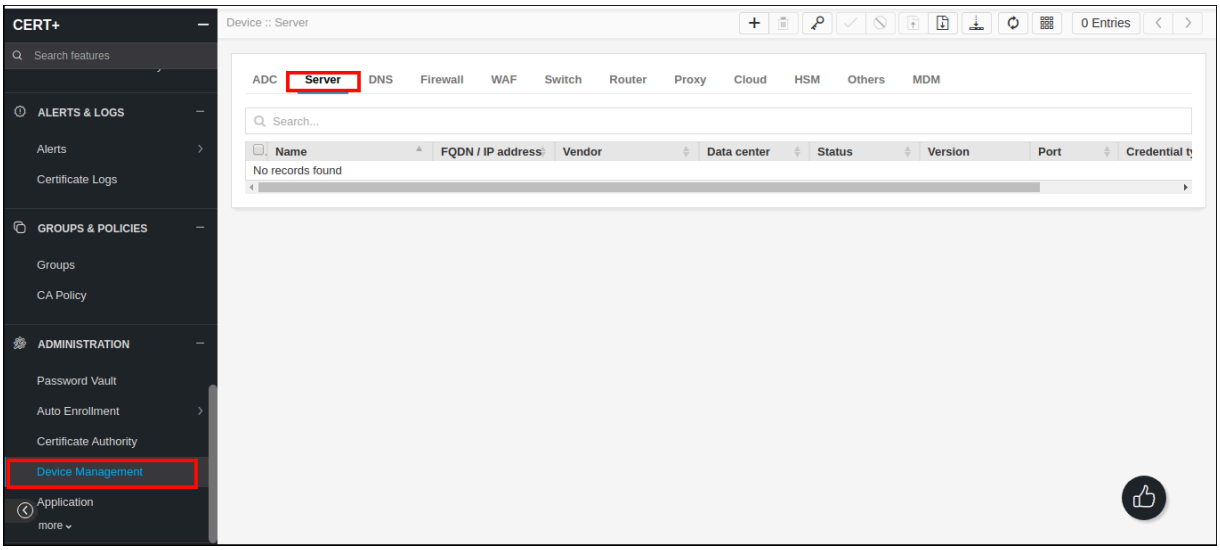
Issues in Device Addition using AppViewX UI

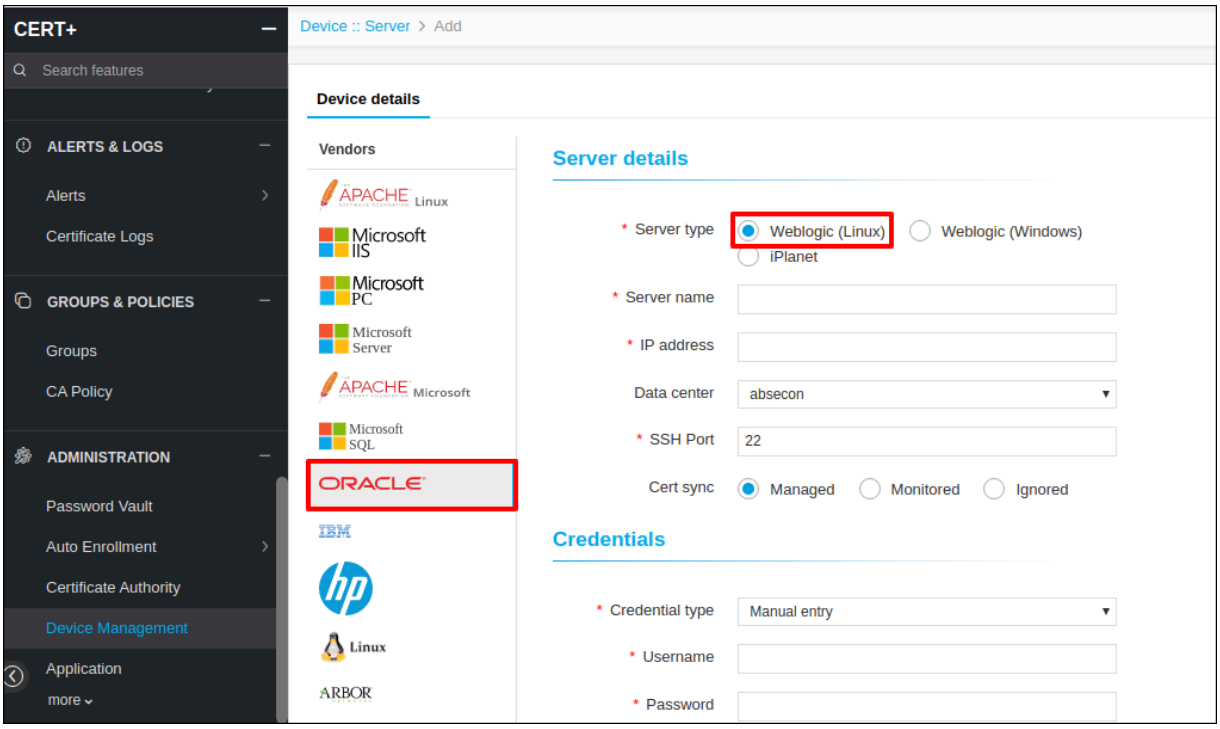
Issues in the Device Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Oracle**.
7. Click **Server type** as **Weblogic(Linux)**.
8. Fill in the appropriate details.
9. Click **Add**.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

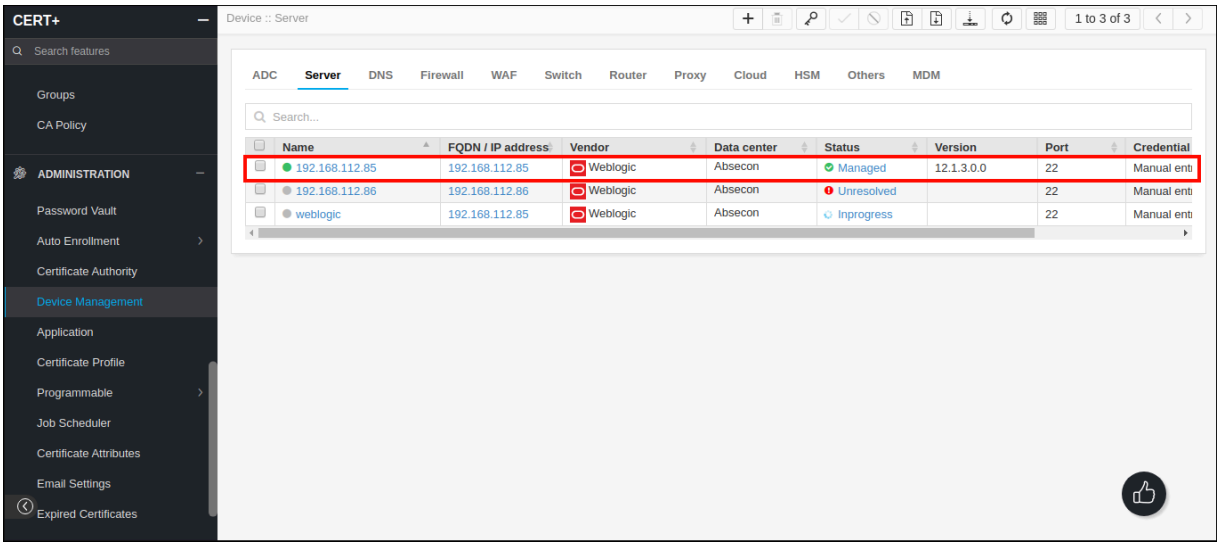
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

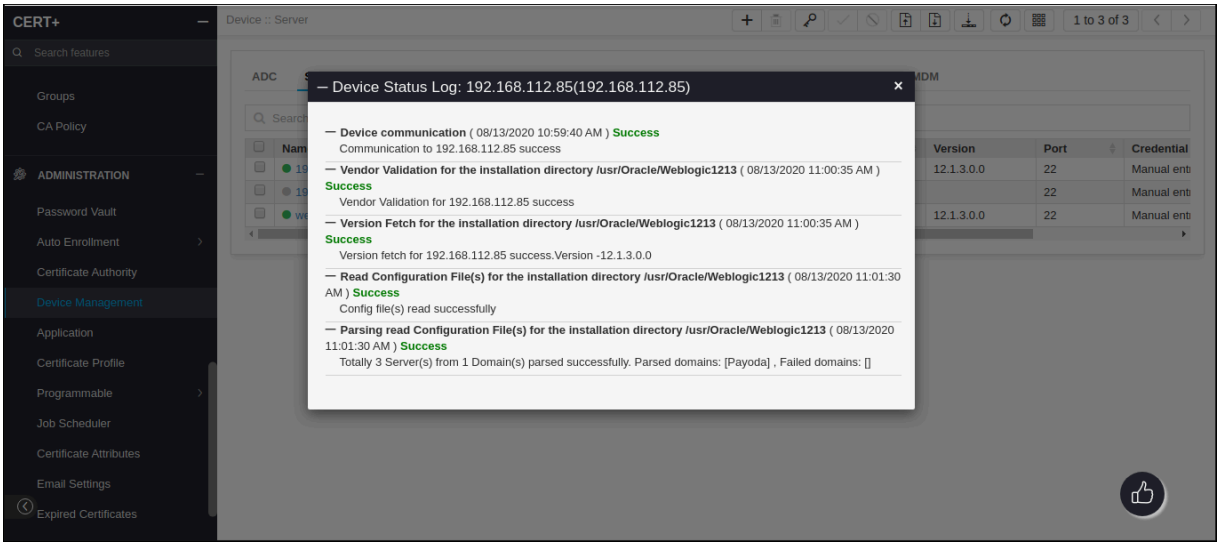
Issues in Communicating to Weblogic Linux

Issues in the Communicating to Weblogic Linux

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Failed to connect to the server.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
No weblogic process is running	Weblogic processes running on the destination machine might be down.	Kindly check the status of the Weblogic process running in the destination machine.

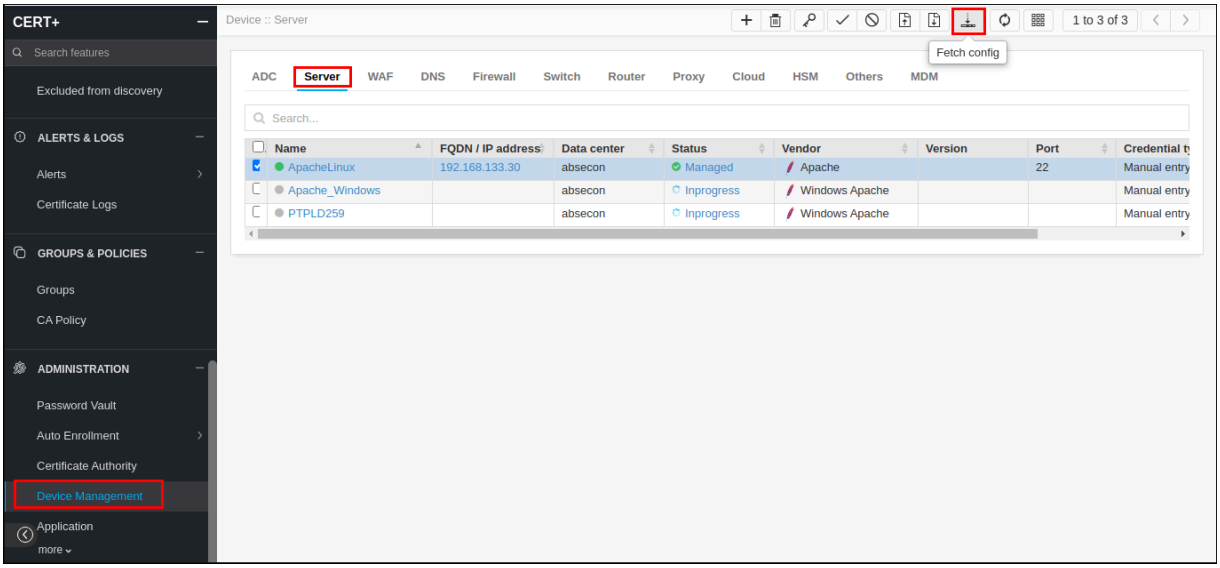
Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Domain-registry.xml is not accessible in the given path.	Given path may be invalid or AppViewX does not have permission to access the file in the path.	Please enter a valid path or Check permissions to access the file.
Config file parsing failed.	1. Configuration file might be corrupted/ empty. 2. AppViewX is not able to read/ parse the Config files from the server.	1. Verify if the configuration file is correct. 2. Check if the server has proper config files related to the Weblogic server and AppViewX has proper read permissions.

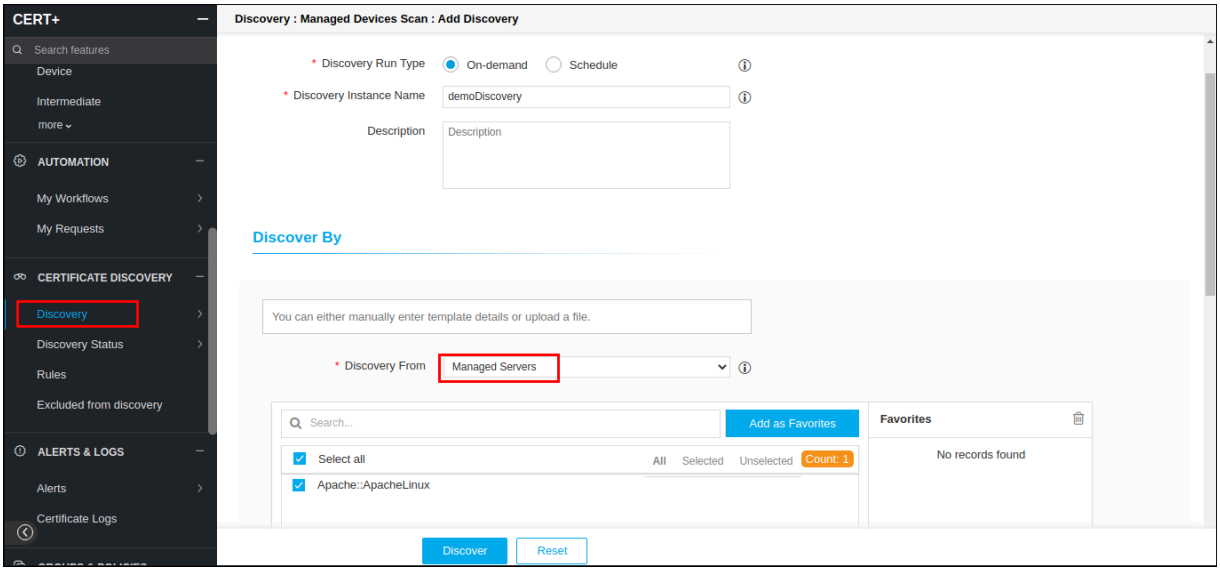
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not entered or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception while fetching key and location details from request.	Certificate location details provided during the server addition might be wrong.	Check and provide the valid certificate location during server addition.

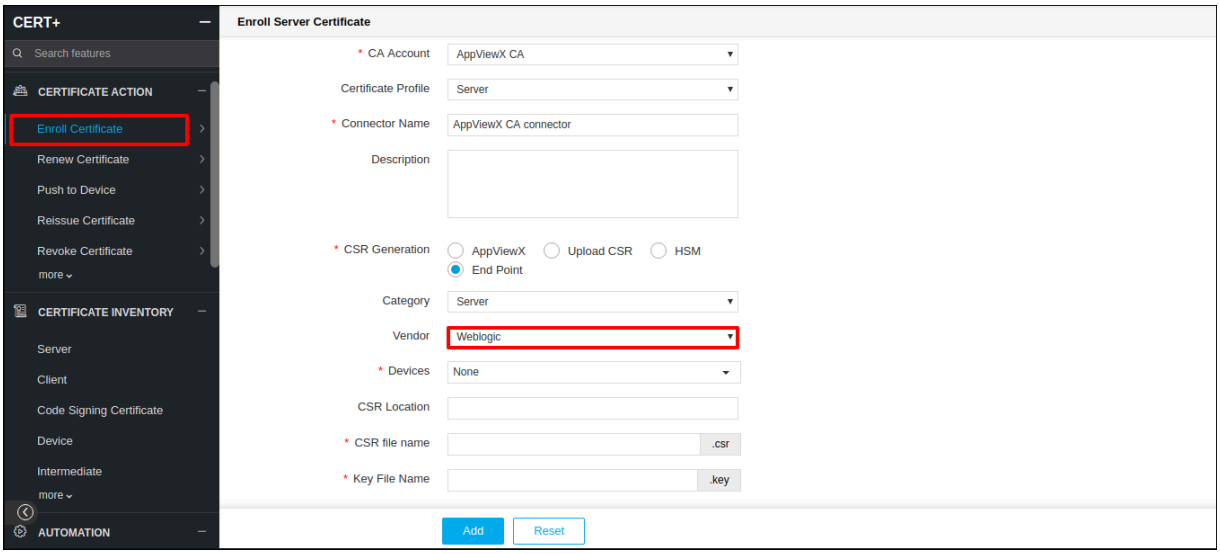
Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the correct **Category** from the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Select **Weblogic** as the **Vendor** from the dropdown. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to parse configuration to fetch currently associated data.	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
No server certificate is found	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
Exception while downloading trust store / Exception while parsing certificate	AppViewX is not able to download the trust store from the server.	Check if AppViewX has permission to download the trust store from the device.
Certificate and/or key missing	Certificate provided in the push request might be invalid.	Check if the certificate that is being pushed is valid.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is supported by Weblogic servers.
Push cannot be performed automatically for the Keystore type 'DemoIdentityAndDemoTrust'. Kindly customize the keystore locations in the connector.	Customize push location not provided during push operation.	Provide a location to push the certificate inside the server.
Parsing a certificate is failed	Certificate content might be invalid.	Check the certificate content.
Exception while writing file to avx local.	AppViewX may not have access to the local/export directory.	Check if AppViewX has permission for the local/export directory.
Certificate push is failed.	Invalid location provided.	Check the location provided is valid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	User is not having permission to push file to the location.	Check if the user has permission to access the location.
Unable to perform Bind for the server.	Server may not be running in the given address and port.	Check if the server is running in the given port and listen address
Unable to open edit session for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to perform edit for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to save the current changes made to the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state. Previous work order is in progress and not completed. AppConnector might not be in sync.	Push to device after certificate has been retrieved from CA. Initiate push after previous work order is finished. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/ rollback workflow from the Workflow section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Linux

- Overview
- Issues in Device Addition using AppViewX GUI
- Issues in Communicating to Apache Linux
- Issues in Fetch Config
- Issue in Discovery
- Issues in CSR generation
- Issues in Push and Rollback

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

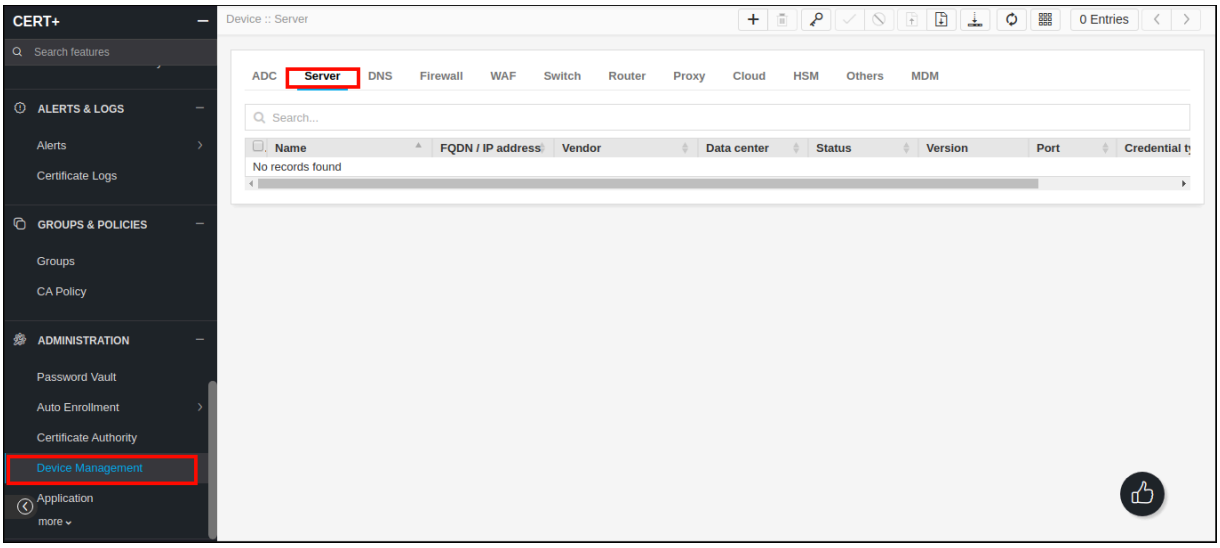
This section helps you troubleshoot the common problems that you might encounter when using Websphere Linux functionalities. This guide will give more troubleshooting processes on issues related to Websphere Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

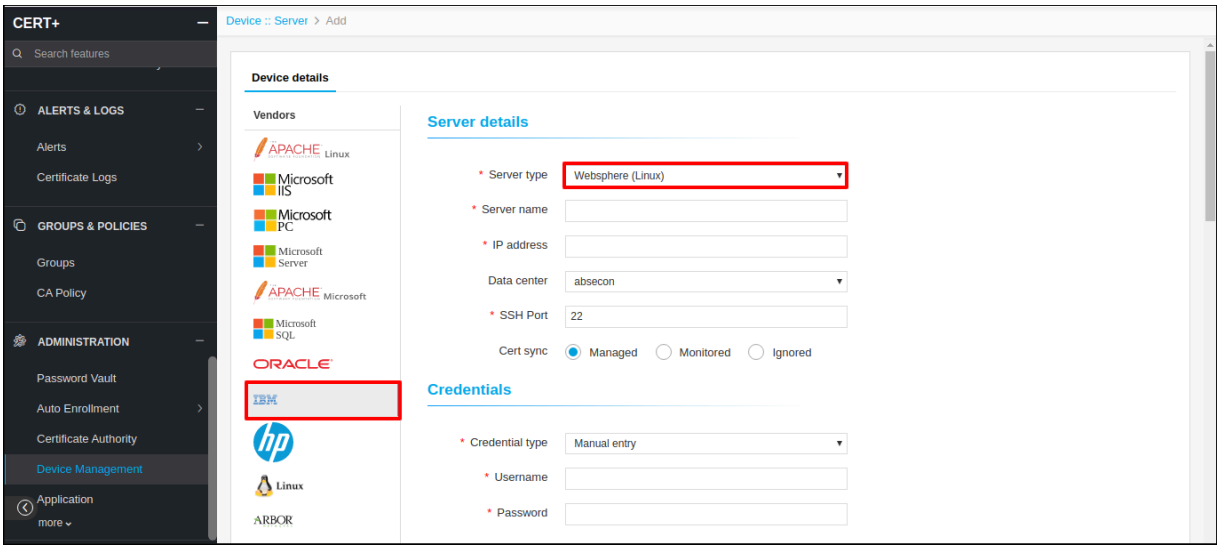
Issues in Device Addition using AppViewX GUI

Issues in Device Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **Oracle**.
7. Click **Server type** as **Websphere(Linux)**.
8. Fill in the appropriate details.
9. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might either be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

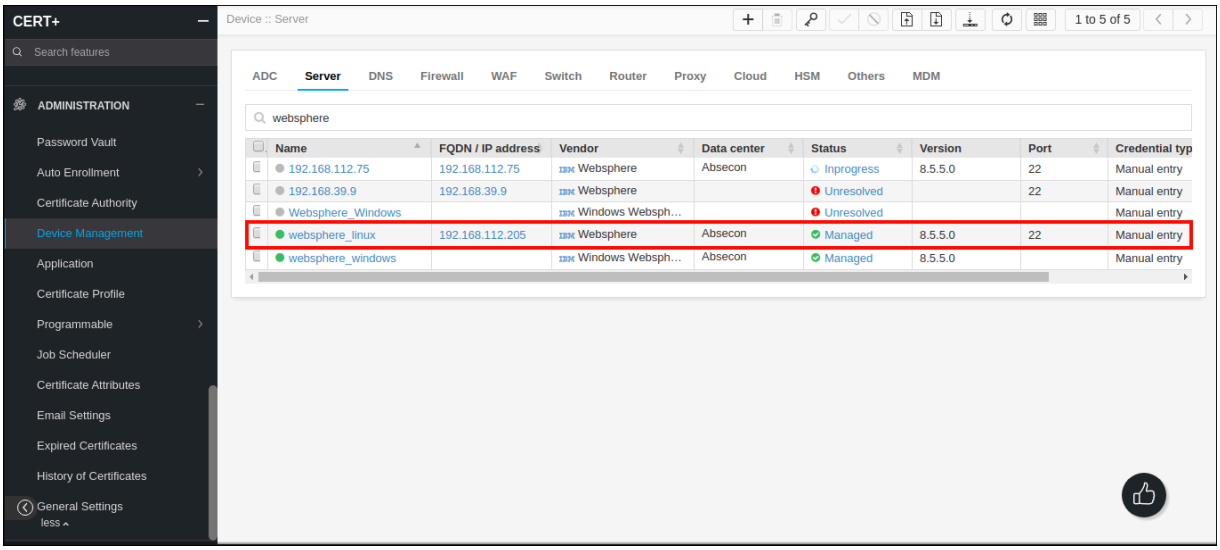
Error Message	Possible Cause	Possible Solution
WSadmin User name and WSadmin Password should not be empty	WSadmin username or password might be empty.	Add the valid WSadmin username and password.
Kindly add at least one WSadmin detail before saving.	WSadmin details are not added.	Add at least a single WS admin details.

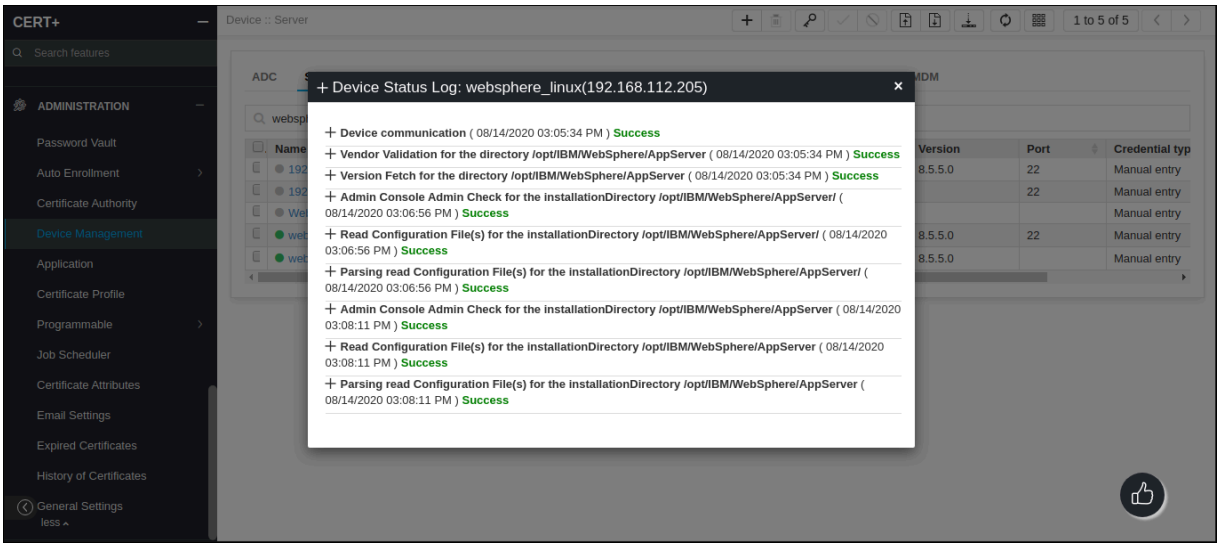
Issues in Communicating to Apache Linux

Issues in Communicating to Apache Linux

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

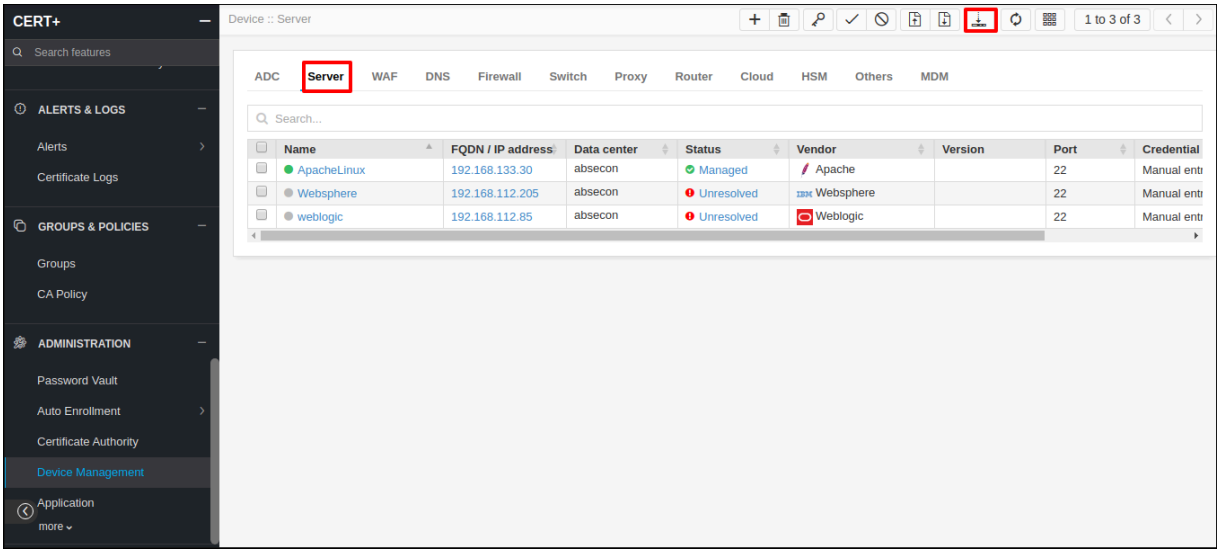
Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Ip does not belongs to Websphere	Destination machine might not have the required configuration for a Websphere application server.	Please check if the machine has Websphere configurations available in the destination machine.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Issues in the Fetch Config

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click Fetch **Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the permission for the installation path.	Check if AppViewX has permission to access the installation path.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid Credentials.	Invalid Credentials given for installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.
Invalid installation path	Installation path does not exist.	Check if the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects are unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check if there is permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

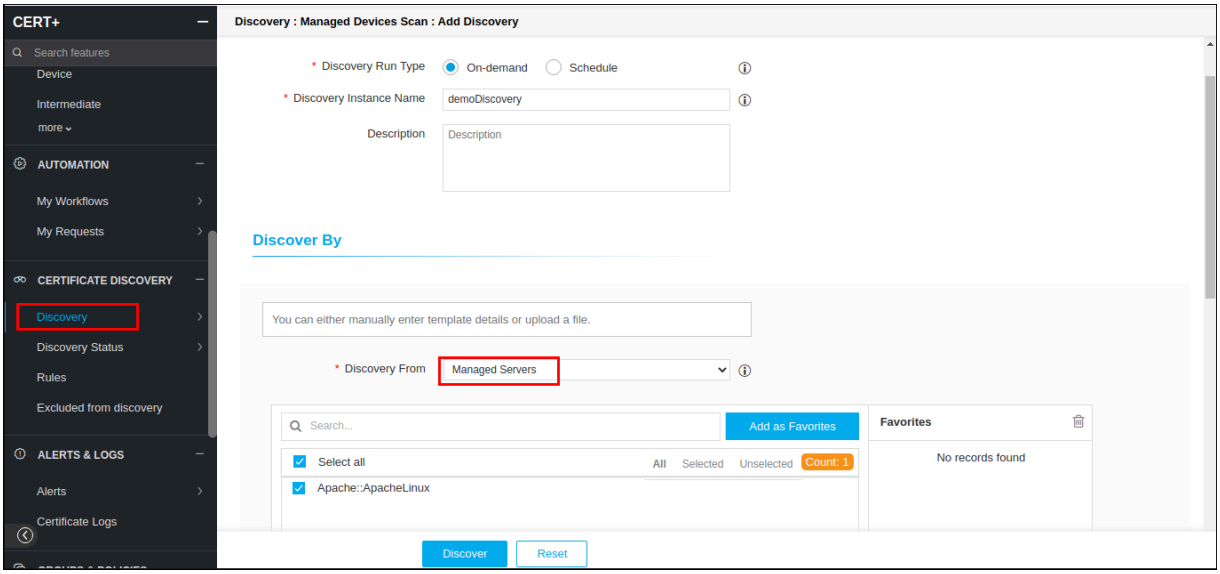
Issue in Discovery

Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or its length is less than 2 characters. Interval between batches info. is missing when execution type is sequential.	Enter a valid name with a minimum of 2 characters. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By “section.	Select at least one device to discover certificates from.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the necessary permission for the installation path.	Check if AppViewX has permission to access the installation path.
Invalid Credentials.	Invalid Credentials are given to installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.
Invalid installation path	Installation path does not exist.	Check the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check for valid permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

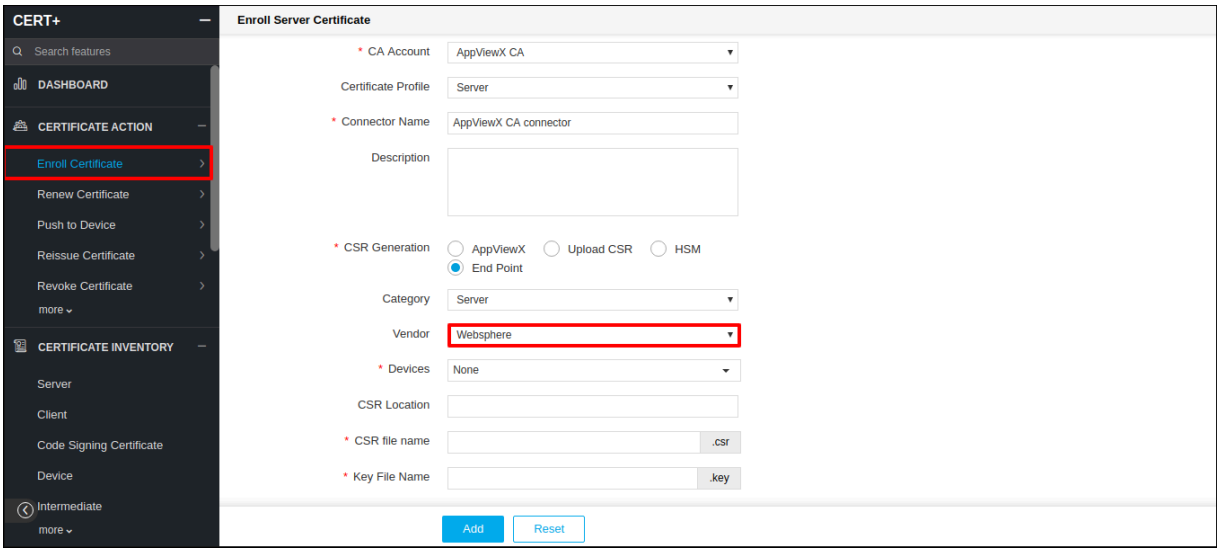
Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. Click the correct **Category** from the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Click **Websphere** as **Vendor** from the dropdown. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Check and provide valid credentials to communicate with the device.
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported in the target machine.	Provide valid key type.
CSR and Private key has been failed.	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
security.xml file read operation failed	AppViewX may not be able to read security.xml of the profile.	Check if AppViewX has permissions to read security.xml of the profile.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Config file parsing failed	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
Insufficient information to fetch backup data available in the server.	Configuration files fetched from the server may not have sufficient information.	Check if the config file has all the information related to server configuration.
Unsupported bit length	Bit length is not supported by the server.	Provide a valid bit length that is supported by Websphere server.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is supported by Websphere servers.
Creating local certificate file failed - <Detailed Message>	AppViewX is not able to create file in a temporary folder.	Check the detailed message to determine the remedy.
Server certificate is not available to push.	Server certificate location may be invalid.	Check if the trust store location is available.
Private Key doesnot exists for certificate	Private key may not be available for the certificate.	Check if the private key for the certificate is available.
Private key parsing failed for the certificate.	Private key may be a invalid one.	Check if the private key is valid.
Writing of converted certificate related files into file in AppViewX local directory is failed.	AppViewX may not have permission to write a file in the export directory.	Check if AppViewX has proper permissions for the export directory.
Certificate created date is earlier than server present time	The starting of certificate validity period is earlier than the servers present time.	The starting of certificate validity period should match with the server’s time. It should be greater than the server’s present time.
Unsupported Type	Certificate format is not supported by the server.	Check for the supported certificate formats.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Error found in wsadmin response	The WSadmin console may not be working on the server.	Kindly check WSadmin console is properly working or not
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Windows

- Overview
- Issue in Server Addition using AppViewX GUI
- Issues in Device communication
- Issue in Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Websphere Windows.

Issue in Server Addition using AppViewX GUI

Issue in Server Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **IBM**.
7. Select **Websphere(Windows)**.
8. Fill in the appropriate details.
9. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

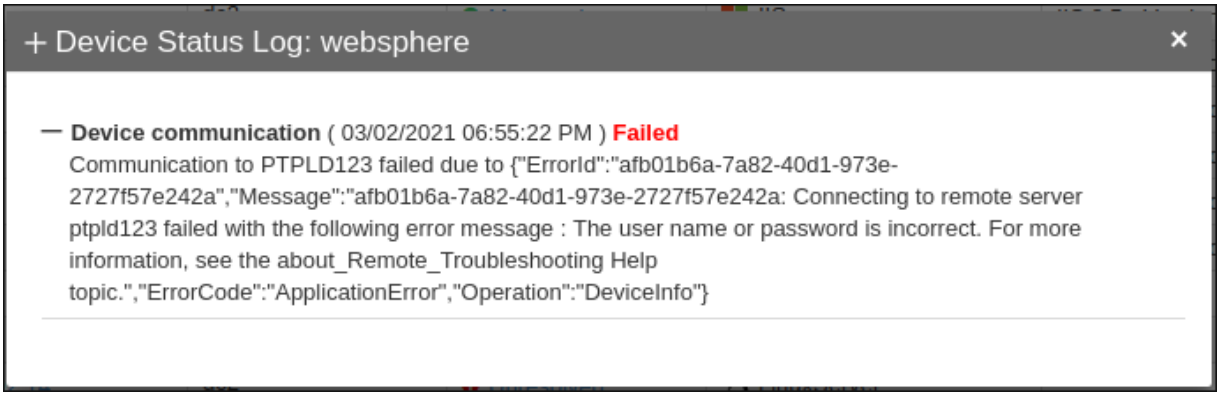
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

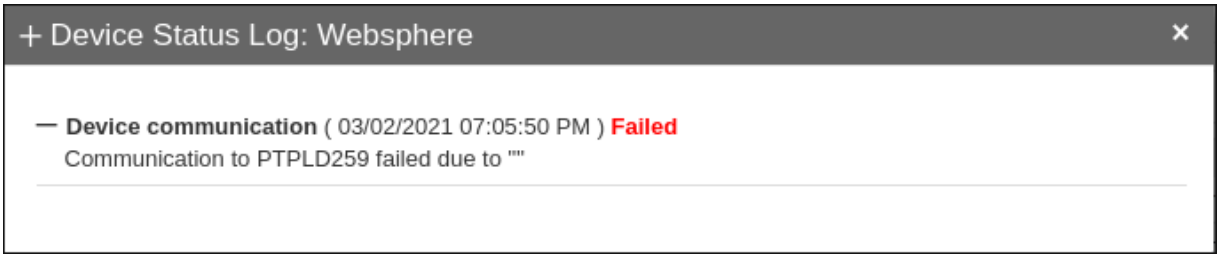
Issues in Device communication

Issues in the Device communication

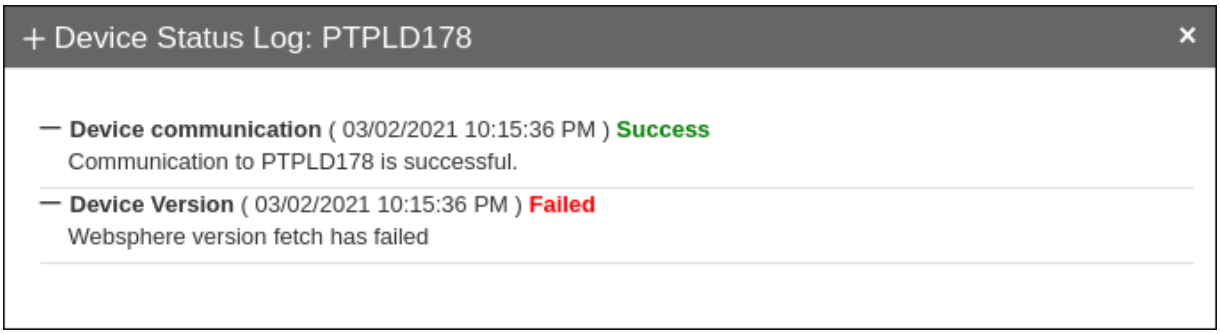
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

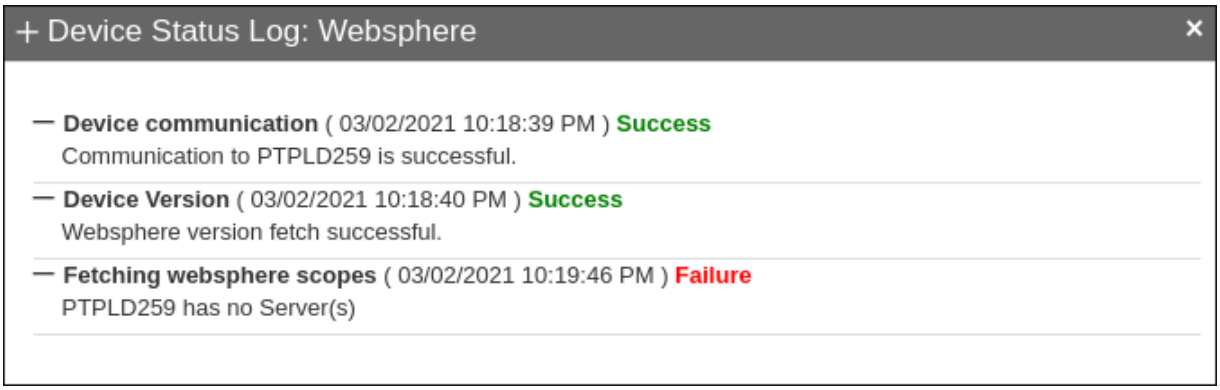






Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Connecting to remote server ptpld123 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	Invalid hostname/ Invalid credential	Kindly check if the given host is reachable. Kindly provide valid credentials and update the device details.
Communication to <host> failed.	Windows Agent is not reachable or down	Kindly check if windows agent configured and in running state.
Websphere version fetch has failed	Websphere setup is not available/not	Kindly validate is Websphere

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	configured in given device	configured properly

Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch.	1. No valid keystore files available in the given path. 2. Users don't have access for the configured location/file. 3. Web Server or WAS console is not active.	1. Kindly Ensure the given certificate location has a valid cert. 2. Kindly ensure users have proper access privilege to read certs. 3. Kindly ensure WebServer is in up and running state .

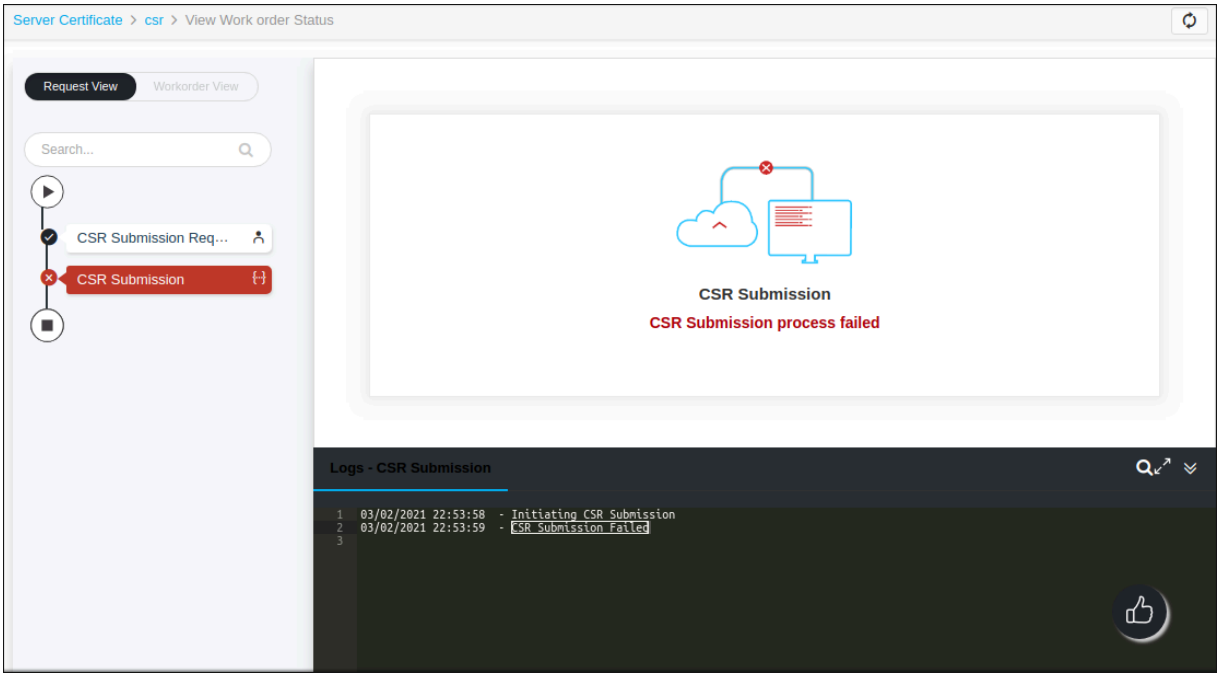
Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **Websphere Windows**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

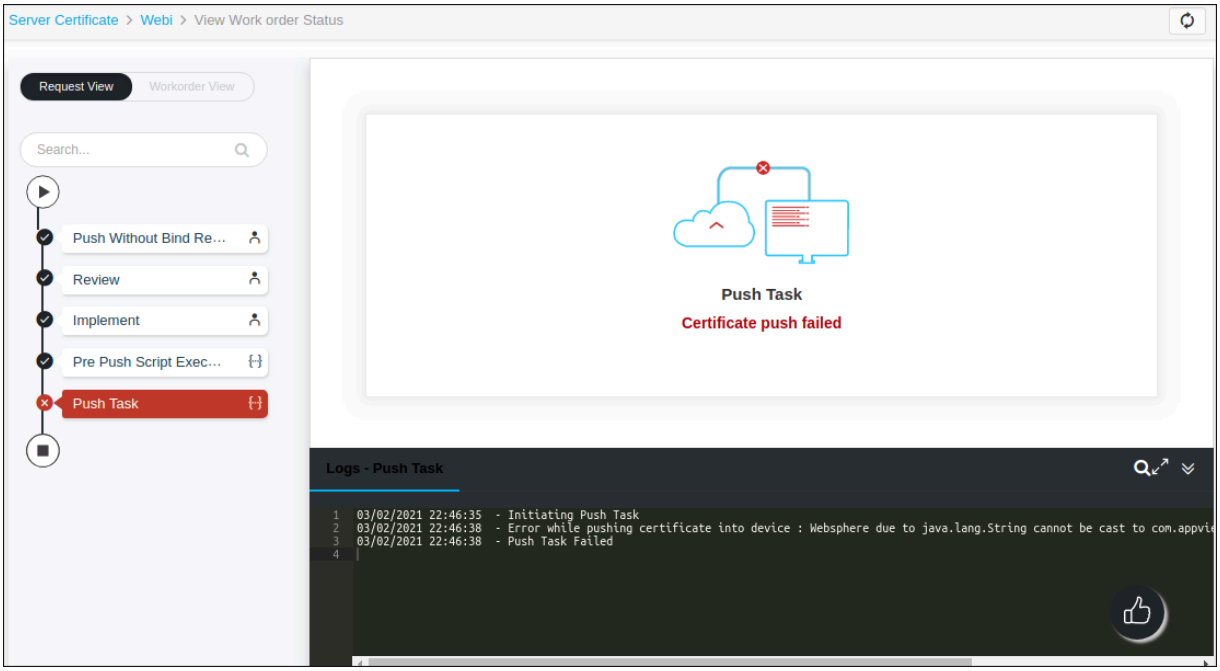
Issues in Certificate Push

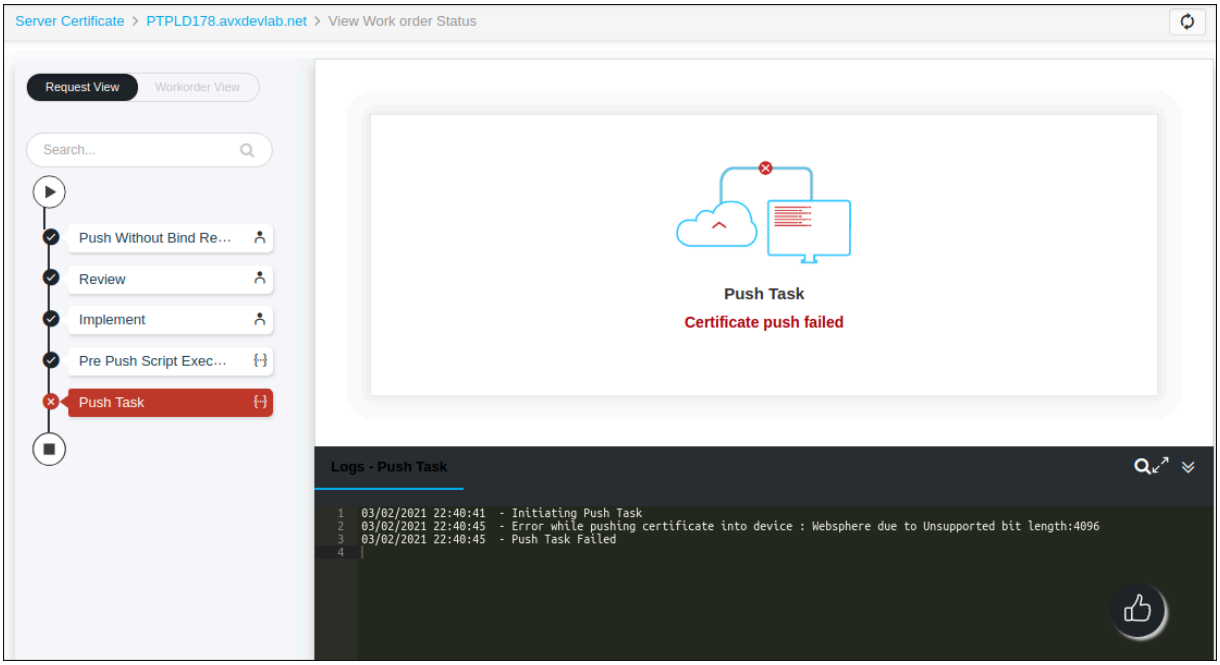
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

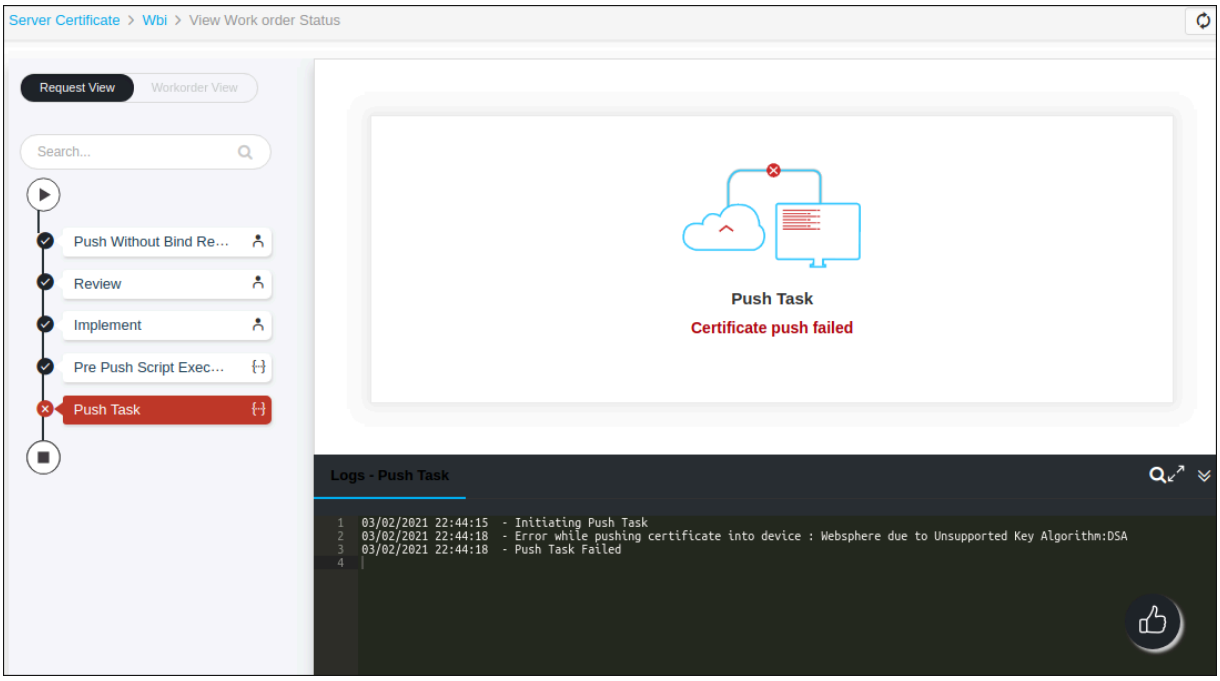
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

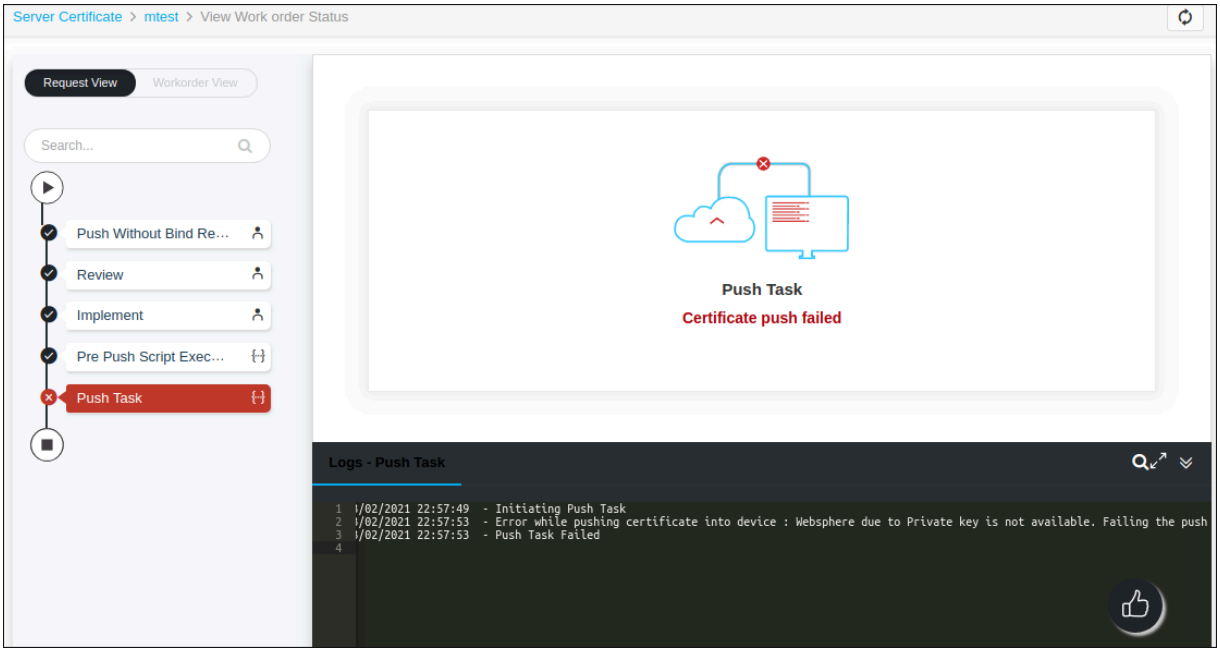
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Linux server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Error while pushing certificate into device.	User has restricted access to the path configured to	Kindly ensure the user is configured while device addition has the read/write access to

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	push the certificate in the application connector	the path configured in application connector to certificate push.
Error while pushing certificate into device : Websphere due to Unsupported bit length:4096.	Websphere will support bitlength up to 2048.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate into device : Websphere due to Unsupported Key Algorithm:DSA	Unsupported key Algorithm.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key. If privatekey is available in the device please select privateKeyInDevice option.

Troubleshooting Windows Apache Server

- Overview
- Issues in Device communication
- Issue in Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

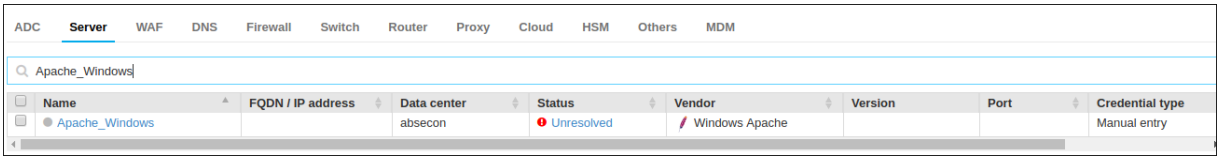
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Apache server.

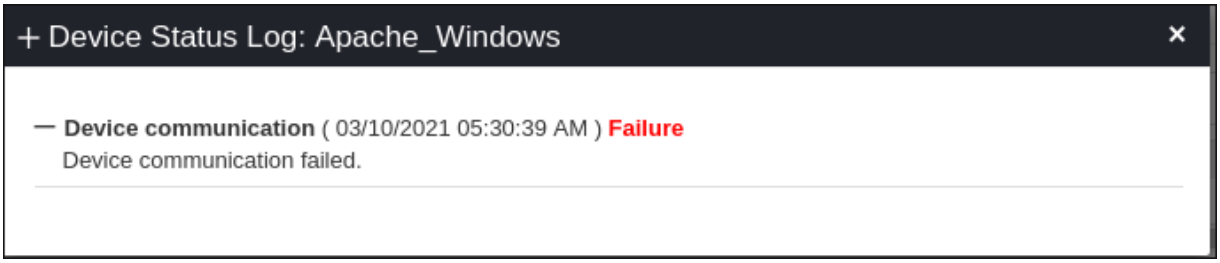
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Windows Apache Device**, click **Status**. The **Device Communication Status** is displayed.





Error Messages

Error Message	Possible Cause	Possible Solution
Device communication failed	1. Given credential is incorrect. 2. Windows agent may not be working. 3. Device not reachable 4.Hostname value is in-correct	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable 4. Ensure windows agent is working for communication mode gateway 5. When the communication mode selected is SSM, Ensure SSM details given are correct

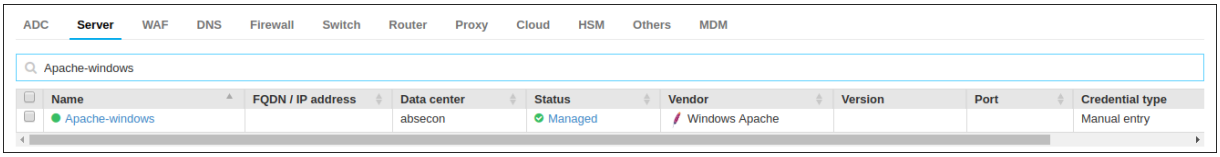
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

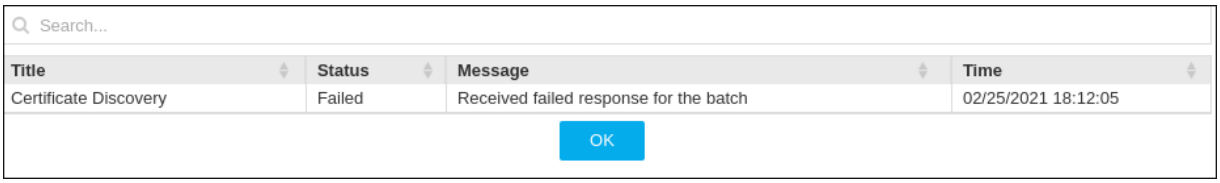
Issue in Discovery

Issue in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.





Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

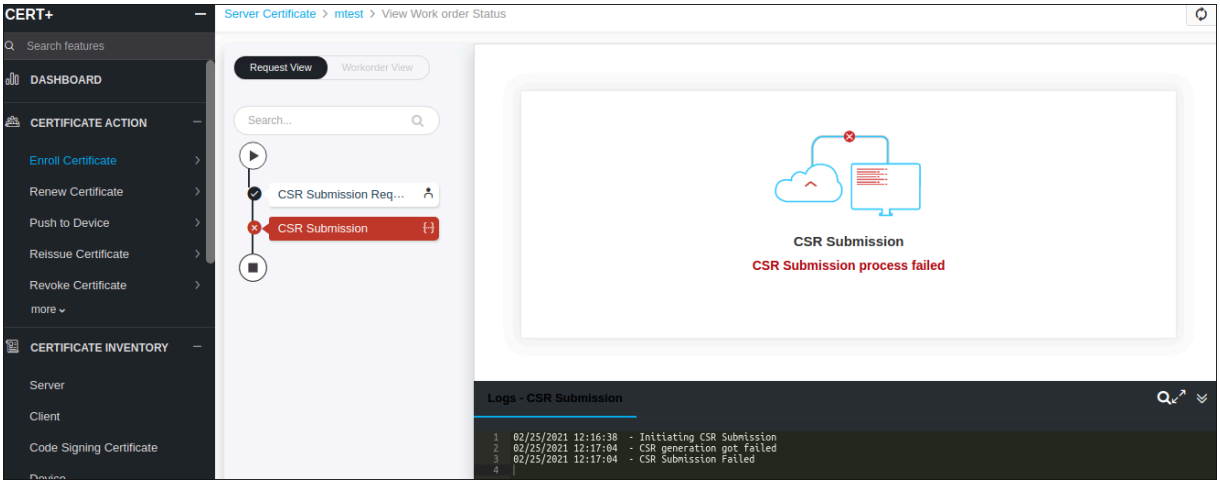
Issues in CSR generation at Endpoint

Issues in CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, Click correct **Category.**
7. From the **Vendor** dropdown, click **Windows Apache**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

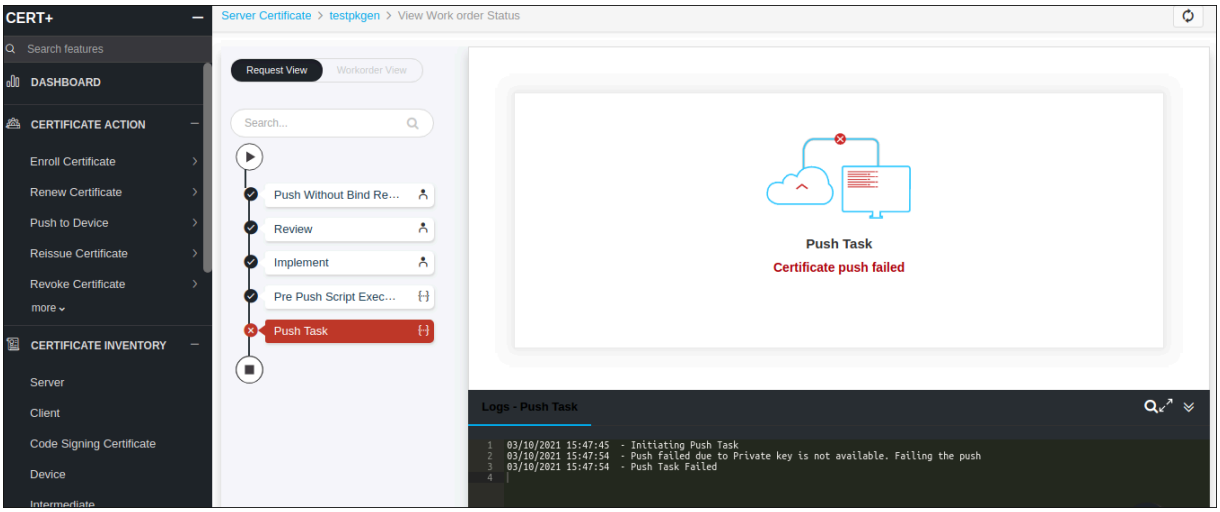
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

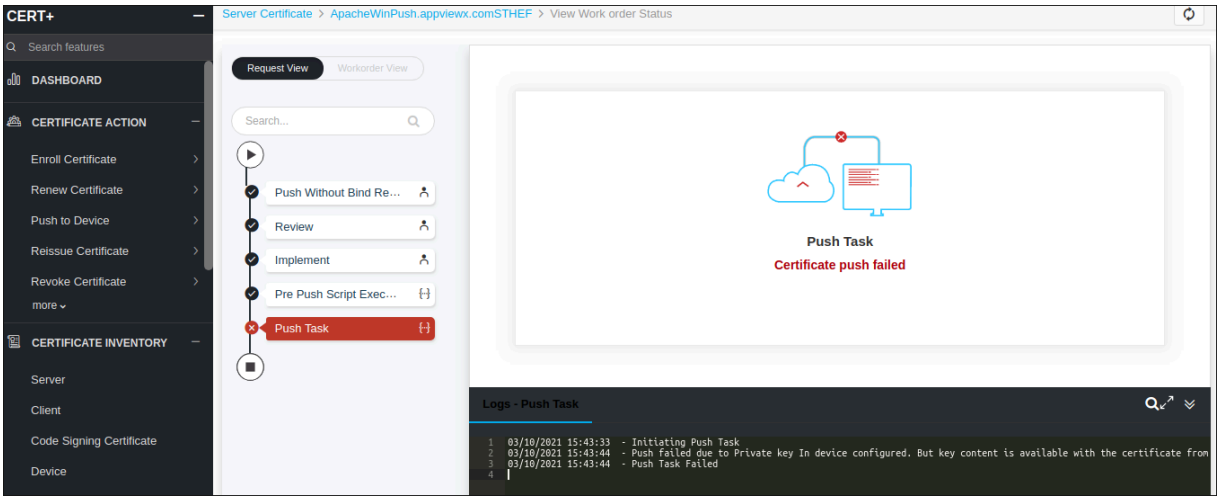
Issues in Certificate Push

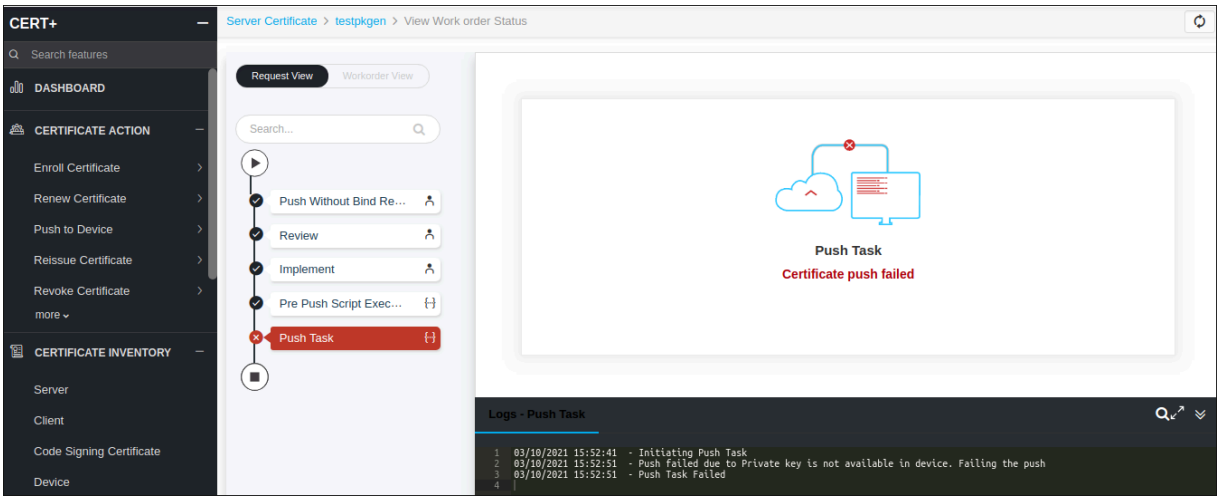
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Windows Apache server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

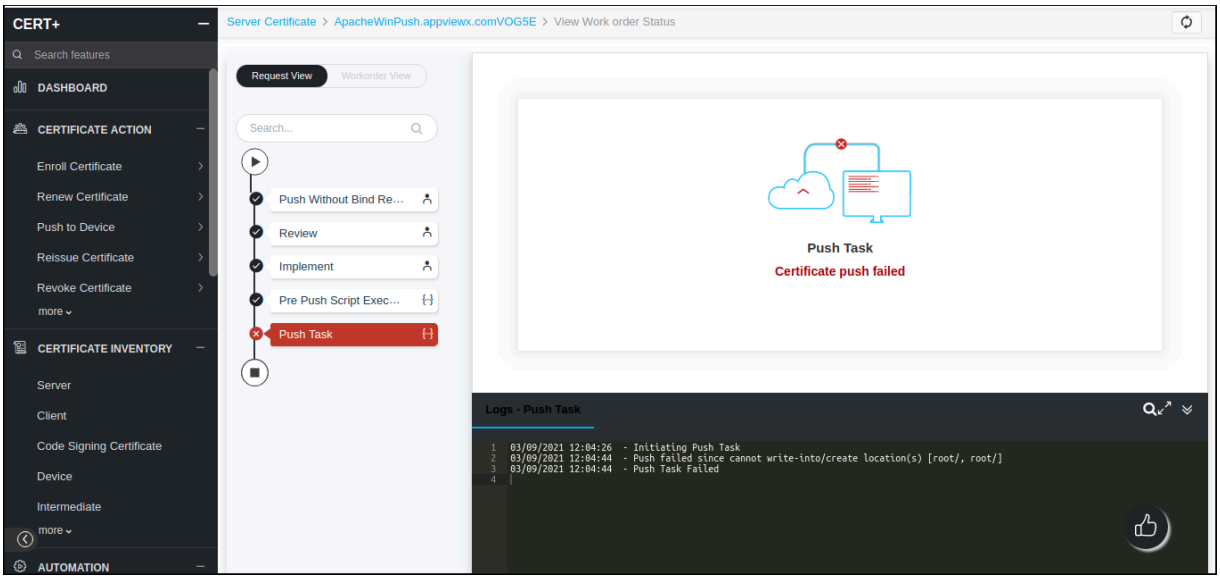
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

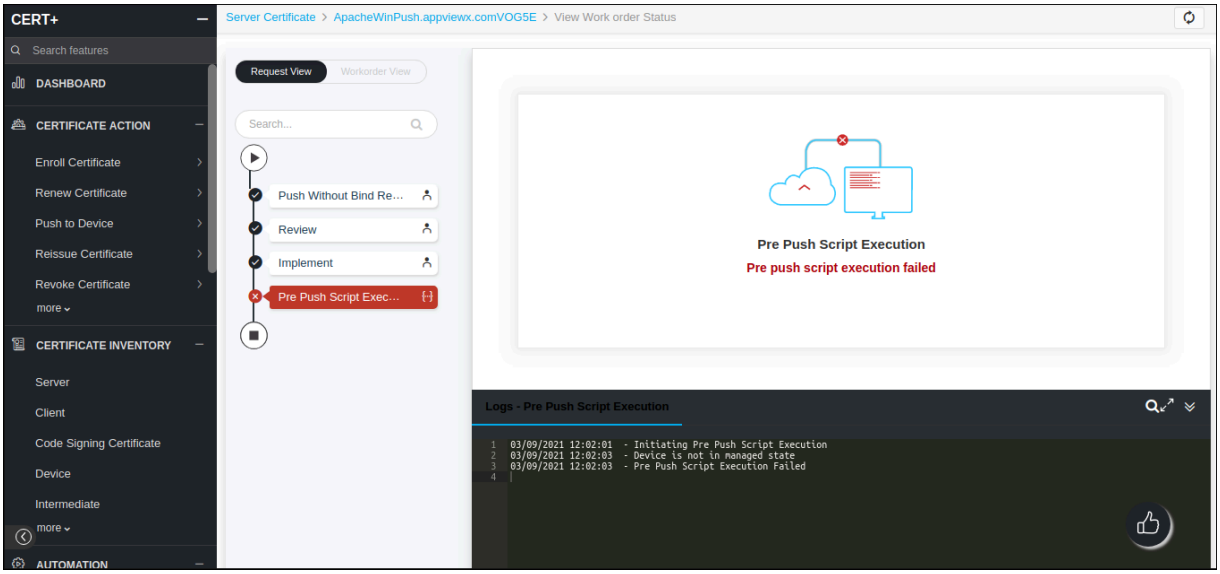






Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Push failed due to Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Push failed due to Private key is not available in device. Failing the push	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have the permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Windows JBoss Server

- Overview
- Issues in Windows JBoss Server Addition using AppViewX GUI
- Issues in Communicating to Windows JBoss Server
- Issues in Accessing Server
- Issues in Config Fetch
- Issues in Certificate Discovery
- Issues in CSR generation
- Issues in Push and Rollback

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

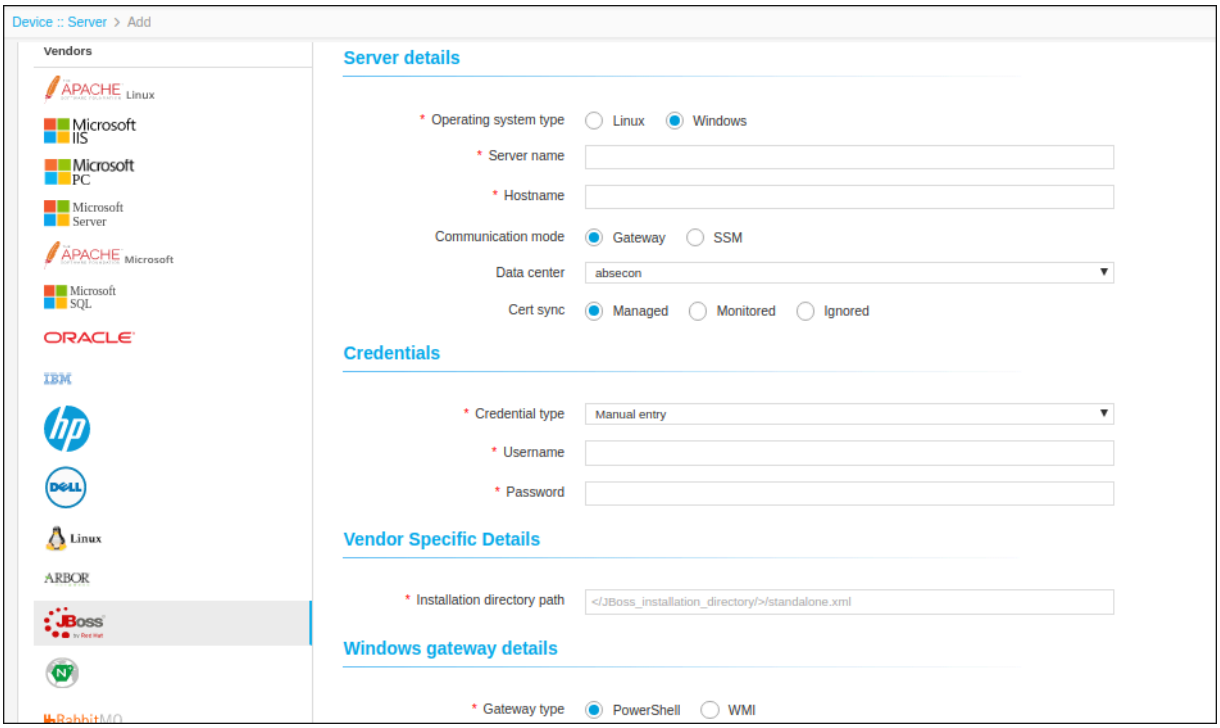
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows JBoss server.

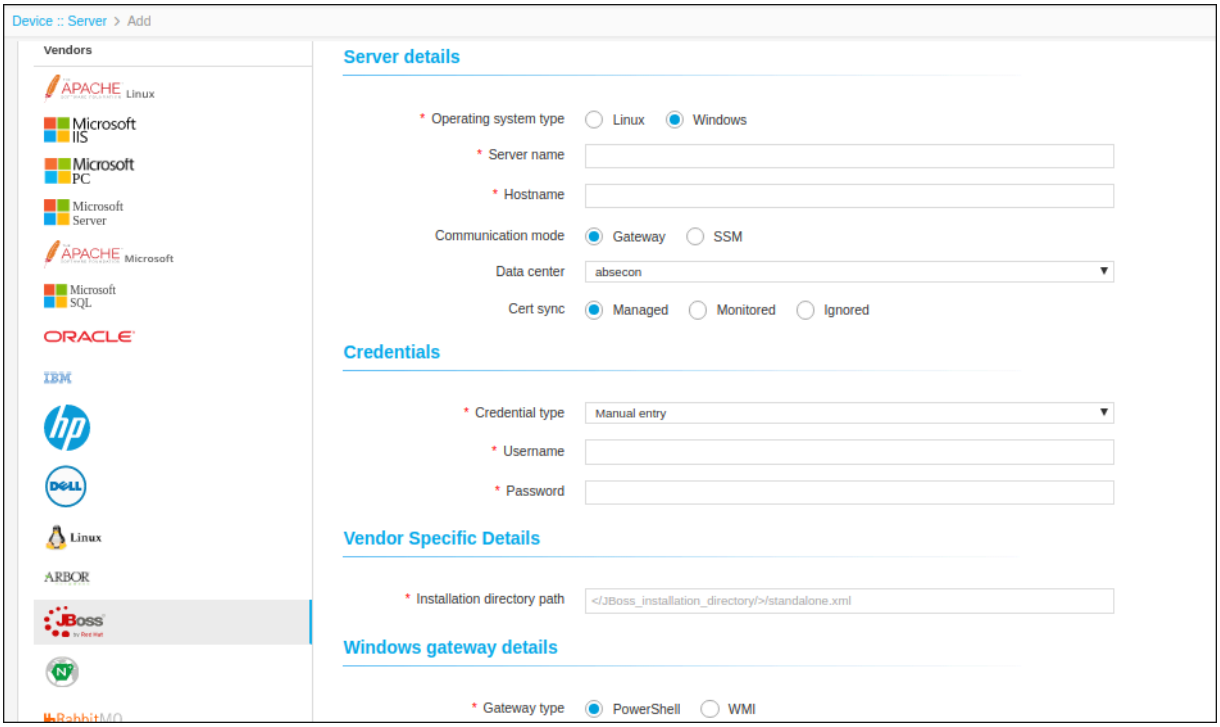
Issues in Windows JBoss Server Addition using AppViewX GUI

Issues in Windows JBoss Server Addition using AppViewX GUI

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. From the icon list at the top right corner, click **Add**. The **Device Addition** page is displayed.
6. From the **Device Details Section** on the left, click **JBoss**.
7. Select **Windows** as **Operating System Type**.
8. Fill in the appropriate details.
9. Click **Add**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

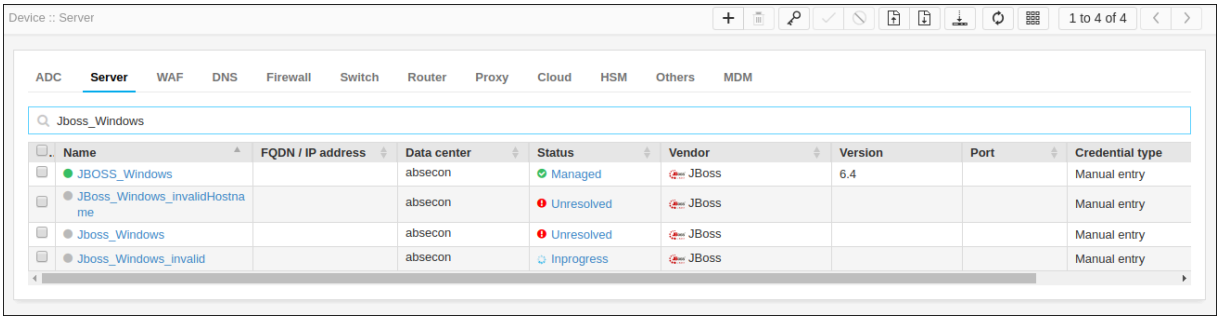
Error Messages

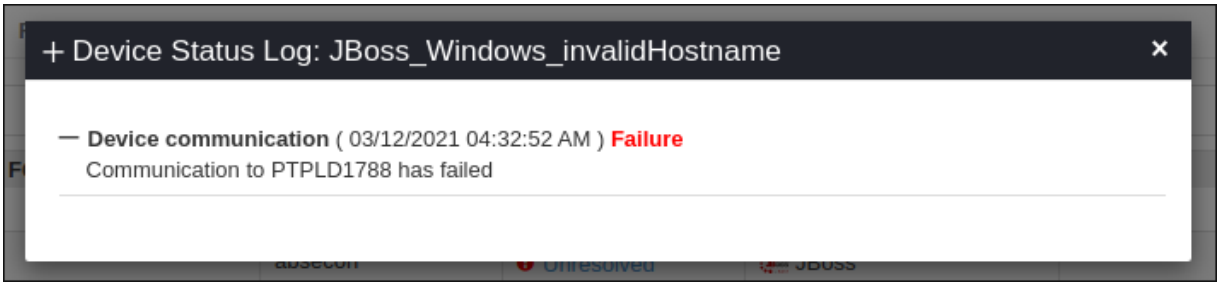
Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Windows JBoss Server

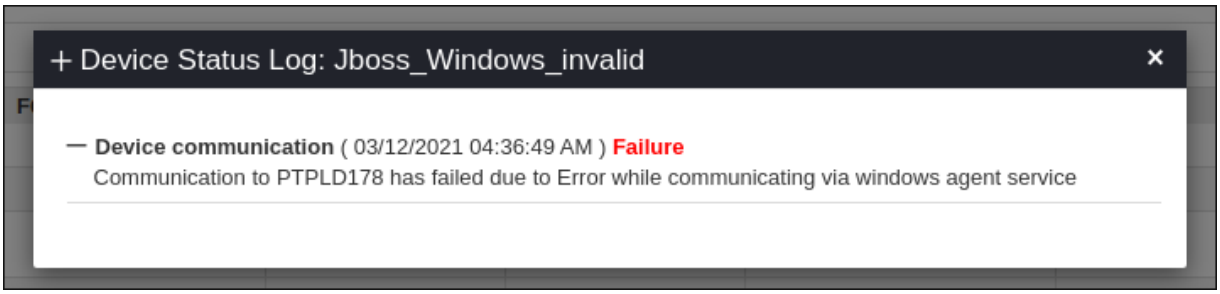
Issues in Communicating to Windows JBoss Server

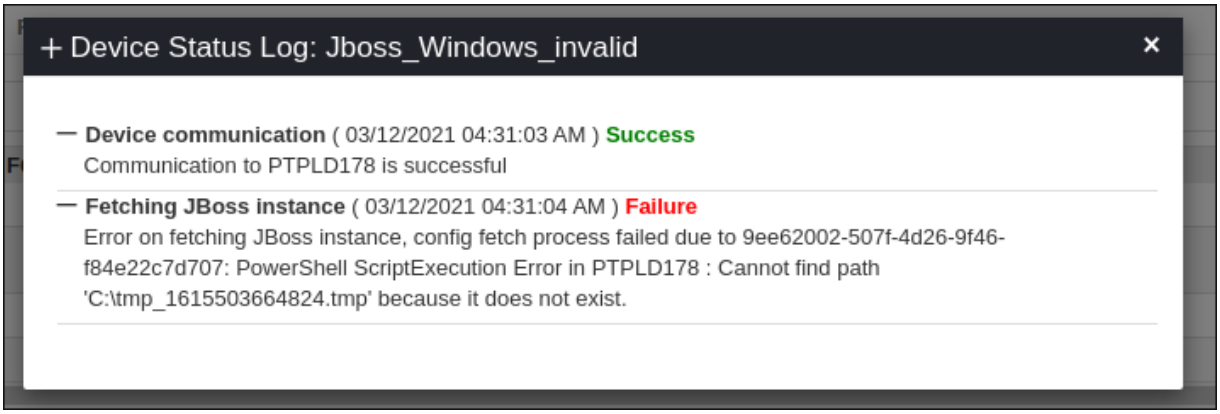
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the device, click **Status**. The **Device Communication Status** is displayed.

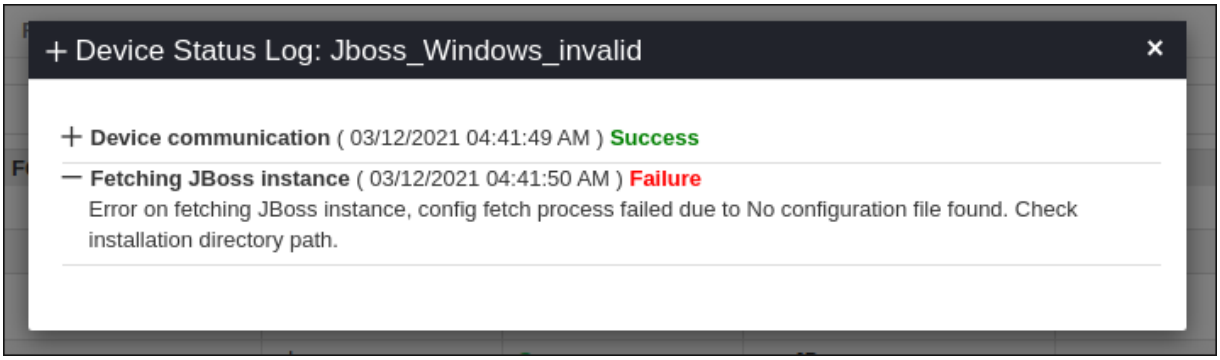




Copyright © 2024 AppViewX, Inc. All Rights Reserved.







Error Messages

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Error on fetching JBoss instance, config fetch process failed due to No configuration file found. Check installation directory path.	Provided installation directory path does not have JBoss configuration files like server.xml / standalone.xml	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.
Error on fetching JBoss instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid installation directory path	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.
JBoss version fetch is failed	No JBoss server running in the target device / something wrong in the JBoss installation	Login manually into the windows server and find the JBoss server bin directory and run the below command to validate the JBoss version For JBoss 4.0.5 <JBoss_server_Directory>/bin/run.bat -V

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		For JBoss 6.4 and 7.0 `<JBoss_server_Directory>/bin/standalone.bat -V` Currently only JBoss 4.0.5, 6.4 and 7.0 versions are supported in AppViewX.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from the environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

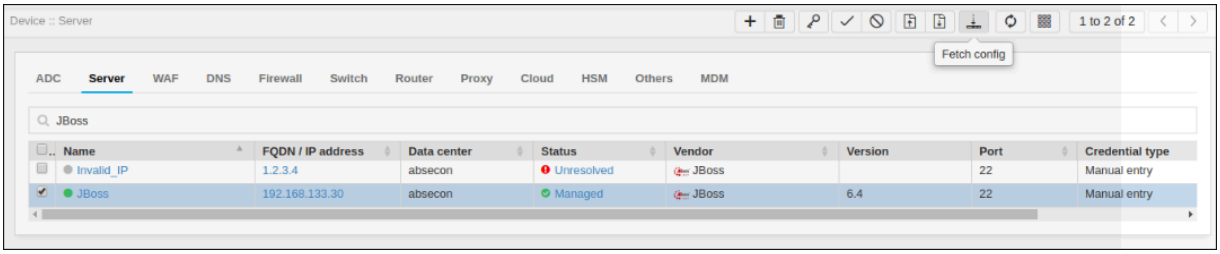
Issues in Config Fetch

Issues in the Config Fetch

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Select the device, click **Fetch Config**.



Error Messages

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	1.Verify the input details and check device status error messages Issues in Communicating to Windows JBoss Server

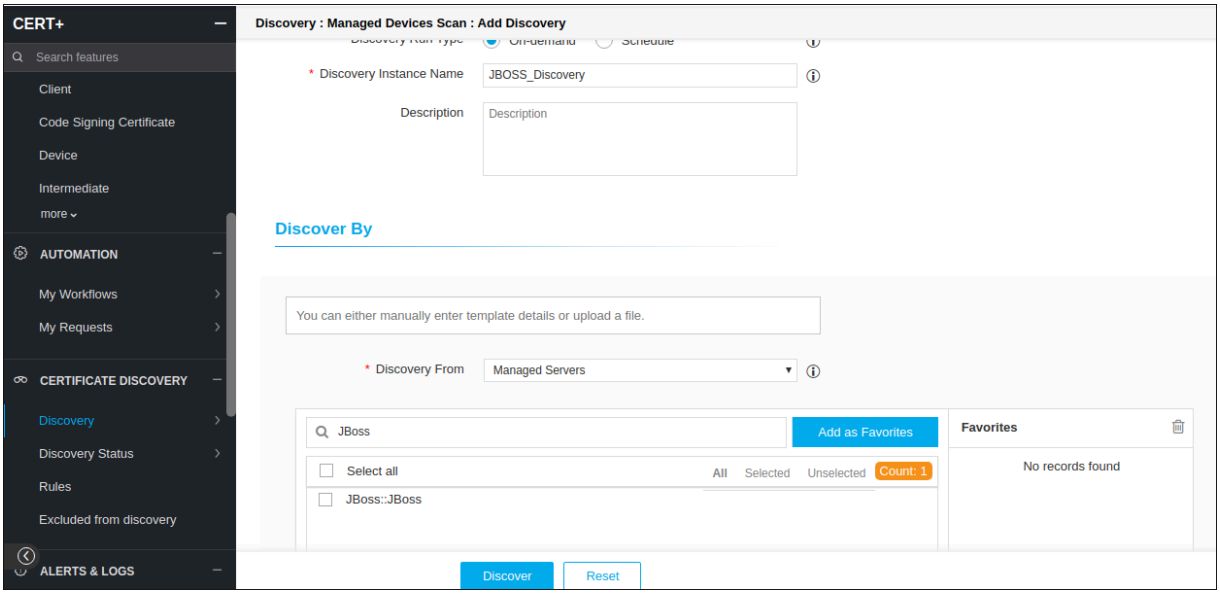
Issues in Certificate Discovery

Issues in the Certificate Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.



Error Messages

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

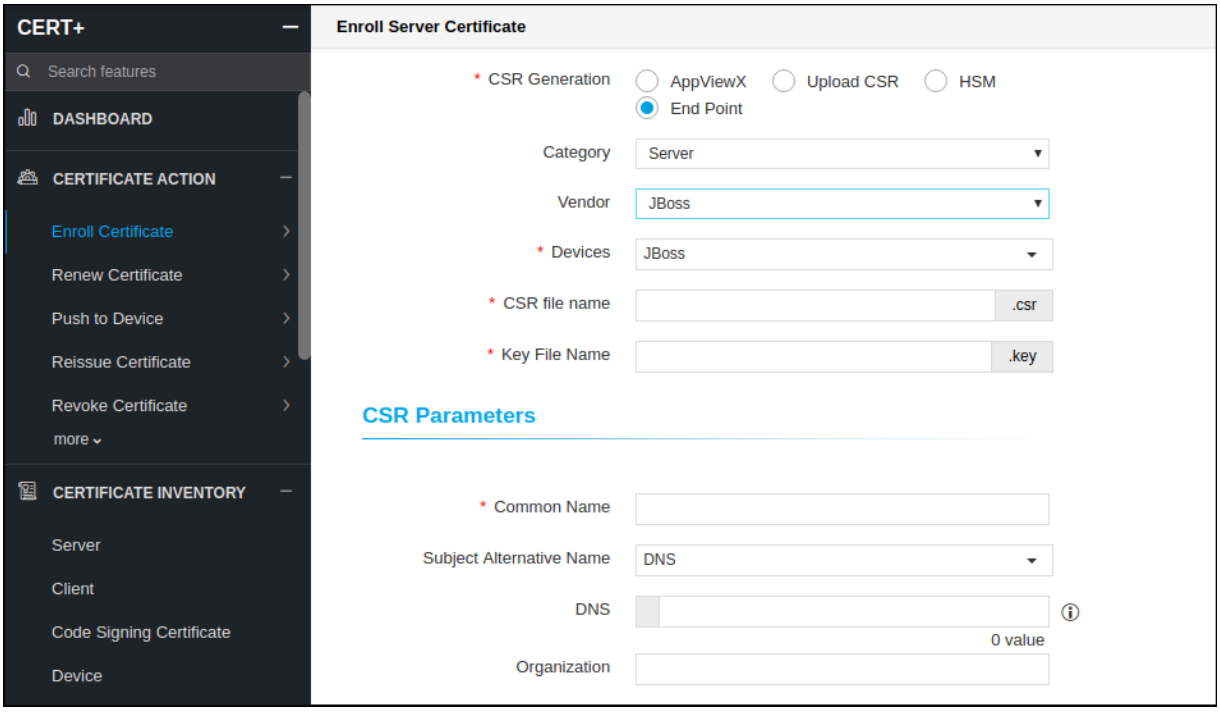
Issues in CSR generation

Issues in the CSR generation

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category**.
7. From the **Vendor** dropdown, click **JBoss**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.

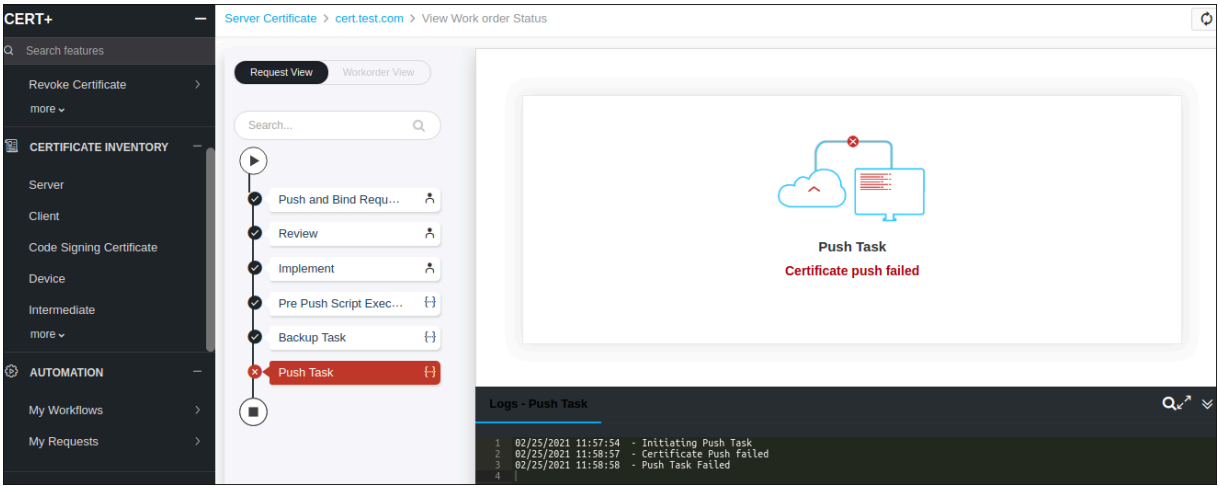
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

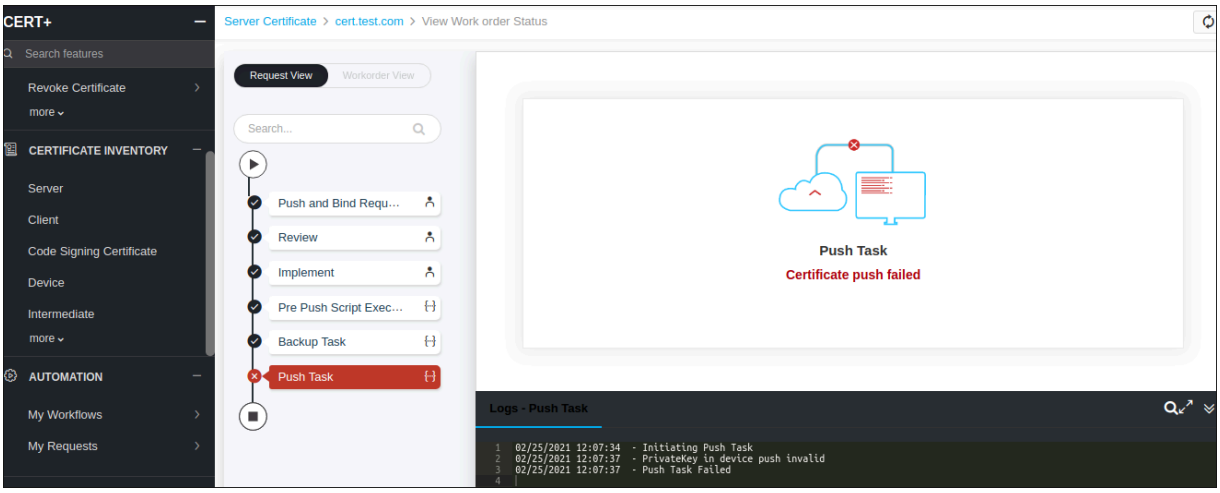
Issues in Push and Rollback

Issues in the Push and Rollback

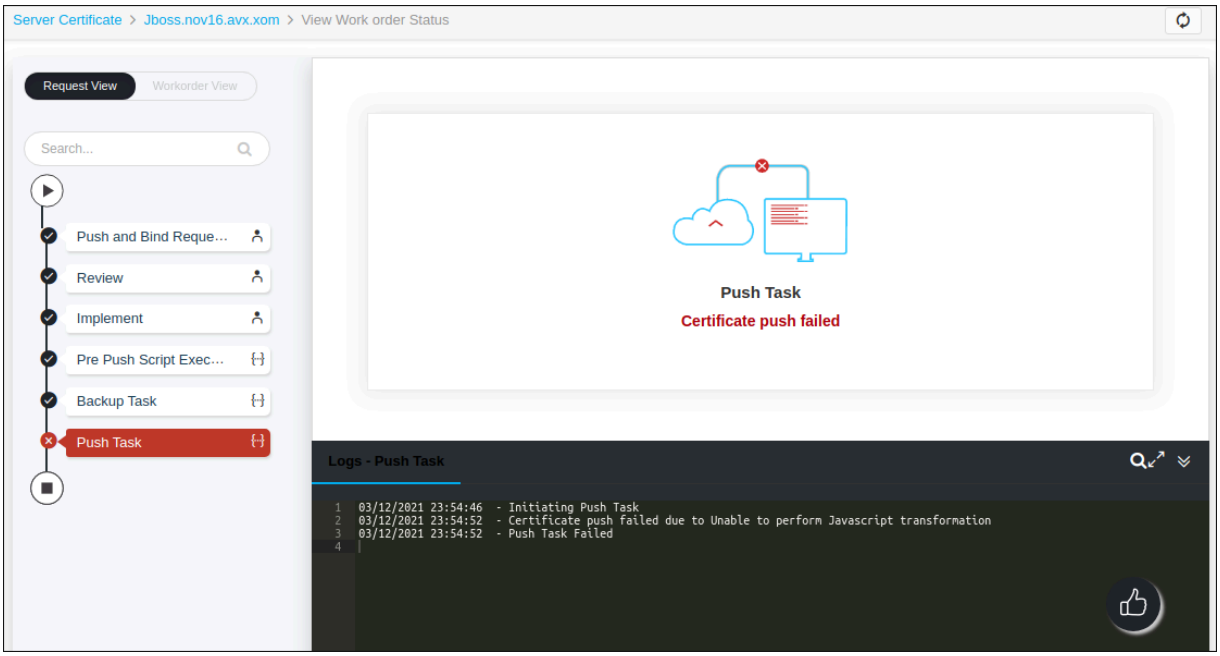
1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **JBoss server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

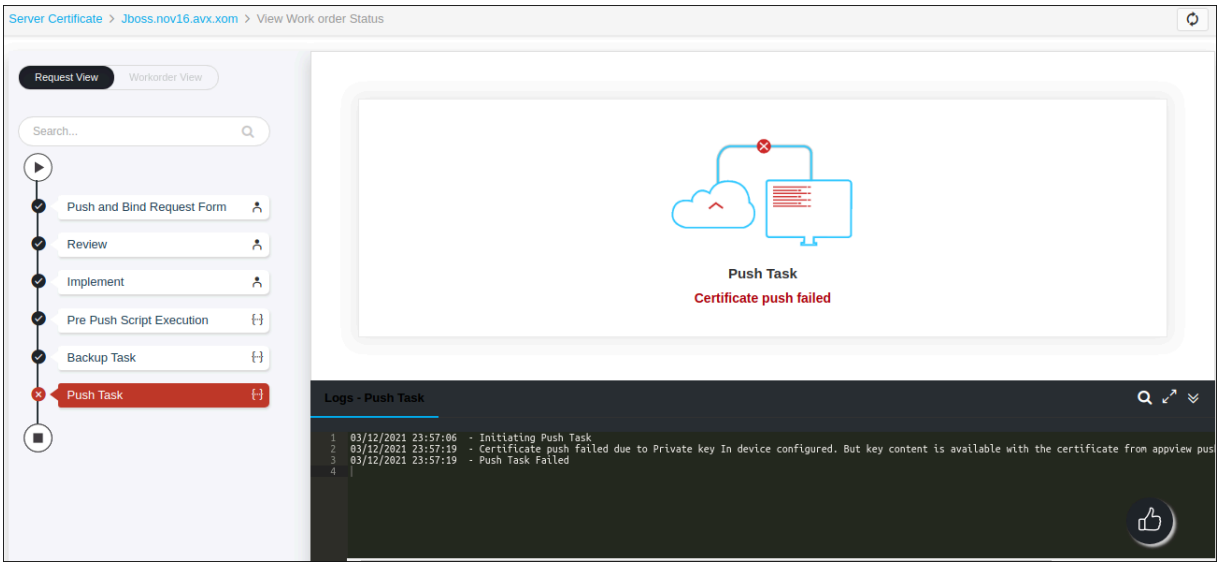


Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is	Push to device after certificate has been retrieved from CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	unavailable, i.e, in a new state.	
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	“Private key in Device” is enabled in application connector and also private key is available in the certificate	Ensure to uncheck “Private key in Device” attribute in application connector
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Windows Weblogic Server

- Overview
- Issues in Device communication
- Issue in Discovery
- Issues in CSR generation at Endpoint
- Issues in Certificate Push

Overview

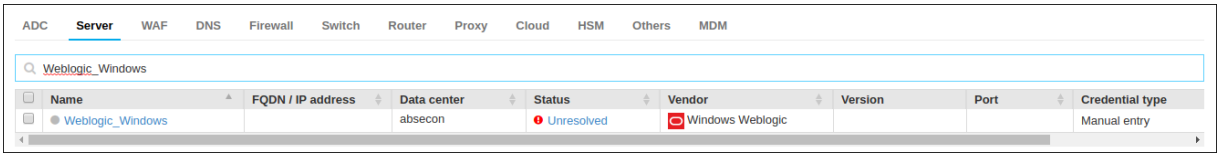
This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Weblogic server.

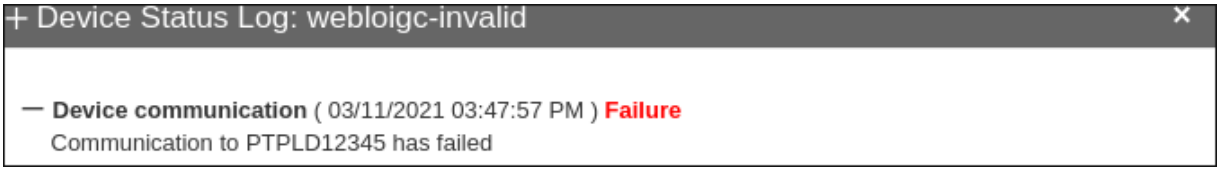
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

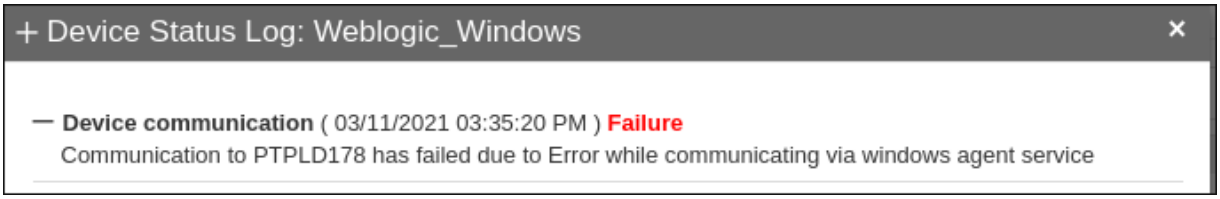
Issues in Device communication

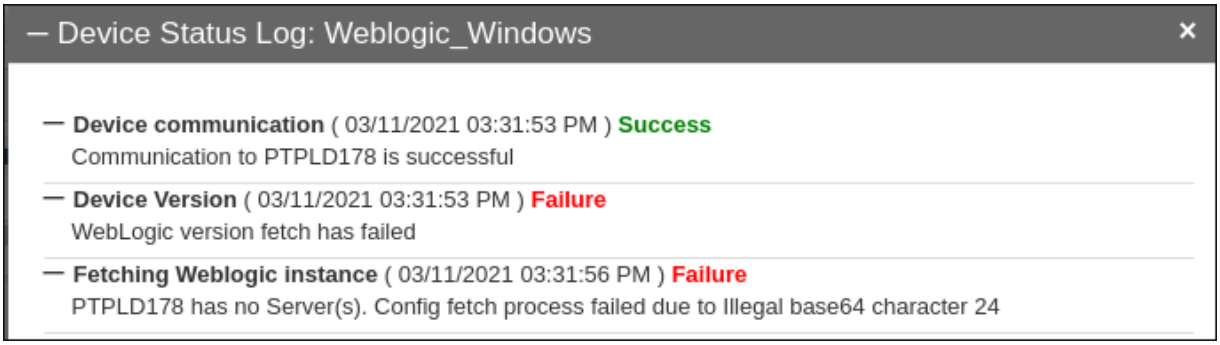
Issues in the Device communication

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration** and click **Device Management**. The **Device Management** page is displayed.
4. On the **Device Management** page, click **Server** Tab.
5. Select the **Windows Weblogic Device**, click **Status**. The **Device Communication Status** is displayed.









Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Messages

Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. Device not reachable 3.Hostname value is incorrect	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable
Error while communicating via windows agent service	Windows agent not reachable	Ensure windows agent is running and it's accessible
Version fetch failed and Fetch weblogic instance failed	Given “Weblogic Installation directory” is in-correct	Check and ensure the given installation path is correct

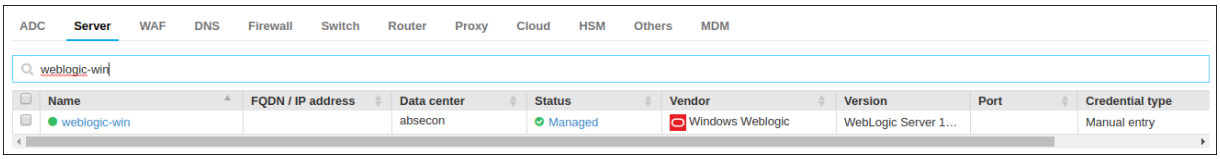
Issue in Discovery

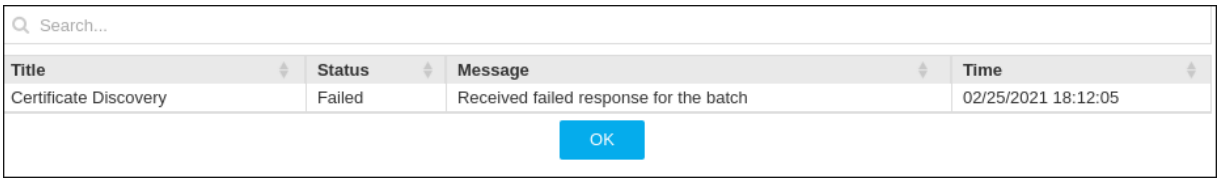
Issue in the Discovery

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Discovery**, select **Discovery**.
4. Click **Managed Devices Scan**.

> **Note:** To discover certificates from Managed devices, the device should be managed under AppViewX Inventory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Messages

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

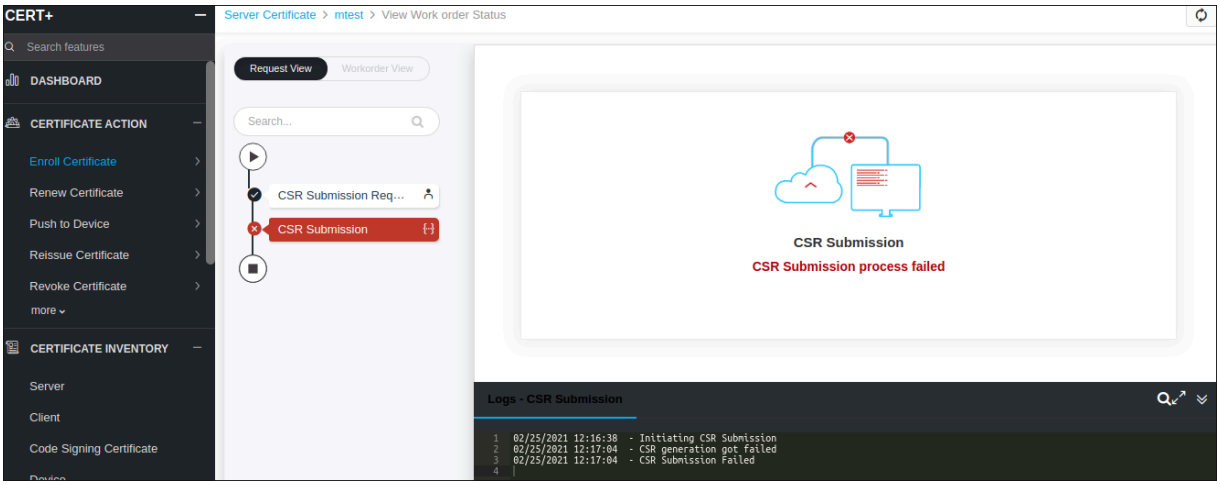
Issues in CSR generation at Endpoint

Issues in the CSR generation at Endpoint

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**. The **Server Certificate** page is displayed.
3. From the left pane, expand **Certificate Action** and select **Enroll Certificate** submenu.
4. Click **Server** Tab. The **Enroll Server Certificate** page is displayed.
5. Click **End Point** as **CSR Generation Source** option.
6. From the dropdown, click correct **Category.**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. From the **Vendor** dropdown, click **Windows Weblogic**. A list of devices will be generated in the **Devices dropdown**.



Error Messages

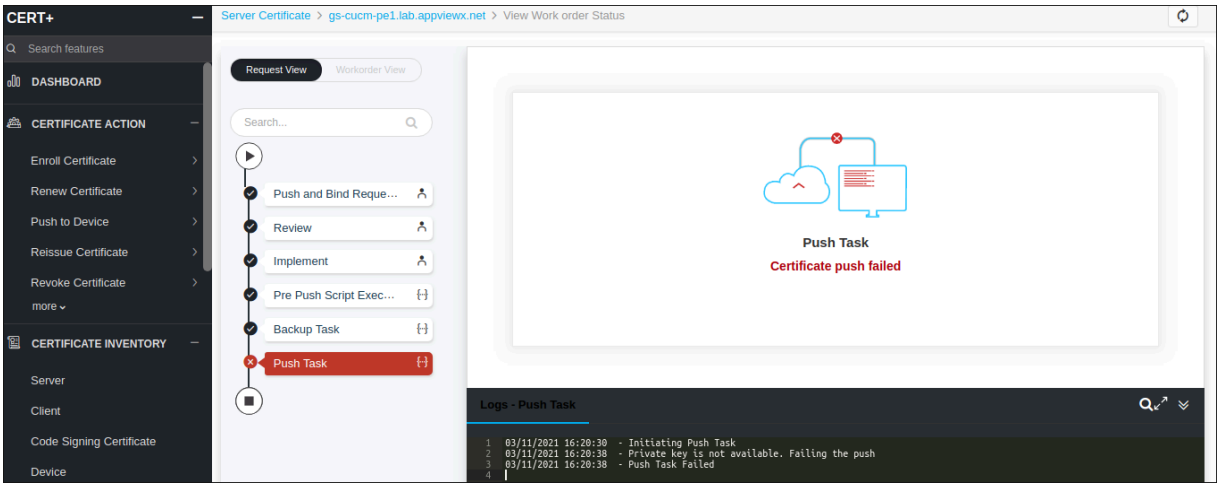
Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1.Kindly ensure the user configured for device addition has read/write access to the path configured.

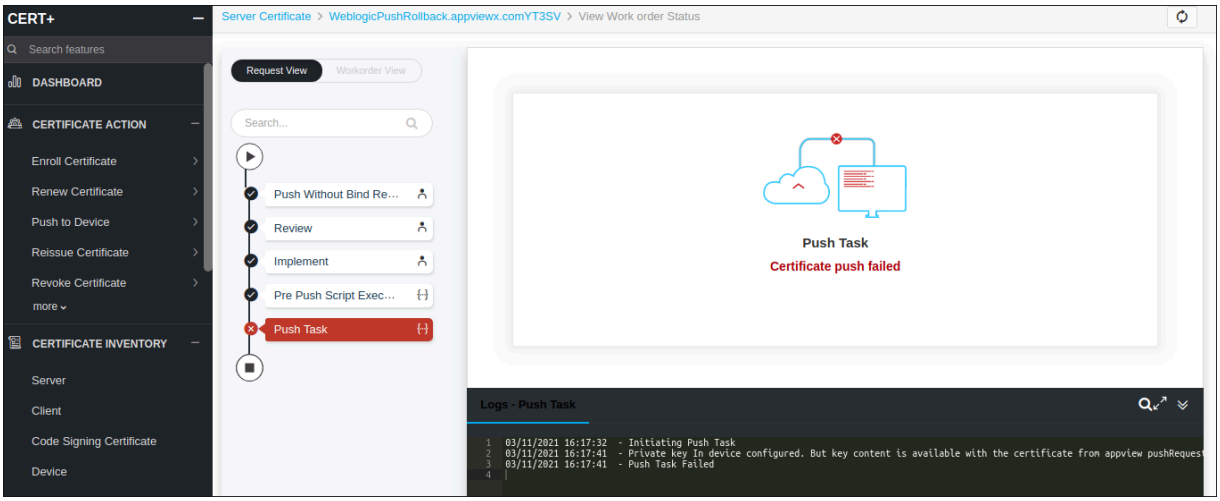
Issues in Certificate Push

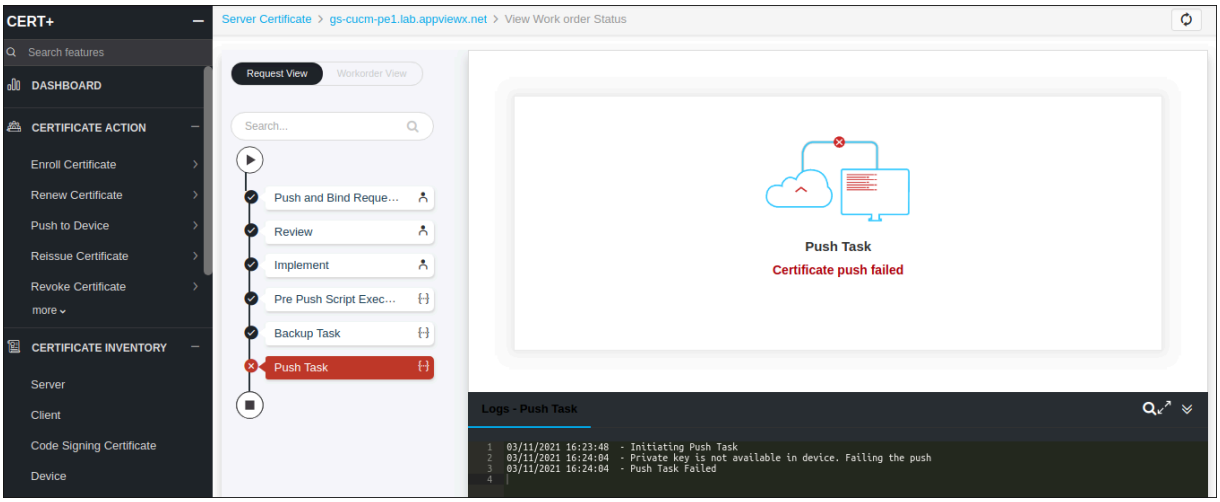
Issues in the Certificate Push

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **Cert+**.
3. From the left pane, expand **Certificate Inventory** and click **Server**. The **Server Certificate** page is displayed.
4. Click any **Windows Weblogic server**. A holistic view of the **Certificate** will be displayed.
5. From the dropdown of **Connector Actions**, select **Add App Connector**.
6. Push the certificate to the device.

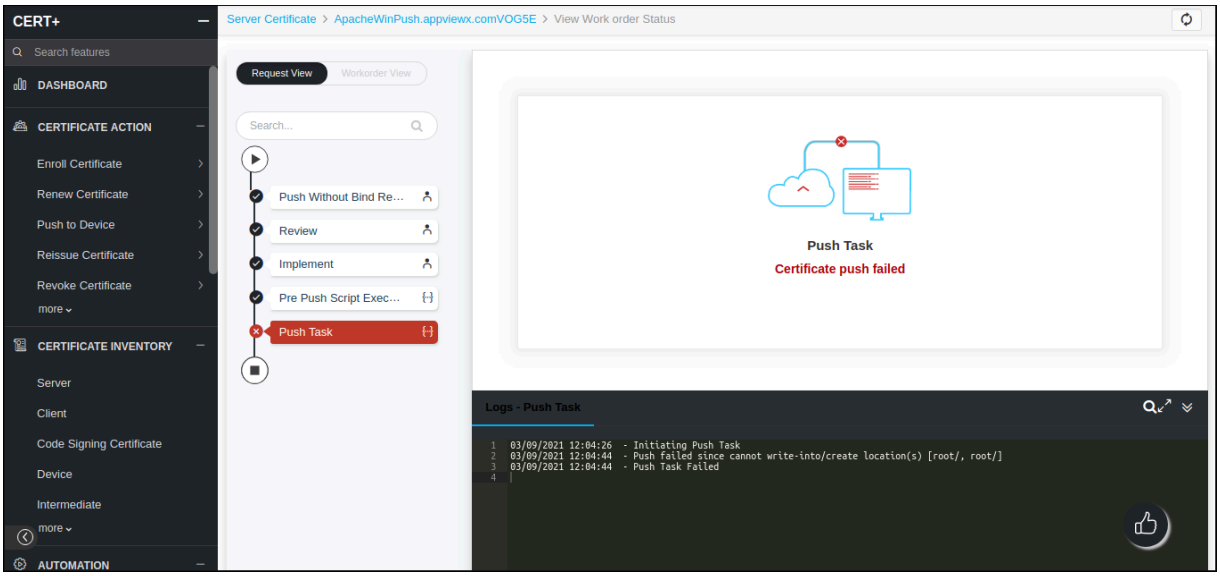
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

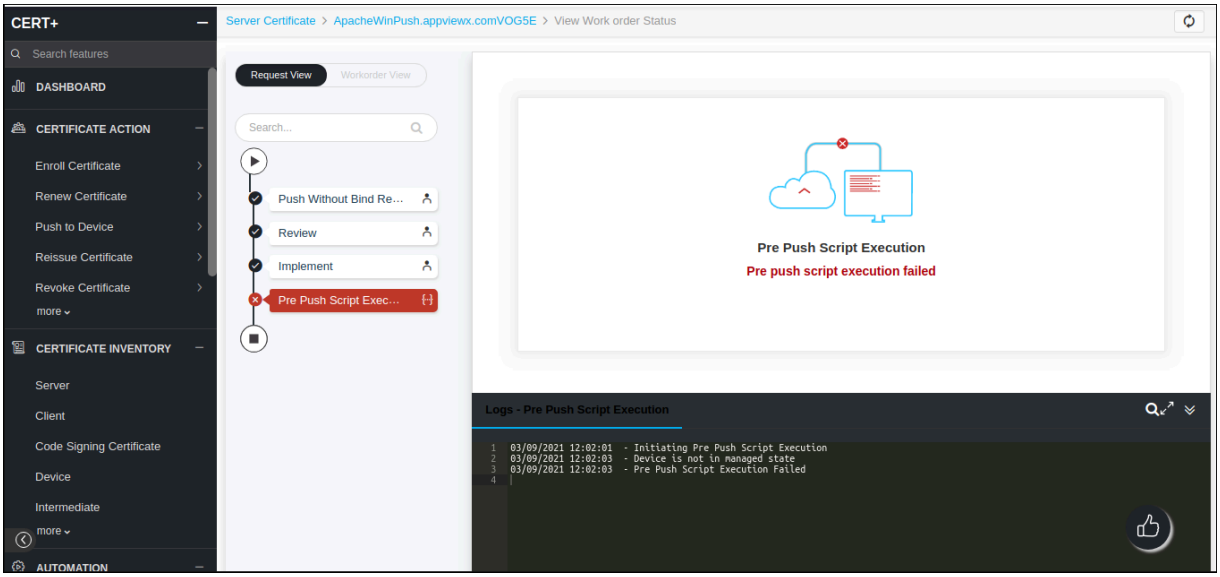






Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Error Mesages

Error Message	Possible Cause	Possible Solution
Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Private key is not available in device. Failing the push	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 7: CERT+ Automation Workflows User Guide

This guide describes AppViewX's predefined Out of the Box (OOB) workflows for CERT+ that will assist you in self-servicing workflows for the certificate expiry notification, certificate enrollment, and certificate renewal. These workflows automate tasks like the intimation of expiry of certificates, generating reports of expiry of orphan certificates, updating certificate attributes, enrolling new certificates based on different input methods (manual, policy based, CSR), renewing and regenerating certificates, pushing certificates to devices, and incident automation with ServiceNow and JIRA.

This guide also talks about the OOB tasks available in the Workflow Studio. These tasks can be used to design workflows for certificate expiry notification, enrolling certificates, and renewing certificates as per your requirements.

• Getting Started
• Certificate Expiry Workflows
• Certificate Enrollment Workflows
• Renew Certificate Workflows
• Automation Workflow Tasks
• Designing a Custom Workflow using OOB Tasks
• Scheduling an OOB workflow
• Customizing an OOB Workflow

Getting Started

• Prerequisites
• Role-Based Access Control
• Accessing CERT+ Automation Workflows
• Accessing CERT Automation Workflow Tasks

Prerequisites

The following table describes the web browser requirements to create and execute workflows as well as tasks.

Web Browser Requirement

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	V74.0.1 (64-bit) or later
Google Chrome	V85.0.4183.83 (64-bit) or later

Role-Based Access Control

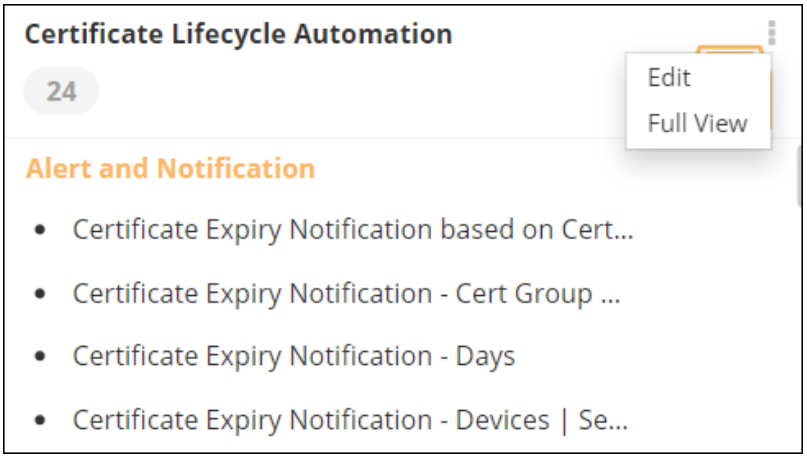
With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to this link and find out more about RBAC.

Accessing CERT+ Automation Workflows

You can access the CERT+ Automation workflows, available on the **Request :: View/Run** page, in the following ways:

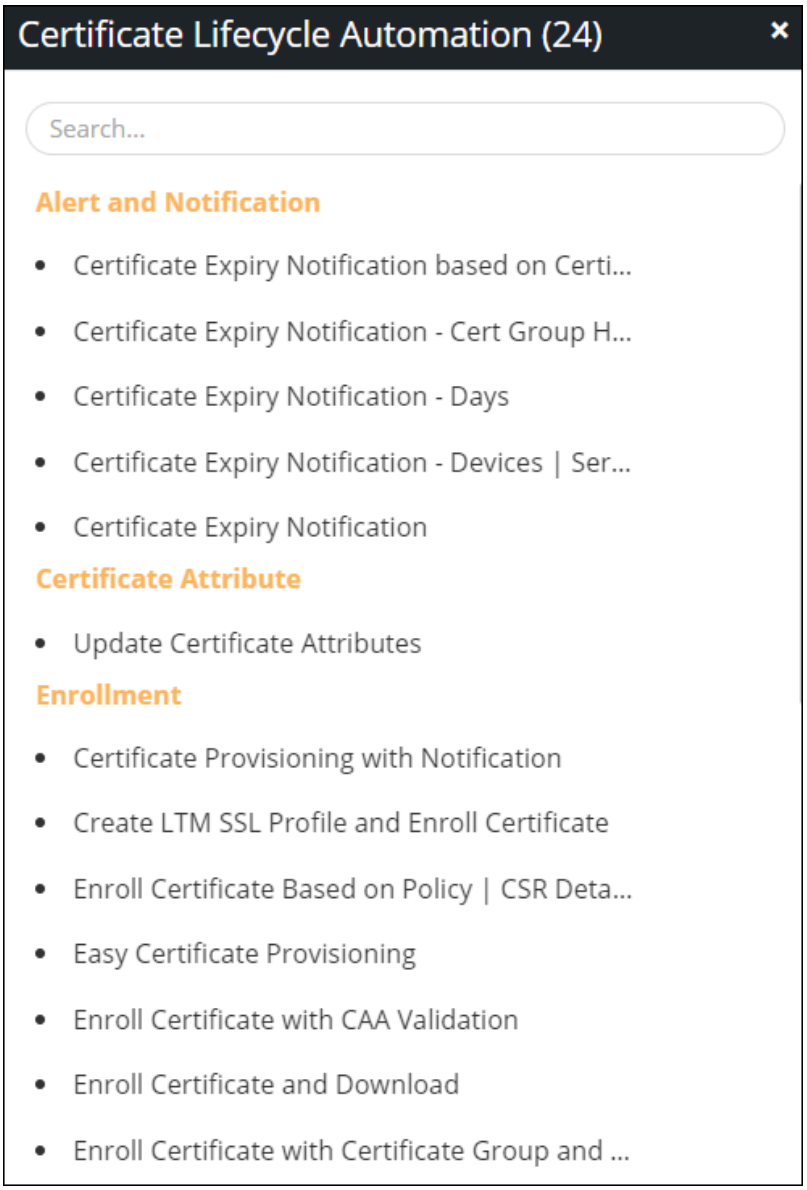
- In the **CERT+** module, navigate to **AUTOMATION** > **My Workflows** > **View/Run**
- In the **Automation** module, navigate to **SERVICE REQUESTS** > **View/Run**

1. On the **Request :: View/Run** page, from the top right corner of the **Certificate Lifecycle Automation** catalog, click .
2. From the options displayed, select **Full View**.



The CERT+ Automation workflows are displayed in the **Certificate Lifecycle Automation** window.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Tip: You can also search for a workflow on the **Catalog** page by typing the keyword(s) in the search bar.

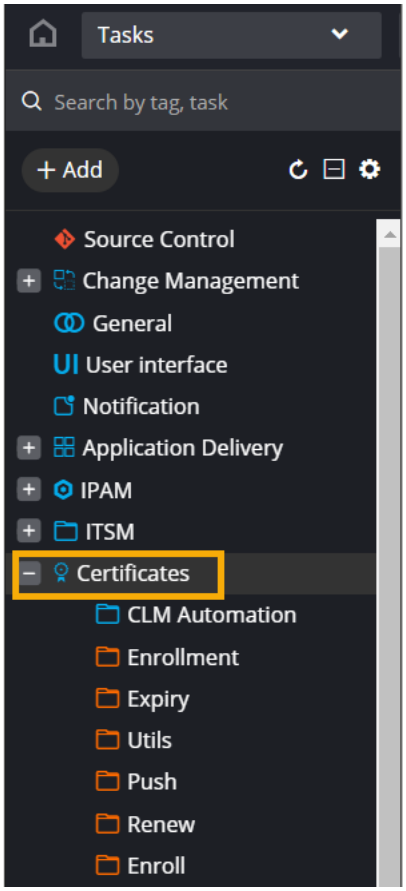
Accessing CERT Automation Workflow Tasks

The CERT+ Automation workflow tasks enable you to design your own custom workflows. These are available in the **Automation** module.

To view these tasks:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. In the **Automation** module, navigate to the **Workflow** page and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.
3. To access the OOB workflow tasks, from the left menu, expand **Certificates**.



The following categories of tasks are available in this folder:

- Enrollment - Lists all the OOB tasks for enrolling certificates from configured CAs.
- Expiry - Lists the Get Expiry Certificates task.
- Renew - Lists the Renew and Regenerate tasks.
- Push - Lists all the OOB tasks for pushing certificates to devices and servers.

Note: For more information on how to design a custom workflow using these OOB tasks, click here.

Certificate Expiry Workflows

- Overview
- Certificate Expiry Notification based on Certificate Attributes

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

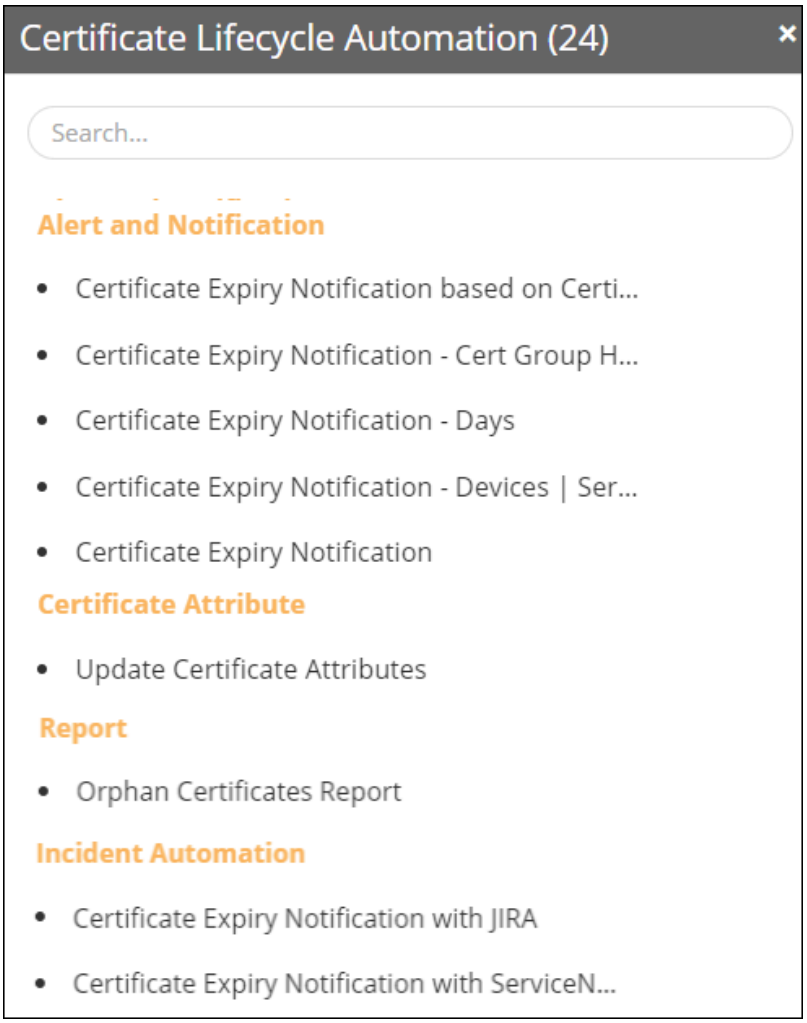
- Certificate Expiry Notification - Cert Group Hierarchy
- Certificate Expiry Notification - Days
- Certificate Expiry Notification - Devices | Servers
- Certificate Expiry Notification
- Update Certificate Attributes
- Certificate Expiry Notification with JIRA
- Certificate Expiry Notification with ServiceNow
- Orphan Certificates Report

Overview

This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. Some workflows also allow you to create tickets for expiring certificates on Jira/ServiceNow, update certificate attributes, and generate an orphan certificates report.

These workflows are available in the **Certificate Lifecycle Automation** catalog under four categories.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



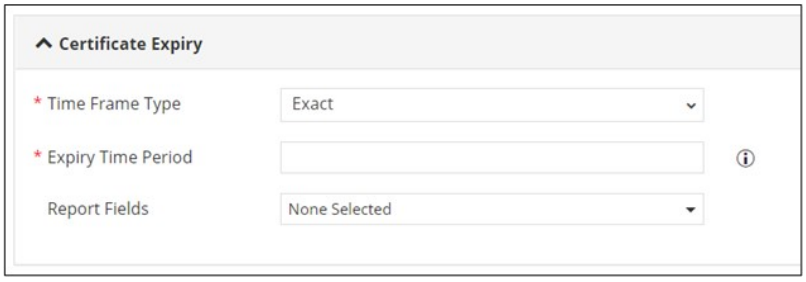
Certificate Expiry Notification based on Certificate Attributes

This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification based on Certificate Attributes** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

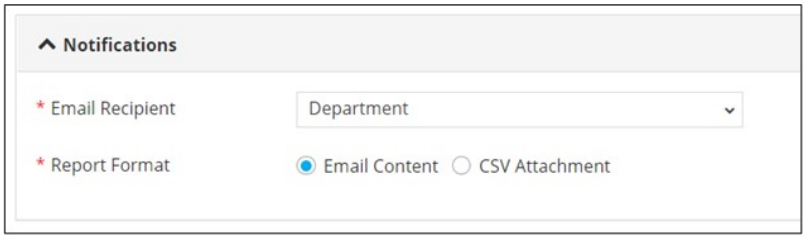


Field Description for Certificate Expiry section:

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description in Notifications section:

Field	Description
***Email Recipient**	Select the email recipient from the dropdown list.
***Report Format**	Select the required checkbox to send the report as: • **Email content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and an email notification listing the certificates expiring in specific number of days with selected certificate attribute details is sent to the recipient email address(es) entered in the input form.

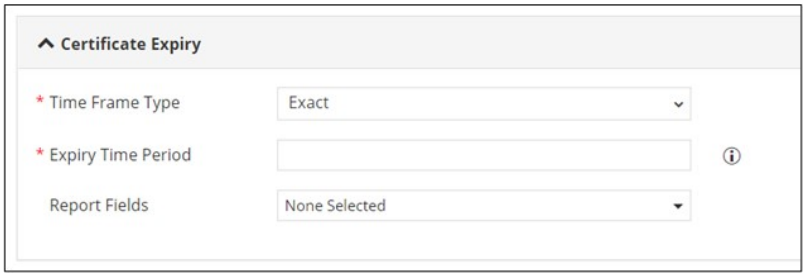
Certificate Expiry Notification - Cert Group Hierarchy

This workflow allows you to send a certificate expiry report notification to the certificate group and its associated hierarchical groups.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Cert Group Hierarchy** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

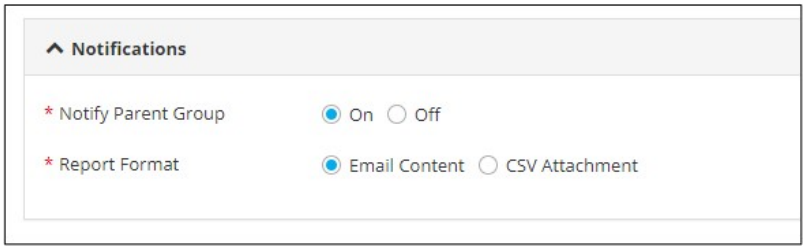


Field Description for Certificate Expiry section.

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Notifications section.

Field	Description
***Notify Parent Group**	Select: • **On** to send the notification to the certificate group's parent group. • **Off** if you don't want to send the notification to the certificate group's parent group. **Note: On** is the default selection.
***Report Format**	Select the required option to send the report as: • **Email content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   Workflow is executed successfully and a certificate expiry report notification is sent to certificate group and associated parent group(s).

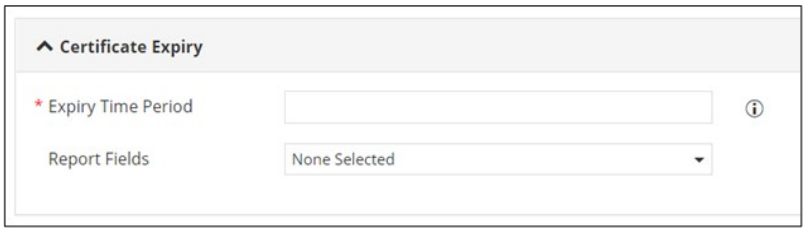
Certificate Expiry Notification - Days

This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.

To trigger this workflow:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

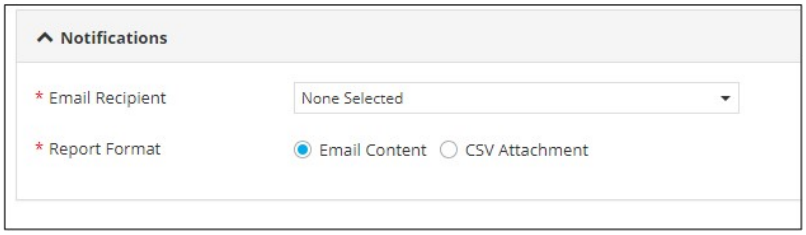
1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Days** workflow and click  .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.



Field Description for Certificate Expiry section.

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Notifications section.

Field	Description
***Email Recipient**	Select the required recipient of the notification. You can select: • **Select all** • **Certificate Email**: The notification will be sent to the email addresses associated with the certificate. • **Certificate Group Email**: The notification will be sent to the entire certificate group to which the certificate belongs.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and an email notification with a report listing certificates expiring in time period as specified in the input form is sent to the recipient email address(es).

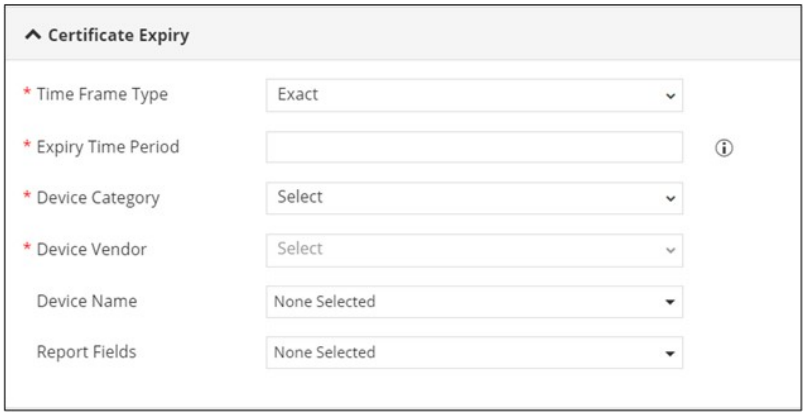
Certificate Expiry Notification - Devices | Servers

This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Devices | Servers** workflow and click  .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



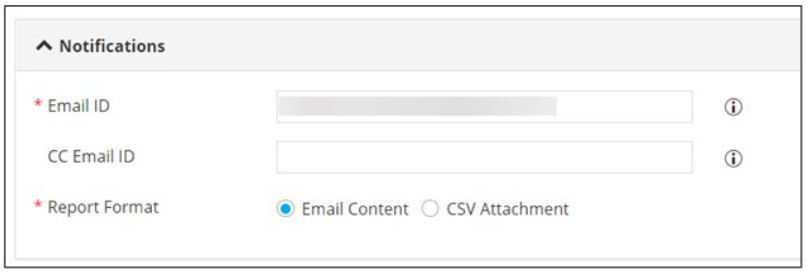
Field Description for Certificate Expiry section.

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the Expiry Time Period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in Expiry Time Period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day. **Note: Exact** is the default selection.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
***Device Category**	Select the device category for the report from the dropdown list.
***Device Vendor**	Select the device vendor for the report from the dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Device Name	Select the specific device for the report.
Report Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.



Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.

   The workflow is executed successfully and an email notification with the list of devices and certificates present on that device expiring in a specific number of days is sent.

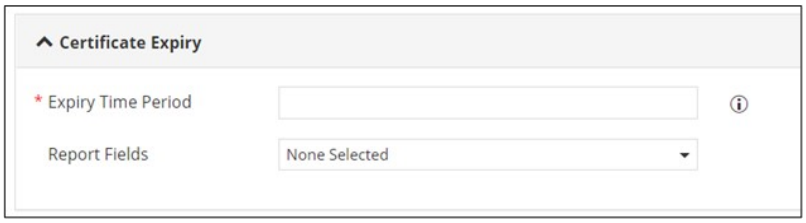
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate Expiry Notification

This workflow enables you to generate a report listing certificates expiring in a specific number of days and notify the recipients via email. You can also mention email addresses of the recipients who need to be informed additionally in CC mails.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification** workflow and click  .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

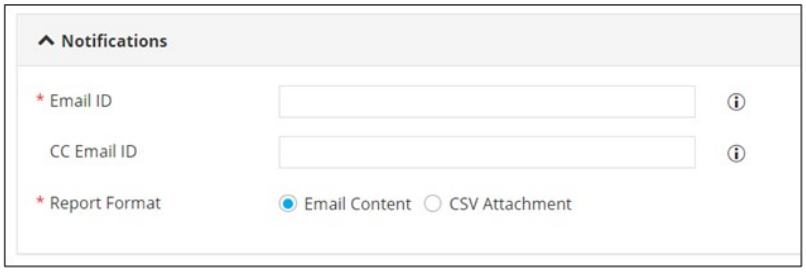


Field Description for Certificate Expiry section.

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma-separated values can be entered for multiple email addresses.
CC Email ID	Enter the email address of the additional recipients in the 'CC' field. Comma-separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and email notification listing certificates expiring in a specific number of days is sent to the email address(s) configured in the workflow input form.

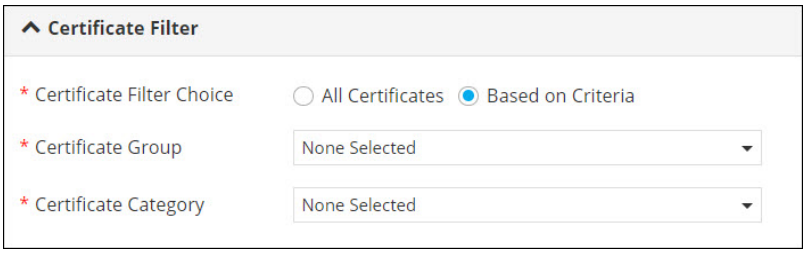
Update Certificate Attributes

This workflow allows you to update the certificate attributes in bulk.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Update Certificate Attributes** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Filter** section, enter or select the requested field information as described in the table below.

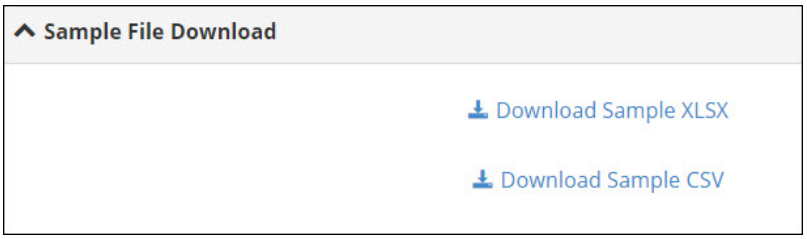
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Certificate Filter section.

Field	Description
***Certificate Filter Choice**	Select the required checkbox to fetch: • **All certificates**: This is the default selection and will fetch all the certificates. • **Based on Criteria**: Select this option to fetch certificates based on criteria such as certificate group and certificate category.
***Certificate Group**	Select the appropriate certificate group from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
***Certificate Category**	Select the appropriate certificate category from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
All asterisk (*) marked fields are mandatory.	

3. Click **Submit**.
   Certificates are fetched based on the selection criteria.
4. In the **Update Certificate Attribute Input** stage of workflow execution, select the option for downloading the file as a CSV or Excel file.



The file is downloaded to your device. You can now update the certificate attributes in this file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Once you have updated the certificate attributes, under **File Upload**, click to upload the modified file.



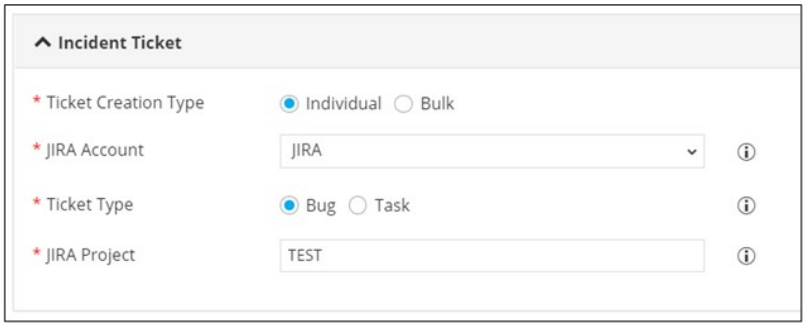
6. Click **Next** and in the **Confirmation** pop-up window, click **Ok**.
   The **Update Certificate Status** stage of the workflow displays the list of updated certificates. To download this list, from the top right corner of the screen, click . An email report is also sent to the requester.

Certificate Expiry Notification with JIRA

This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with JIRA** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Incident Ticket** section, select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Incident Ticket section.

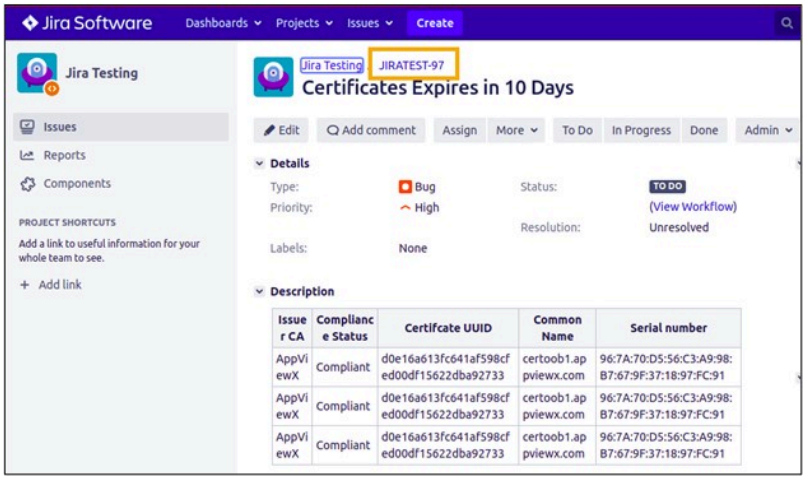
Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual**: A separate ticket will be created for each certificate. • **Bulk**: A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High. **Note: Individual** is the default selection.
***JIRA Account**	Select the **JIRA Account** as configured in the Integration Hub from the options available in the dropdown. **Note: JIRA** is the default selection.
***Ticket Type**	Select the type of ticket with reference to the project: • **Bug**: This will indicate that the ticket is for a bug in the project. • **Task**: This will indicate that the ticket is for a task in the project. **Note: Bug** is the default selection.
***JIRA Project**	Enter the name of the project for which ticket(s) have to be raised. **Note: Test** is the default selection.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
4. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
5. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
6. Under the **Description Fields** section, select certificate attributes from the dropdown that will be displayed in the JIRA issue description.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

7. Click **Submit**.
   The **Ticket Creation Summary** stage of workflow execution displays the JIRA ticket ID and the ticket for Certificate expiry notification is created on JIRA.

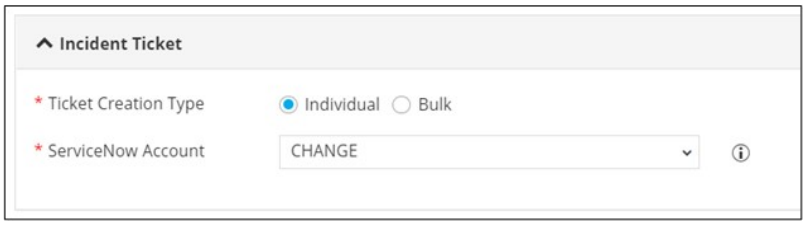


Certificate Expiry Notification with ServiceNow

This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with ServiceNow** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Incident Ticket** section, select the field requested information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for Incident Ticket section.

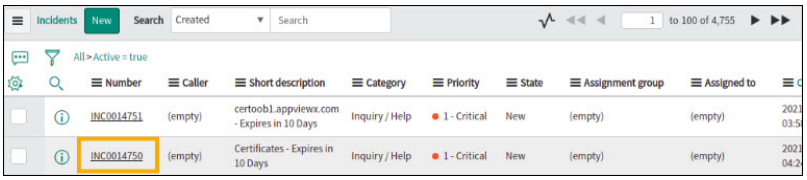
Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual**: A separate ticket will be created for each certificate. • **Bulk**: A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High. **Note: Individual** is the default selection.
***ServiceNow Account**	Select the **ServiceNow Account** as configured in the Integration Hub from the options available in the dropdown. **Note: Change** is the default selection.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
4. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
5. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
6. Under the **Description Details** section, select multiple certificate attributes from the dropdown that will be displayed in the ServiceNow description.

   Note: This is a mandatory field.

7. Click **Submit**.

   The **Ticket Creation Summary** stage of workflow execution displays the ServiceNow ticket ID and the ticket for Certificate expiry notification is created on ServiceNow.



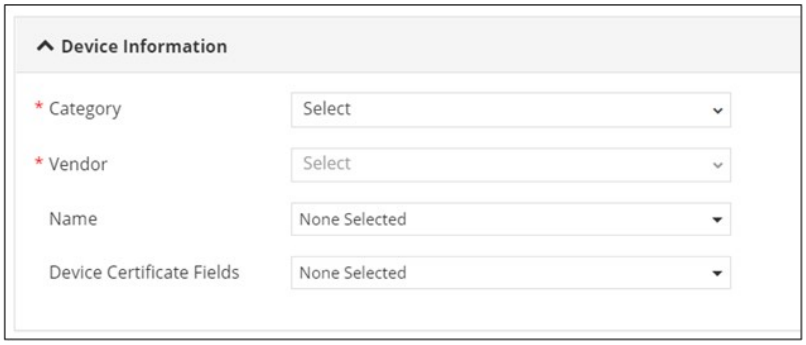
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Orphan Certificates Report

This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Report** category, hover your mouse over the **Orphan Certificates Report** workflow and click  .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Device Information** section, enter or select the requested field information as described in the table below.



Field Description for Device Information section.

Field	Description
***Category**	Select the device category for the report from the options available in the dropdown.
***Vendor**	Select the device vendor for the report from the options available in the dropdown.
Name	Select the specific device for the report.
Device Certificate Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**:The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The **Orphan Certificates List** is generated and an email notification is sent to the recipients specified in the input form.

Certificate Enrollment Workflows

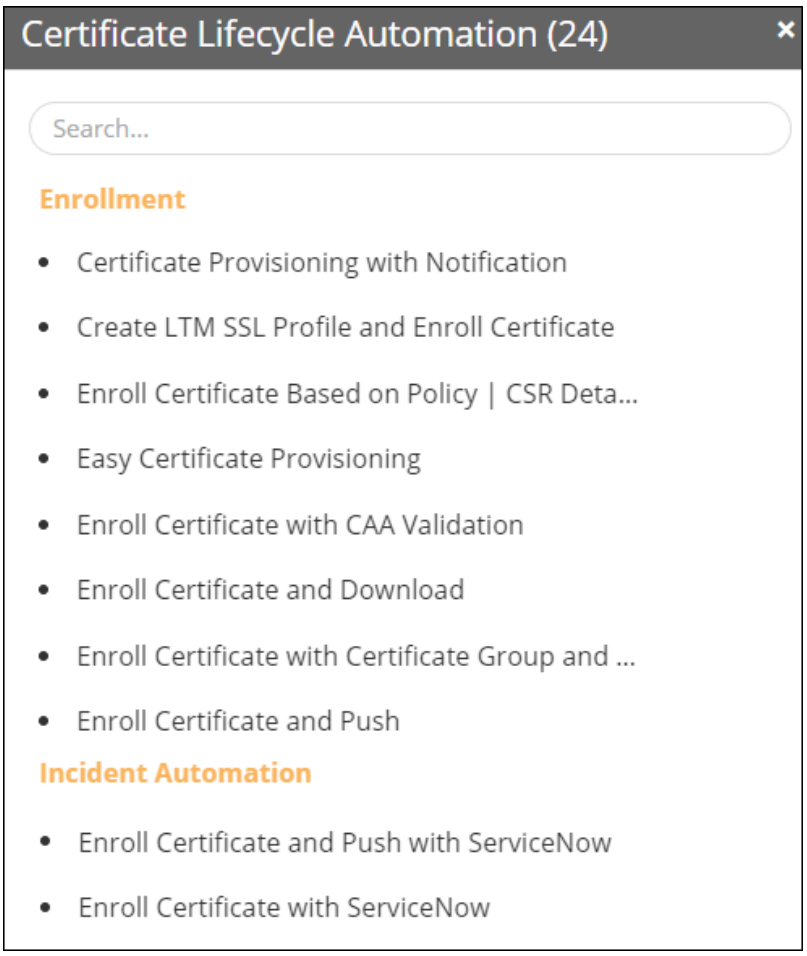
- Overview
- Enroll Certificate and Download
- Certificate Provisioning with Notification
- Enroll Certificate Based on Policy | CSR Details | CSR Upload
- Create LTM SSL Profile and Enroll Certificate
- Enroll Certificate with Certificate Group and CSR Upload

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Enroll Certificate With ServiceNow
- Enroll Certificate and Push with ServiceNow
- Easy Certificate Provisioning
- Enroll Certificate with CAA Validation
- Enroll Certificate and Push

Overview

This section lists and describes the workflows that can be used to enroll certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Enrollment with Incident Automation. These workflows are available in the **Certificate Lifecycle Automation** catalog under the **Enrollment** and **Incident Automation** categories.



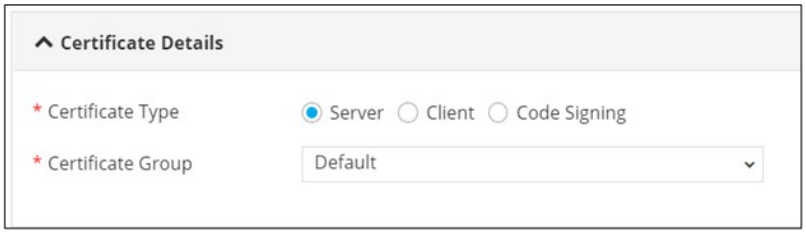
Enroll Certificate and Download

This workflow enables you to create and download certificates based on the certificate group.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

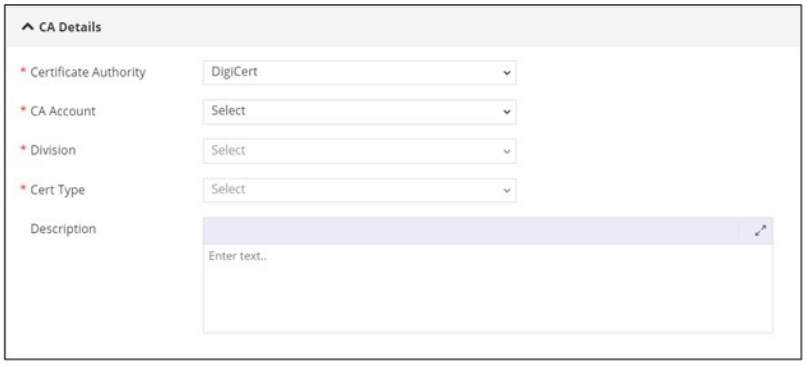
1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Download** workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.



Field description for Certificate Details section

Field	Description
***Certificate Type**	Select the required **Certificate Type** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.



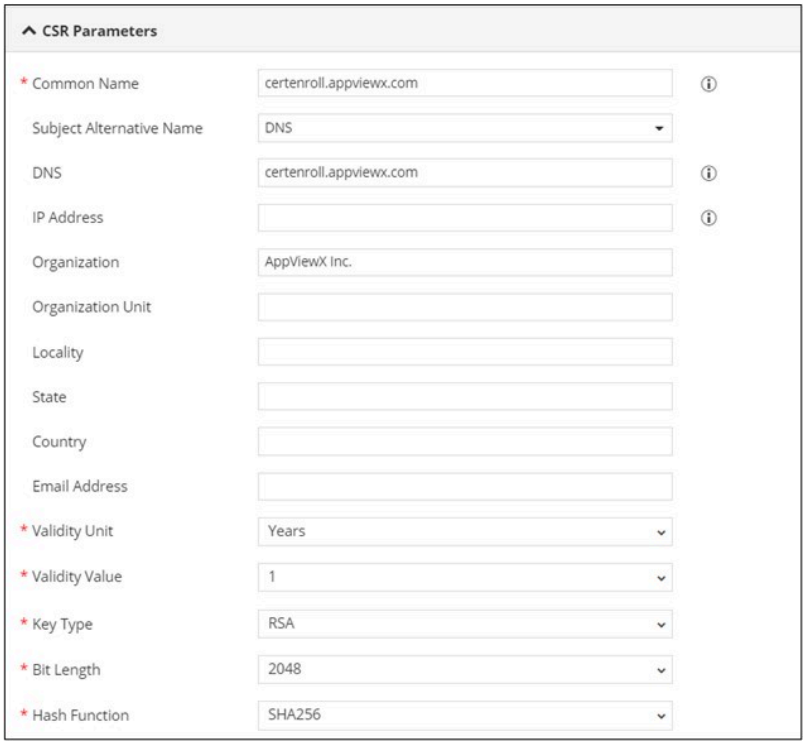
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note**: This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



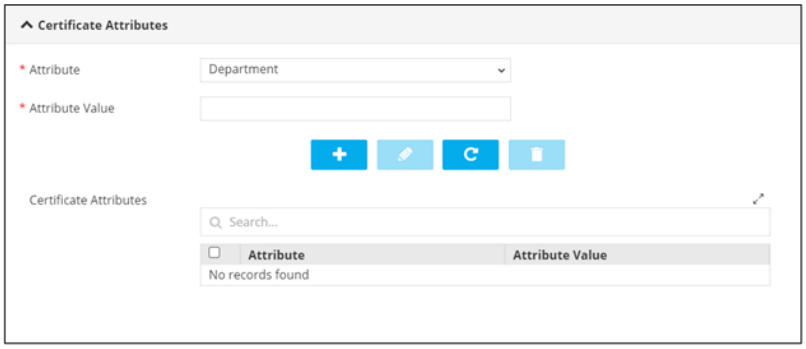
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS, if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP address, if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed in this section will vary based on the CA selected.

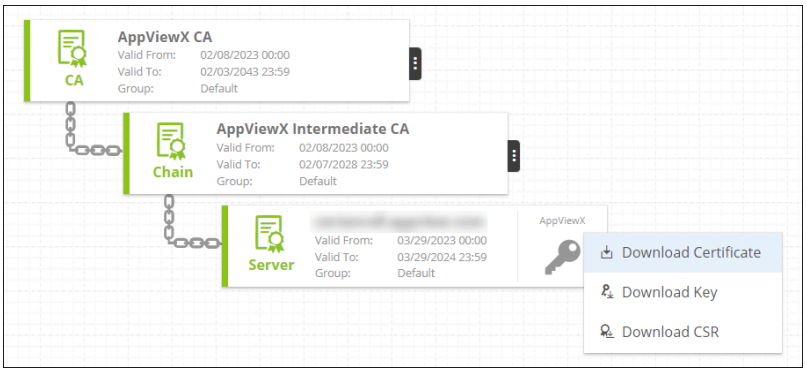
8. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** This field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

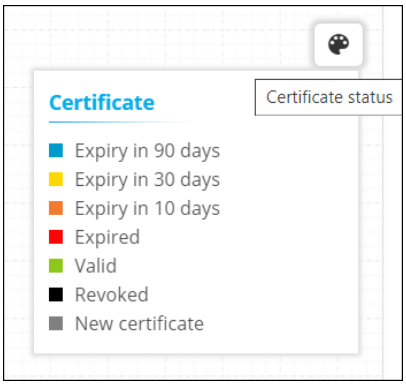
9. Click **Submit**.
   The certificate is created successfully and an email notification is sent to the recipient specified in the input form.

10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



11. Hover your mouse over to view the Certificate status.



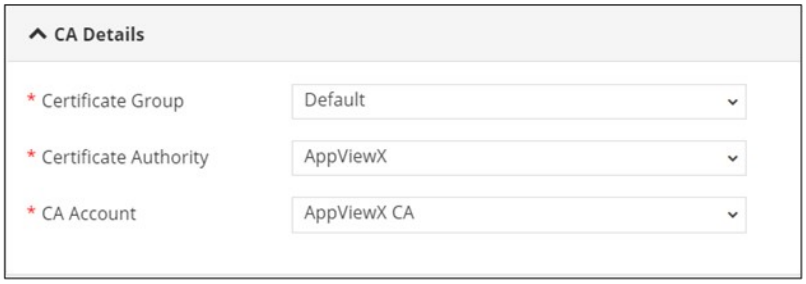
Certificate Provisioning with Notification

This workflow allows you to create a certificate based on the certificate group and the policy associated with it, and push to a device available in the instance. Email approval is required for certificate creation as well as pushing it to the device. Once approved, the logged in user will receive an email informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Certificate Provisioning with Notification** workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field description for CA Details section

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Ebtrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the selected **Certificate Group**.
CA Account	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **CA**selected .
All asterisk (*) marked fields are mandatory.	

3. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

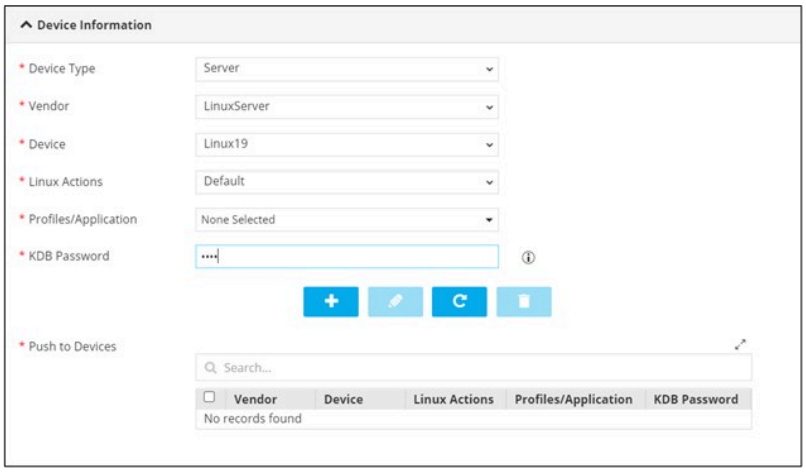


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Type	Select the Subject Alternative Type from the available options: • DNS • IP Address
Subject Alternative Name	Enter a valid Subject Alternative Name.
All Asterisk (*) marked fields are mandatory.	

4. Under the **Device Information** section, enter or select the requested field information as described in the table below.



Field description for Device Information section

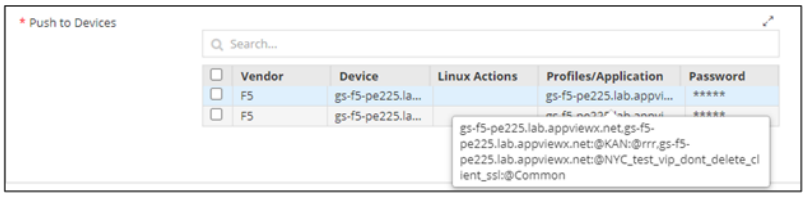
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click  .
   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Under the **Email** section, enter the field information as described in the table below.

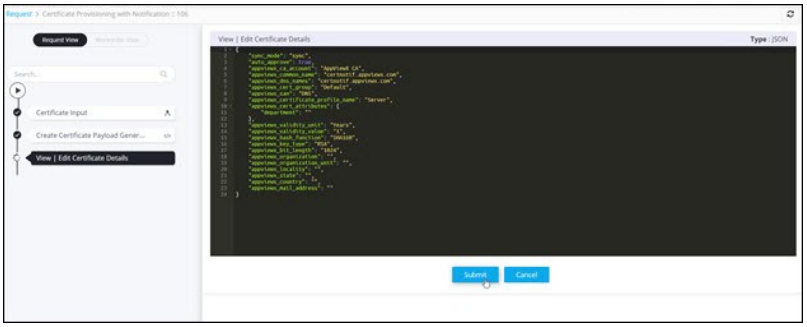
Field description for Email section

Field	Description
***Certificate Approver Email ID**	Enter the email address or multiple addresses, separated by comma, of the user(s) approving the certificate creation request.
***Certificate Push Approver Email ID**	Enter the email address of the user who will approve the certificate push request.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

   The workflow is executed successfully.

8. At the **View | Edit Certificate Details** stage, click **Submit**.



   Email notification for Create Certificate approval is received.

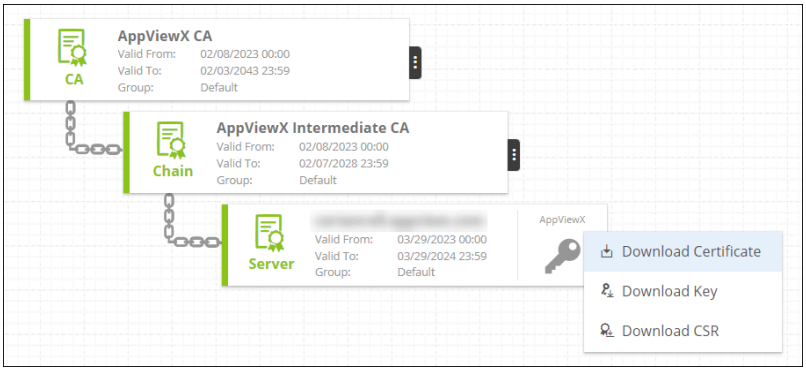
9. Click **Approve** or **Reject** in the **Approval for Creating Certificate** email.



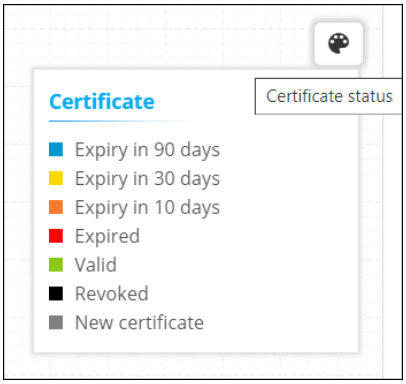
   Certificate is created after the approver clicks **Approve**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  , and from the options displayed, click **Download Certificate**.



11. Hover your mouse over  to view the Certificate status.



12. Click **Approve** or **Reject** in the **Approval for Pushing Certificate to Device** email.



Once the approver approves the request, the certificate is pushed to the selected device and an email notification is also sent to the requester.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

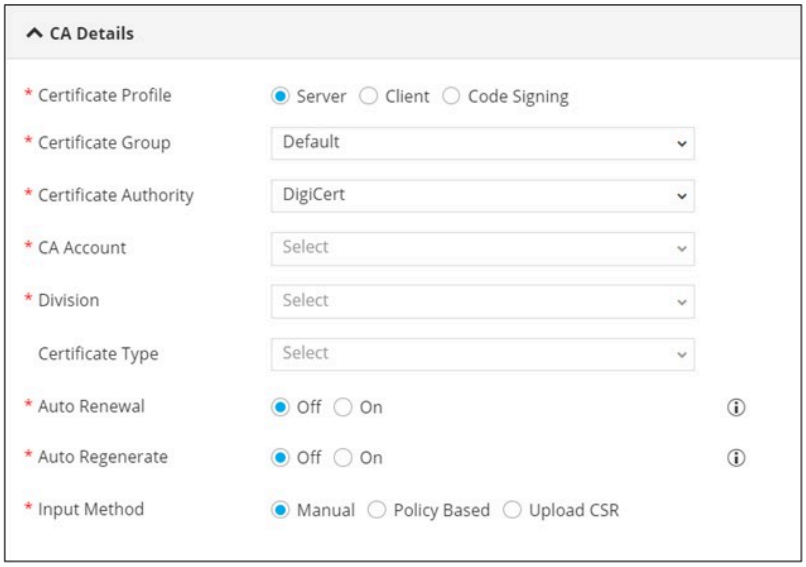
Enroll Certificate Based on Policy | CSR Details | CSR Upload

This workflow allows you to create a certificate using three input methods - Manual, Policy Based, and Upload CSR.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate Based on Policy | CSR Details | CSR Upload** workflow and click .

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.



Field description for CA Details section

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. • **Policy Based**: If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR**: If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters. **Note: Manual** is the default selection.
All Asterisk (*) marked fields are mandatory.	

What to do next:

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

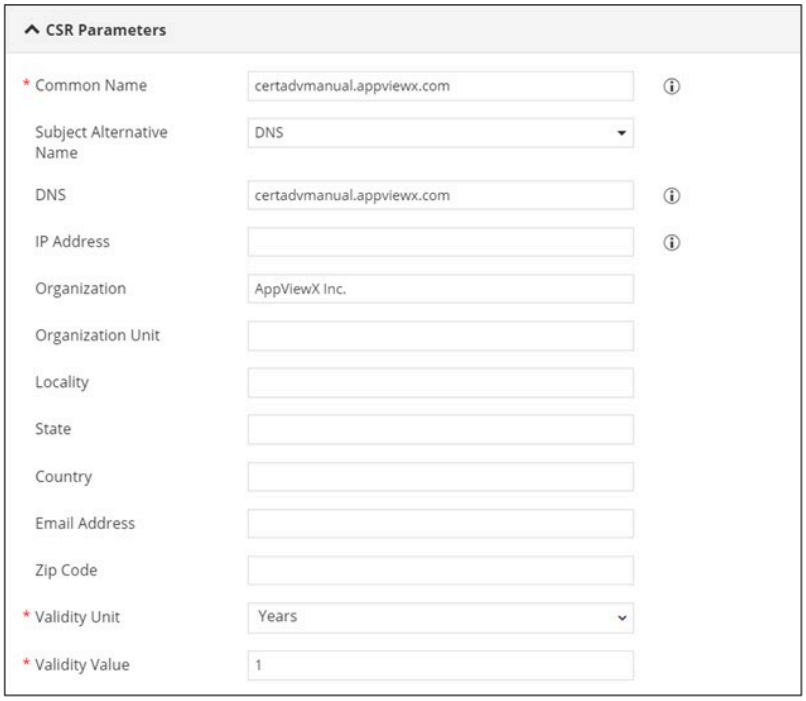
- Manual
- Policy Based
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.





Field description for CSR Parameters section

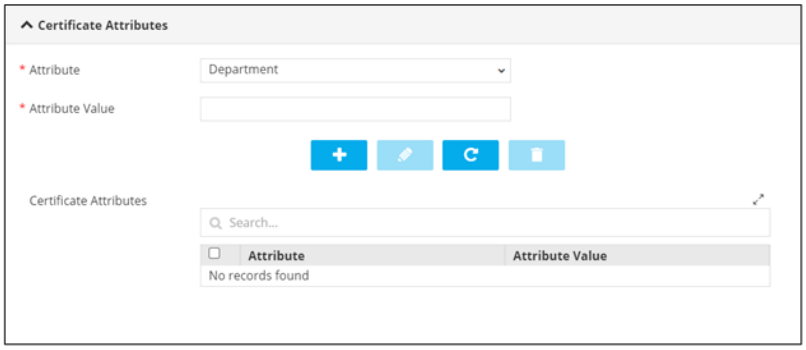
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.  **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

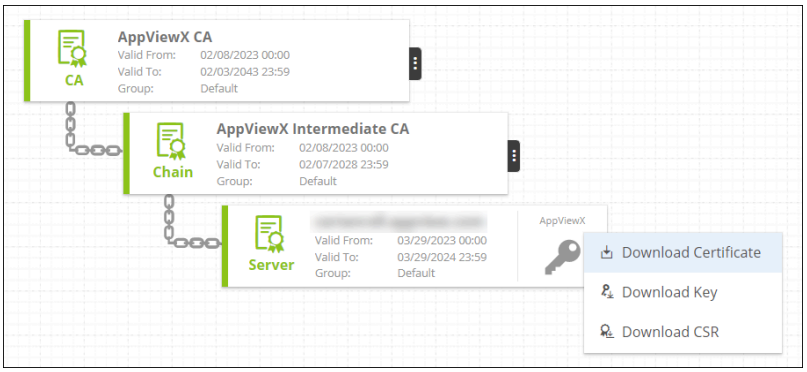
Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

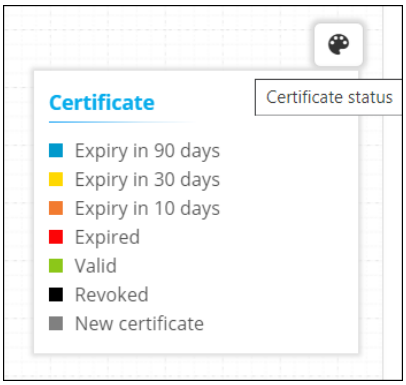
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

6. Click **Submit**.
   AppViewX certificate is created successfully and an email notification is sent to the recipient specified in the input form.
7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



8. Hover your mouse over  to view the **Certificate status**.



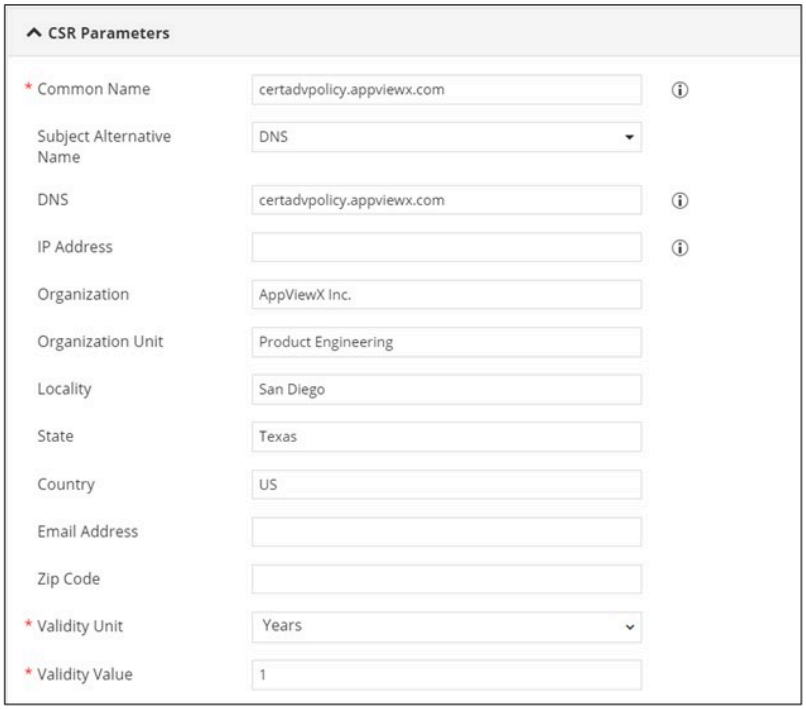
Policy Based

After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

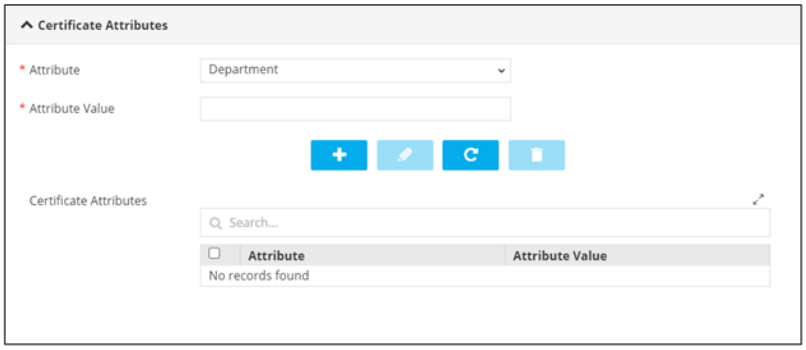




Note: For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

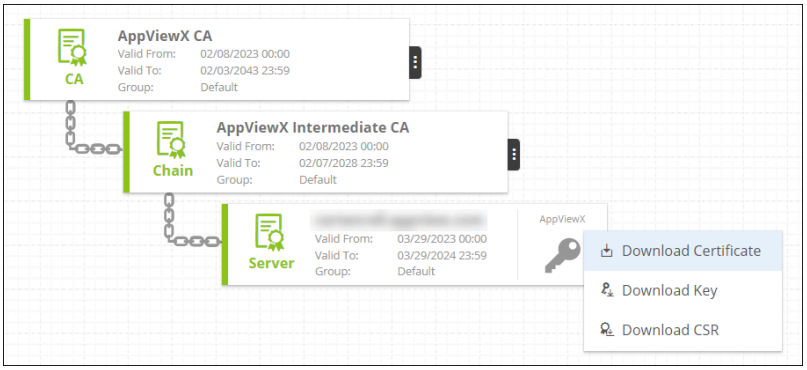
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

6. Click **Submit**.

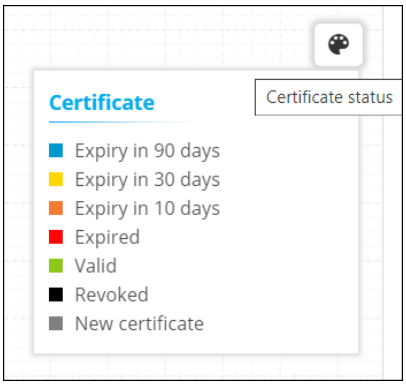
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX certificate is created successfully and email notification is sent to the recipient specified in the input form.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



8. Hover your mouse over  to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click  .

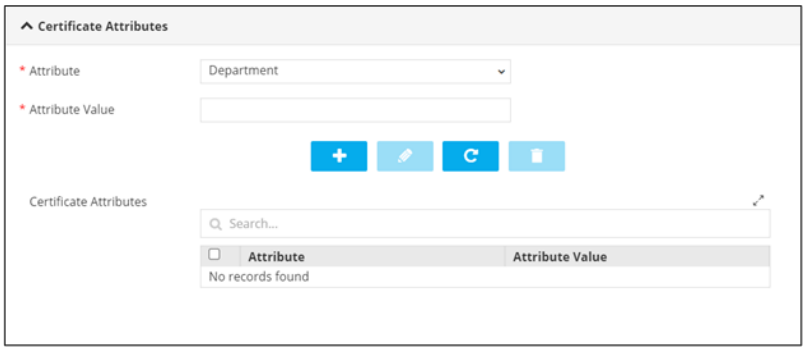


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.
✎	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click ✎, enter the new value for the attribute, and click ✎ again.
🗑	Allows you to delete a certificate attribute.
⤢	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

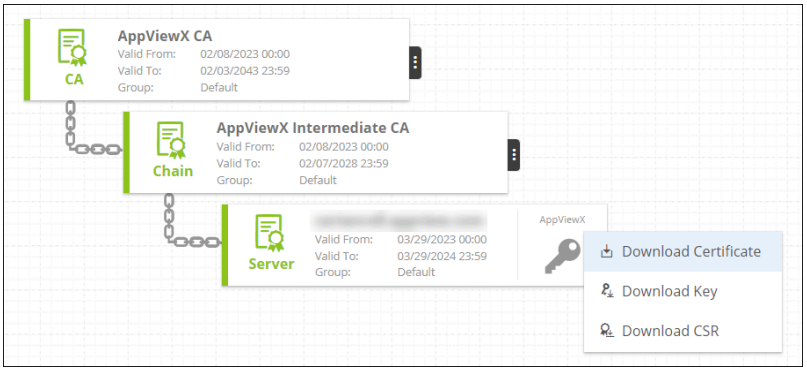
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

6. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

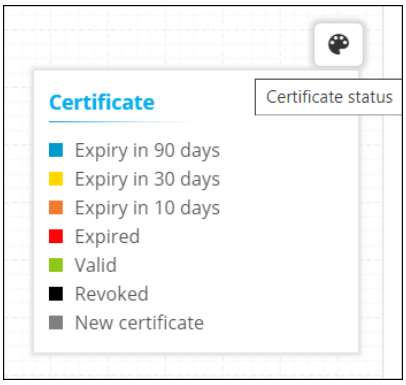
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.
   AppViewX certificate is created successfully and email notification is sent to the recipient specified in the input form.

8. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



9. Hover your mouse over  to view the **Certificate status**.



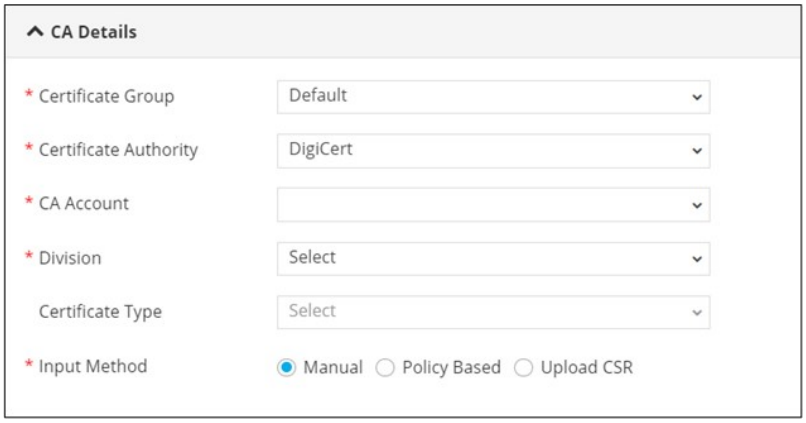
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Create LTM SSL Profile and Enroll Certificate

This workflow allows you to create individual server certificates along with LTM SSL profile creation based on the selected certificate group.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Create LTM SSL Profile and Enroll Certificate**workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.



Field descriptions in the CA Details section

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** The **Certificate Authority** field is populated based on the selected **Certificate Group**.
***CA Account**	Select the **CA Account** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The **CA Account** field is populated based on the selected **Certificate Authority**.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: If you select the **Input Method** as Manual, the CSR parameters will have to be entered/selected manually. • **Policy Based**: If you select the **Input Method** as Policy Based, the CSR parameters fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR**: If you select the **Input Method** as Upload CSR, you can upload the CSR file to fetch the CSR parameters. **Note: Manual** is the default **Input Method**.
All asterisk (*) marked fields are mandatory.	

What to do next:

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

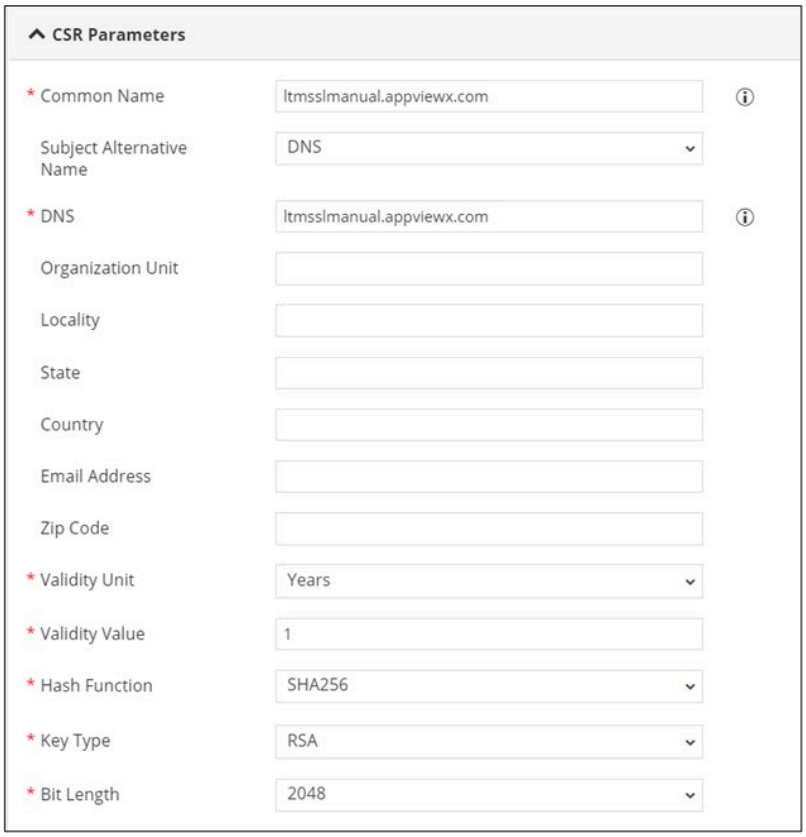
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Manual
- Policy Based
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.



Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**

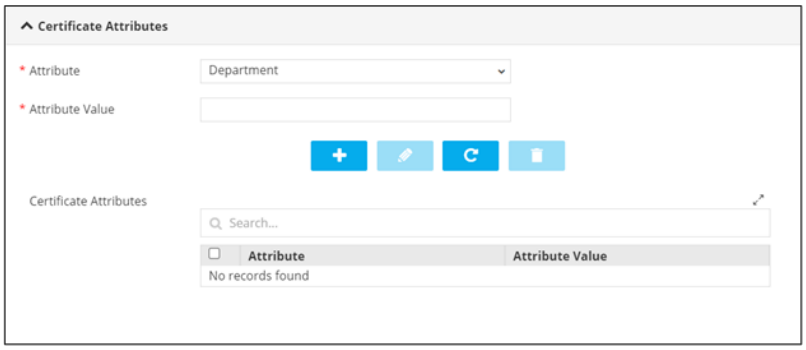
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field. **Note:** This field is displayed if DNS is selected in the **The email id of the logged in user is populated automatically.** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field. **Note:** This field is displayed if IP Address is selected in the **Subject Alternative Name** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter the email address(es).

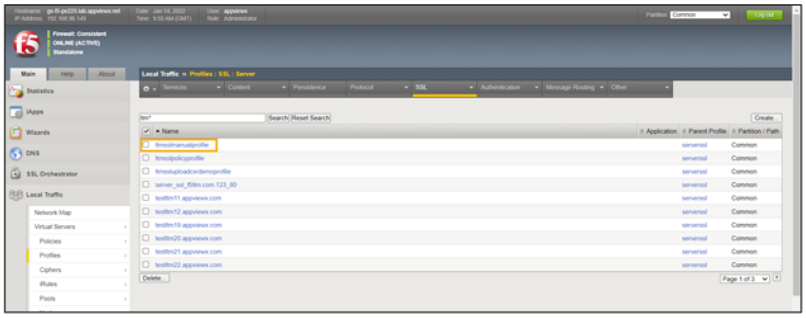
Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.
   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.
8. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

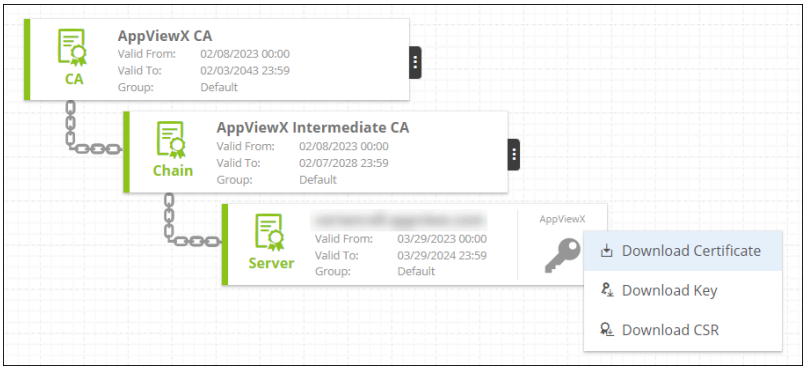
Note: You can change the profile name at this stage.

LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.

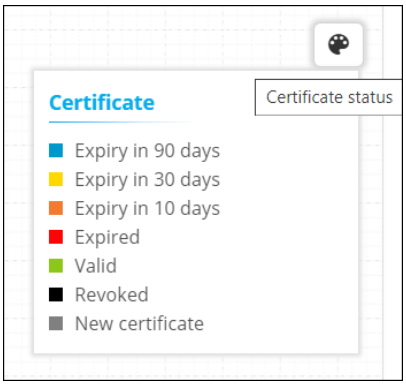
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



10. Hover your mouse over  to view the **Certificate status**.



Policy Based

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

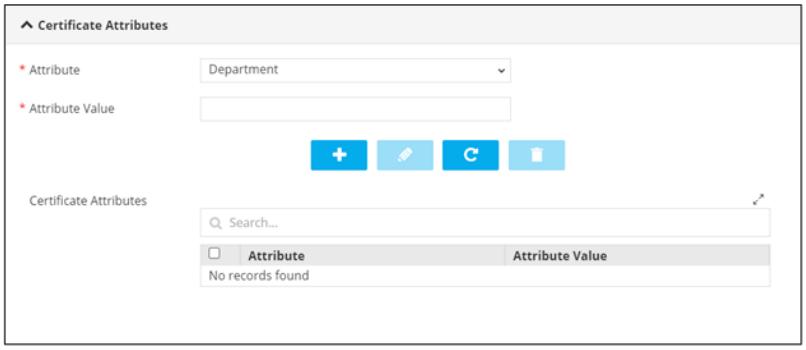
> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.



> **Note:** For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter the email address(es).

Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.

   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.

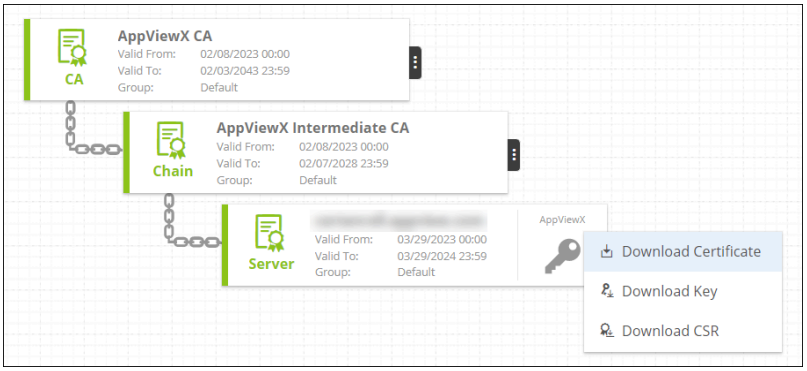
8. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

Note: You can change the profile name at this stage.

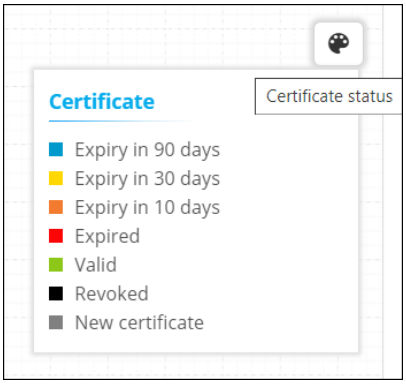
LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



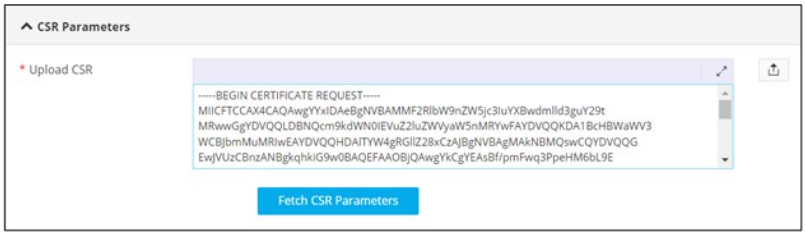
10. Hover your mouse over  to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click  .

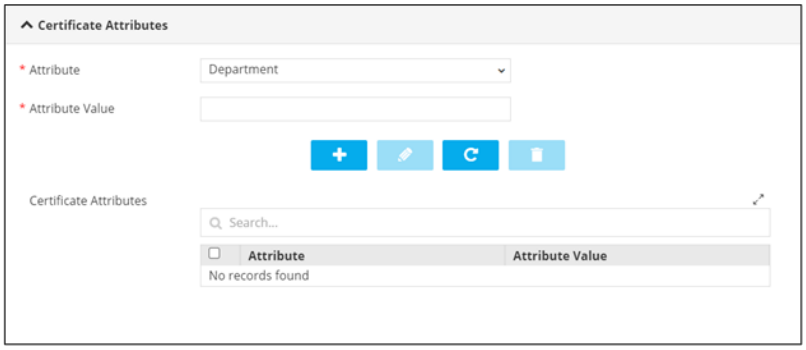


2. Click **Fetch CSR Parameters**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Note: This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

6. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

7. Under the **Notifications** section, enter the email address(es).

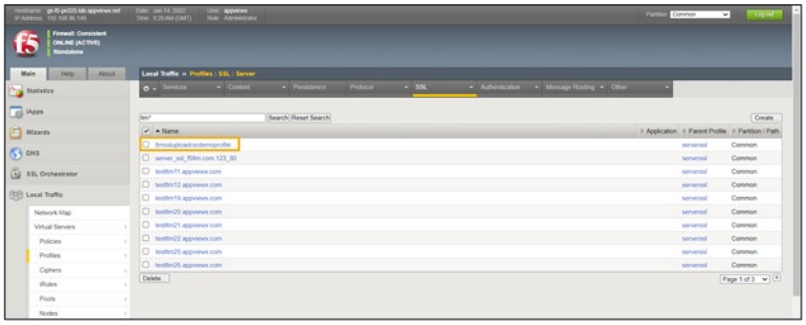
Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

8. Click **Submit**.
   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.
9. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

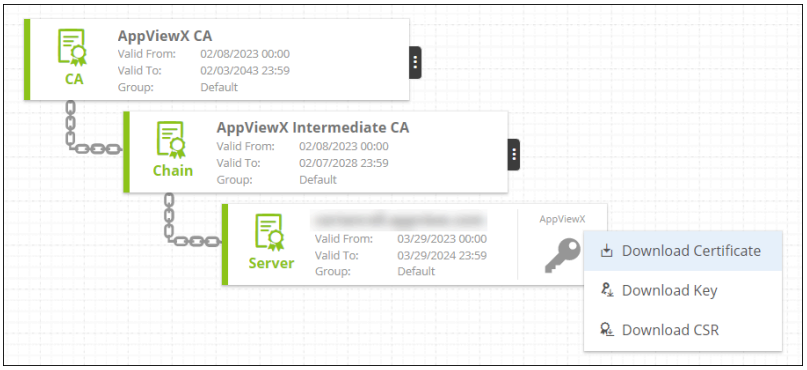
Note: You can change the profile name at this stage.

LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.

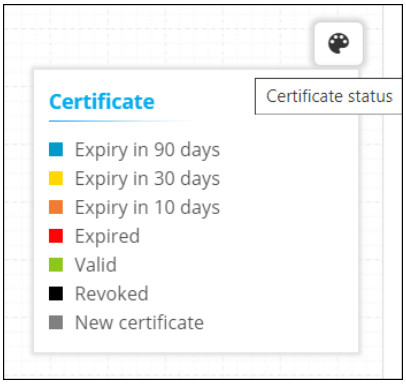
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



10. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



11. Hover your mouse over  to view the **Certificate status**.



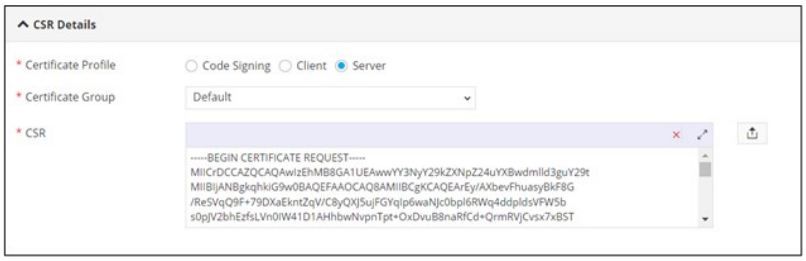
Enroll Certificate with Certificate Group and CSR Upload

This workflow allows you to create a certificate with minimal input. The Certificate Authority (CA) must be associated with the respective policy and Certificate group. In case there are multiple CAs associated with a policy, the first available CA will be considered for certificate creation.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with Certificate Group and CSR Upload** workflow and click . The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CSR Details** section, select the requested field information as described in the table below.

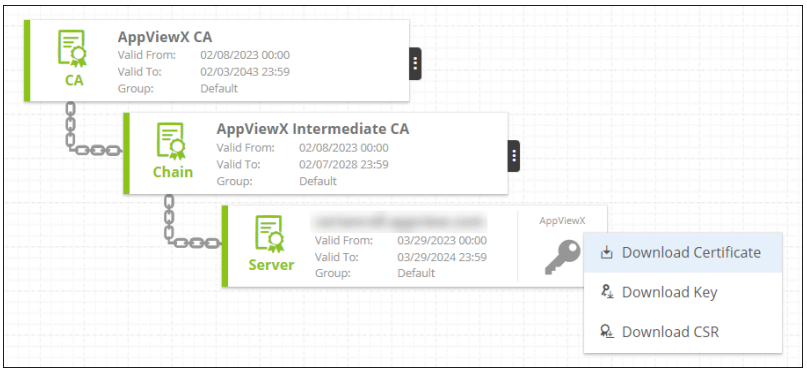


Field description for CSR Details section

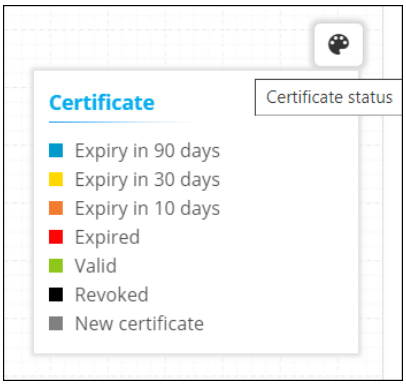
Field	Description
***Certificate Profile**	Select the **Certificate Profile** from the following options: • **Code Signing** • **Server** • **Client** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***CSR**	Click to upload the **CSR** file.
All asterisk(*) marked fields are mandatory.	

3. Click **Submit**.
   AppViewX Certificate is generated successfully.
4. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Hover your mouse over  to view the **Certificate status**.



Enroll Certificate With ServiceNow

This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM).

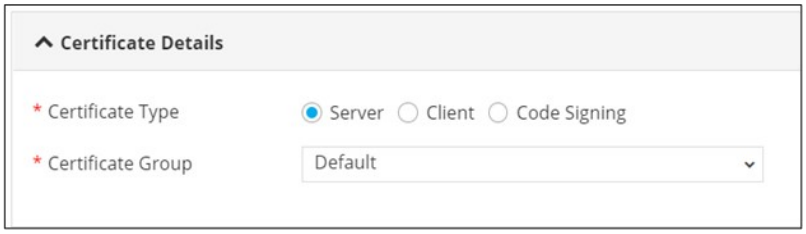
To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with ServiceNow** workflow and click  .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.

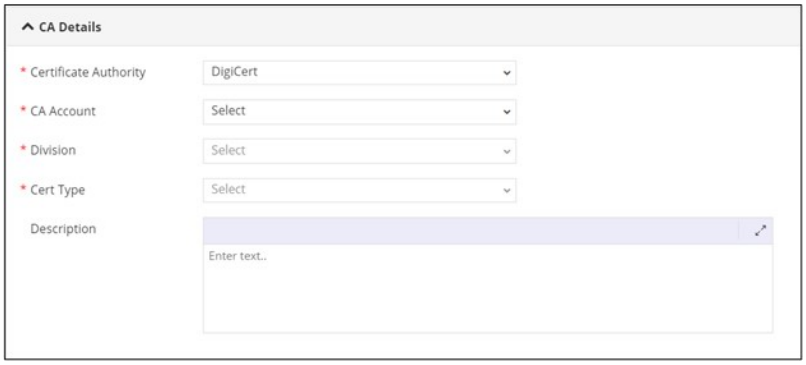
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field description for Certificate Details section

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information described in the table below.



Field description for CA Details section

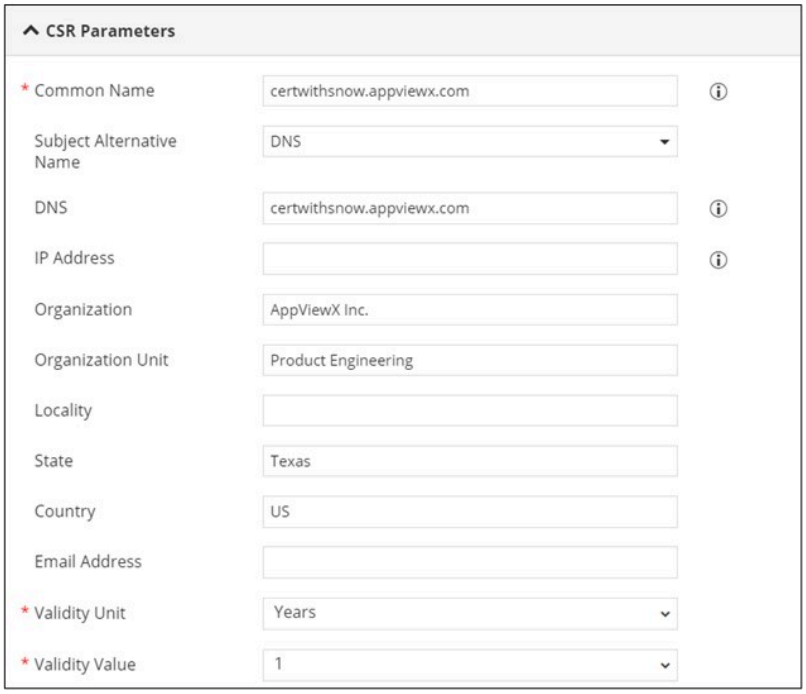
Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA

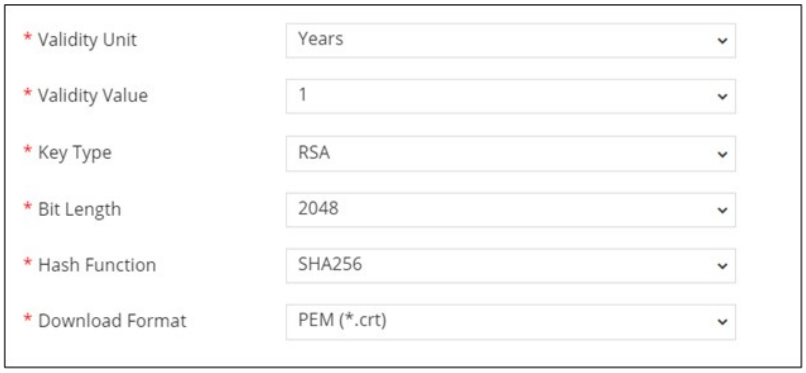
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	• Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Provide a Description for the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Field description for CSR Parameters section

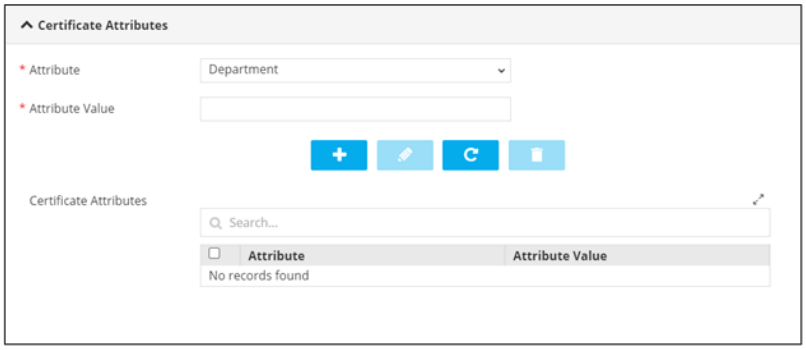
Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.
***Subject Alternative Name (SAN)**	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization**	Enter the name of the organization .
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

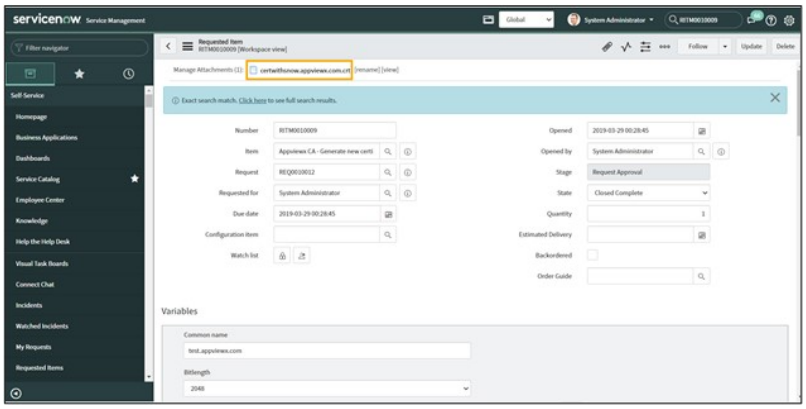
8. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
9. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).



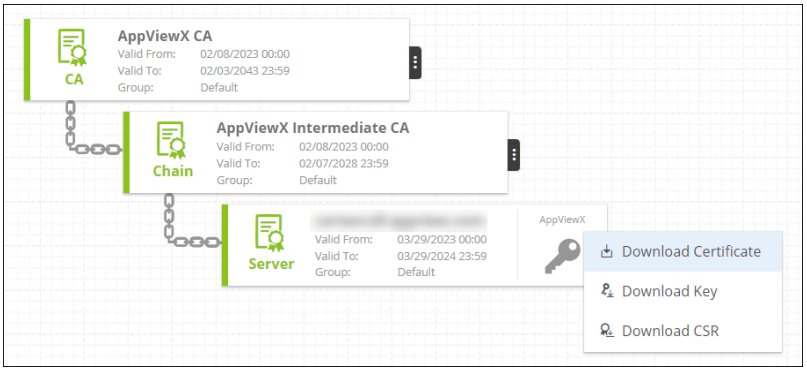
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.
11. Click **Submit**.

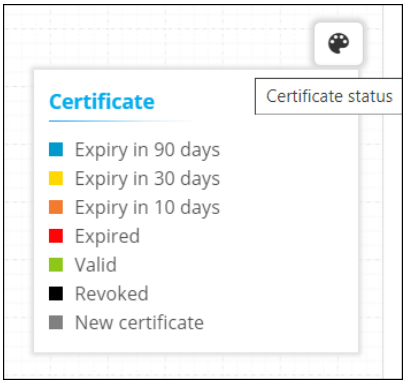
    AppViewX Certificate is created successfully and the RITM ticket status updated. The certificate is updated in the ServiceNow ticket.



12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



13. Hover your mouse over  to view the **Certificate status**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Enroll Certificate and Push with ServiceNow

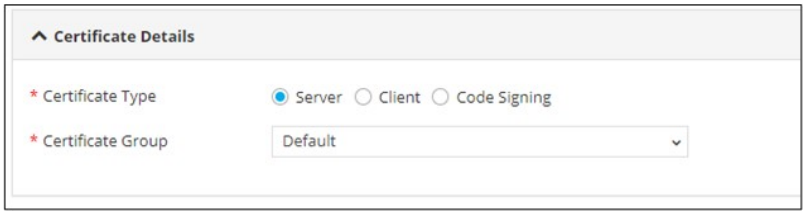
This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push with ServiceNow** workflow and click  .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.

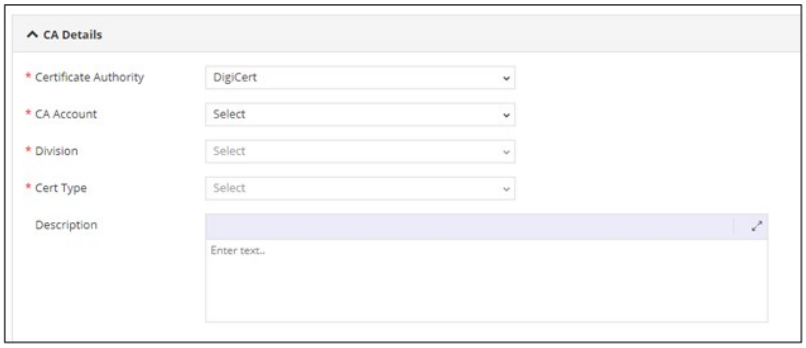


Field description for Certificate Details section

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

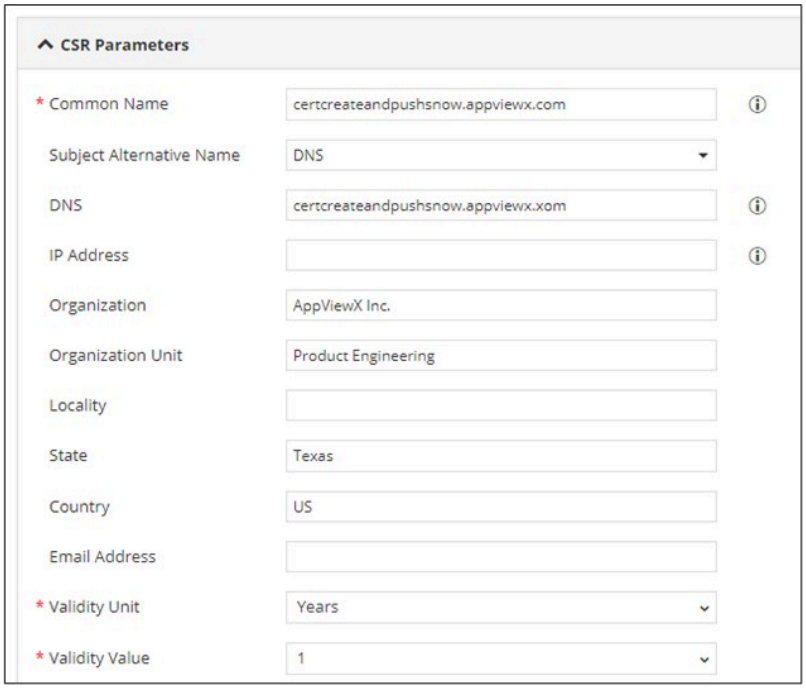


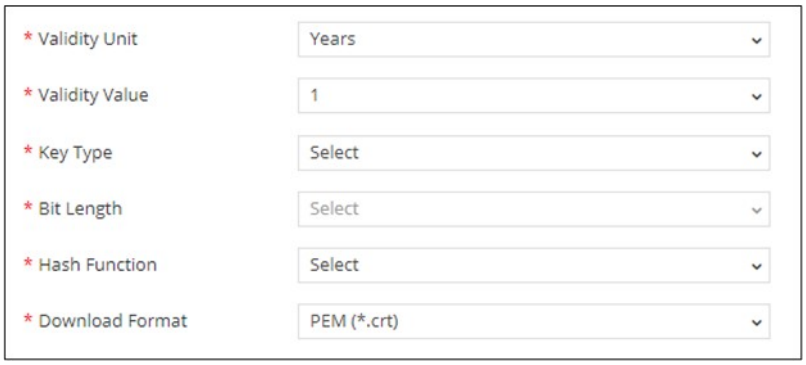
Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Provide a description of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Field description for CSR Parameters section

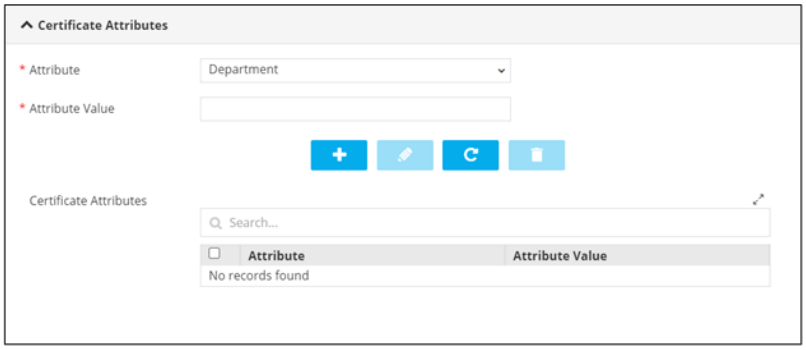
Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization**	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.

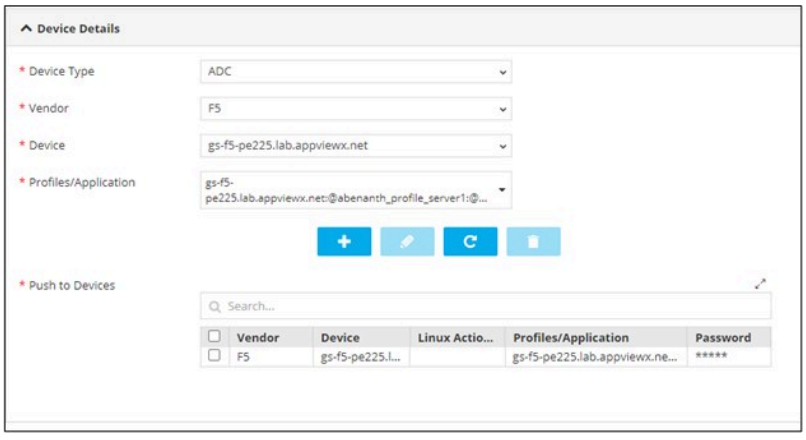
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Device Details** section, select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

8. To add the selected profile/application to the grid, click +.
   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

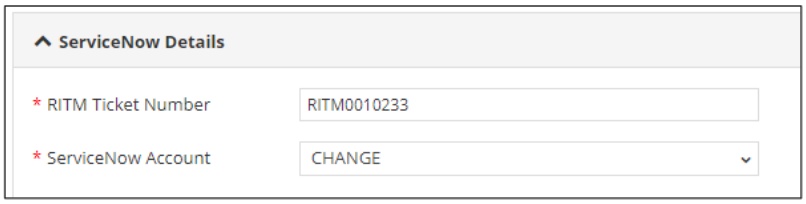
Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

9. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

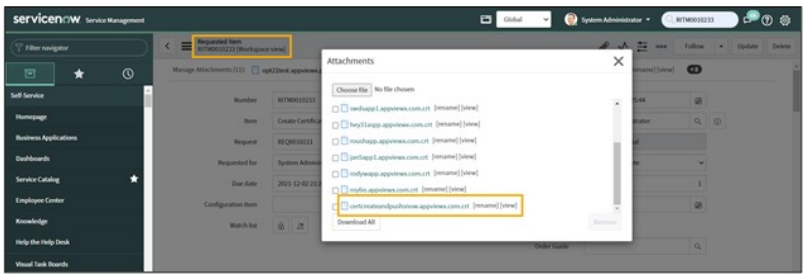
> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

10. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
11. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).



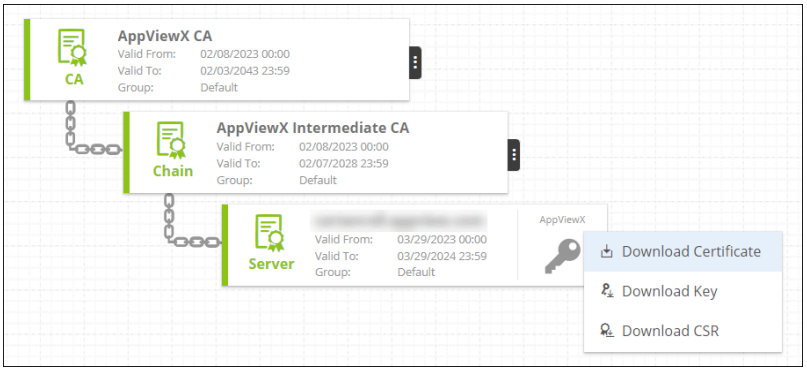
12. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.
13. Click **Submit**.

AppViewX Certificate is created successfully and pushed to the selected device. RITM ticket status updated and the certificate updated in the ServiceNow ticket.

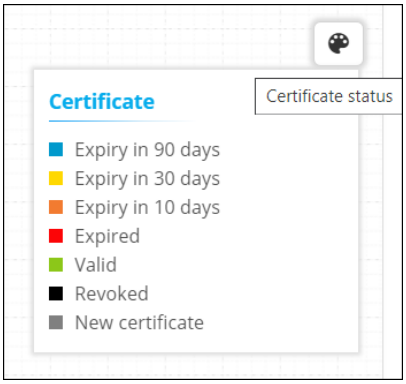


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



15. Hover your mouse over  to view the **Certificate status**.



Easy Certificate Provisioning

This workflow allows you to create an AppViewX certificate and push to a device available in the instance. Once the certificate is created, an email is sent to the logged in user informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** window, under the **Enrollment** category, hover your mouse over the **Easy Certificate Provisioning** workflow and click  .

> **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

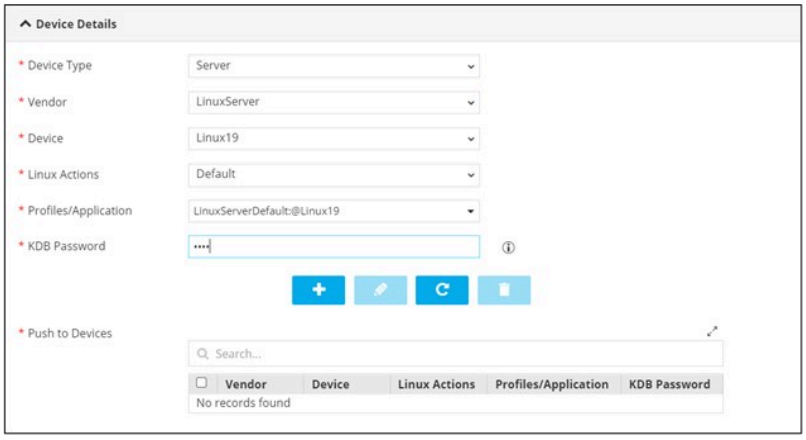
2. Under the **CSR Parameters** section, enter the **Common Name**.

> **Note:** This is a mandatory field.

3. Under the **CSR Parameters** section, enter the **Subject Alternative Name**.



4. Under the **Device Details** section, enter or select the requested field information as described in the table below.



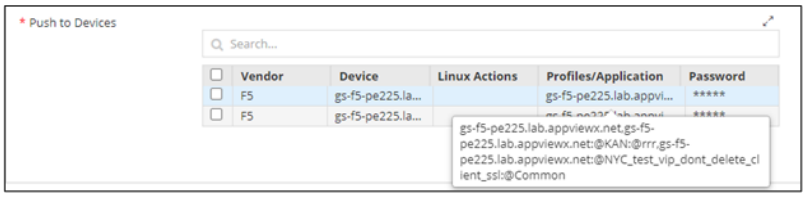
Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the Push to Devices grid, click  .
   The profile/application is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the Push to Devices grid, under the **Profiles/Applications** column as comma-separated values.

Actions available in the Push to Devices grid

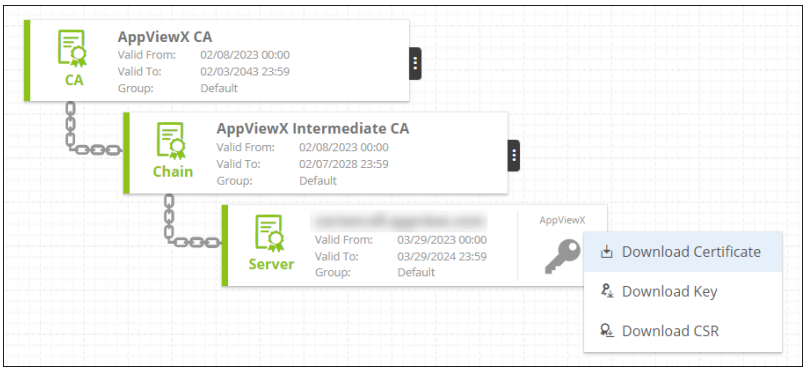
Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a profile/application.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

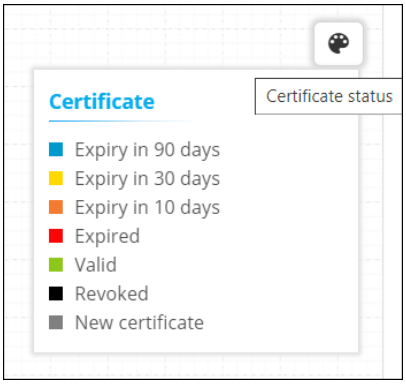
Action	Description
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Click **Submit**.
   AppViewX certificate is created and pushed to the selected device. At the **Summary** stage of workflow execution, a Push to Device Status grid is displayed, which can be downloaded by clicking from the top right corner of the screen.

7. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



8. Hover your mouse over to view the Certificate status.



Enroll Certificate with CAA Validation

This workflow allows you to create a certificate by validating the Certificate Authority that can issue the certificate based on the given domain name.

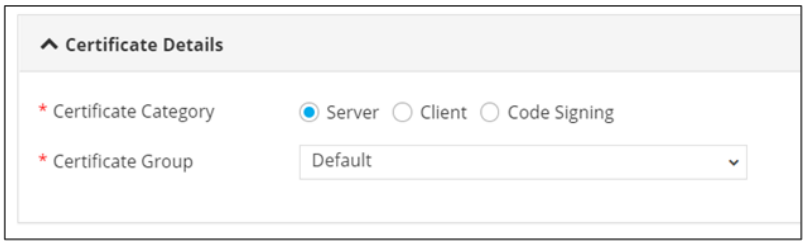
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with CAA Validation** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.

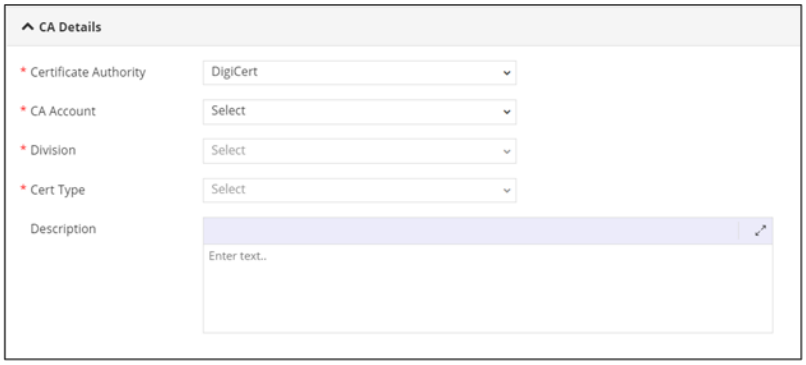


Field description for Certificate Details section

Field	Description
***Certificate Category**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

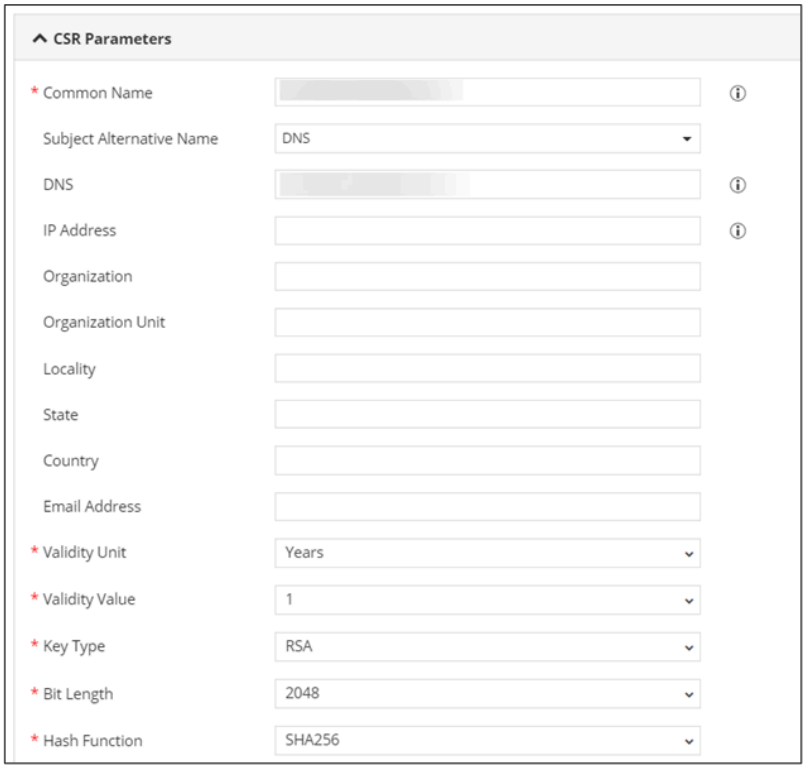


Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Under the **CSR Parameters** section, enter or select the field information as described in the table below.



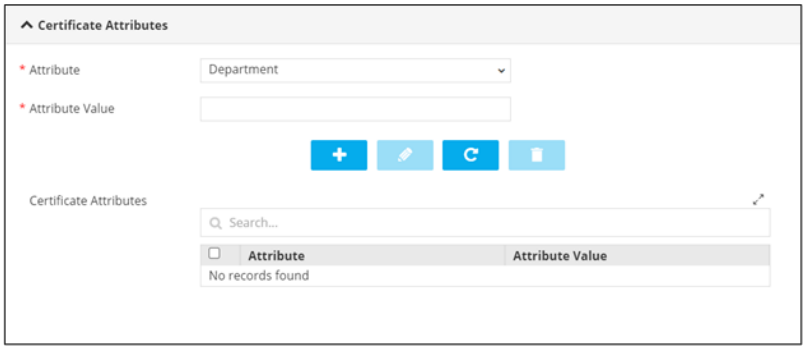
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

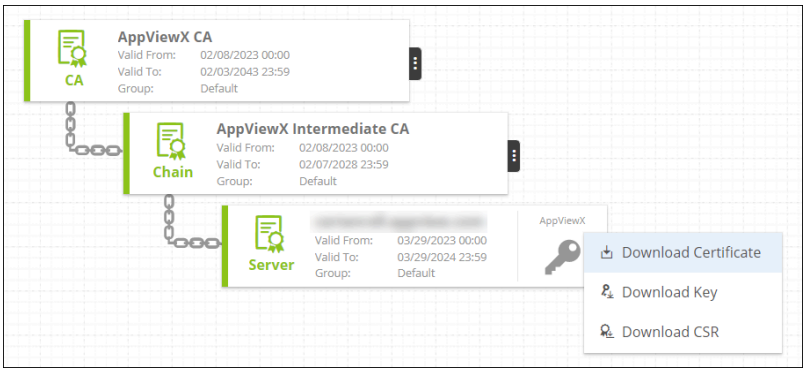
8. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

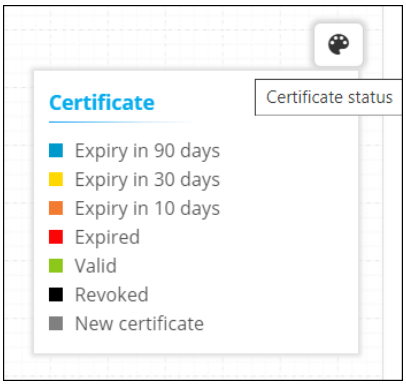
9. Click **Submit**.
   CAA Validation is successful and the certificate is created successfully.

10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



11. Hover your mouse over  to view the Certificate status.



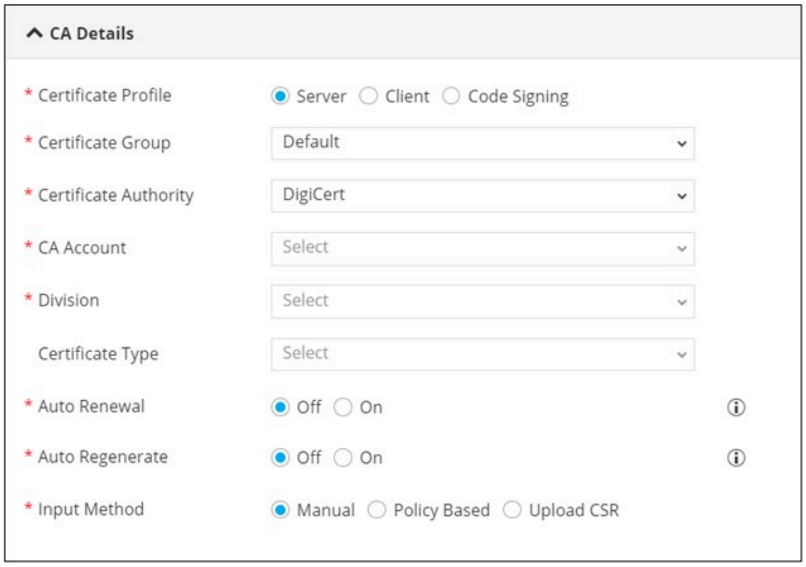
Enroll Certificate and Push

This workflow allows you to create a certificate and push it to the selected device.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push** workflow and click  .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for CA Details section

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field. **Note:** This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. • **Policy Based**: If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR**: If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Manual is the default selection.
All Asterisk (*) marked fields are mandatory.	

What to do next:

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

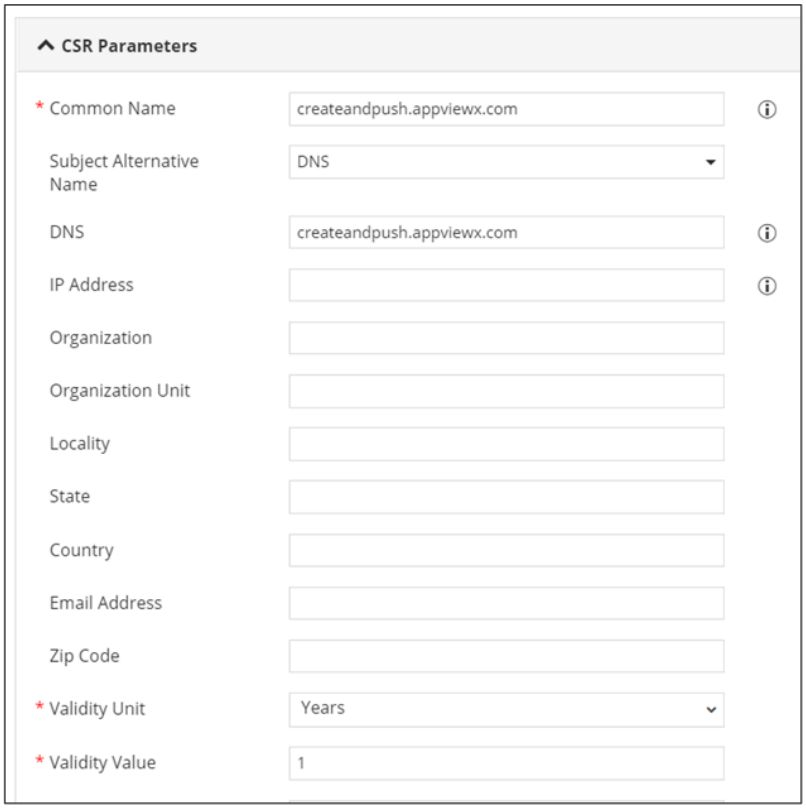
- Manual
- Policy Based
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Under **CSR Parameters**, enter or select the requested field information as described in the table below.





Field description for CSR Parameters section

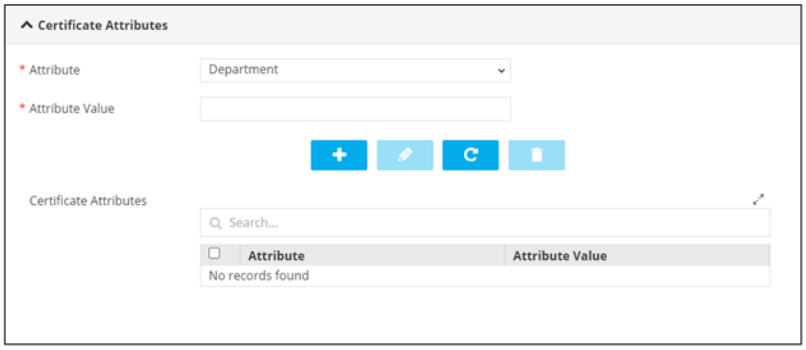
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

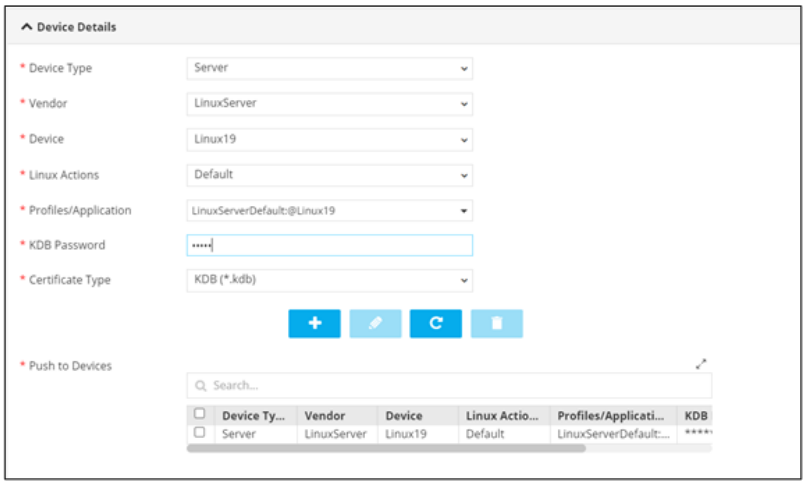
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Device Details** section, enter or select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click  .
   The **Profile/Application** is added to the **Push to Devices** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



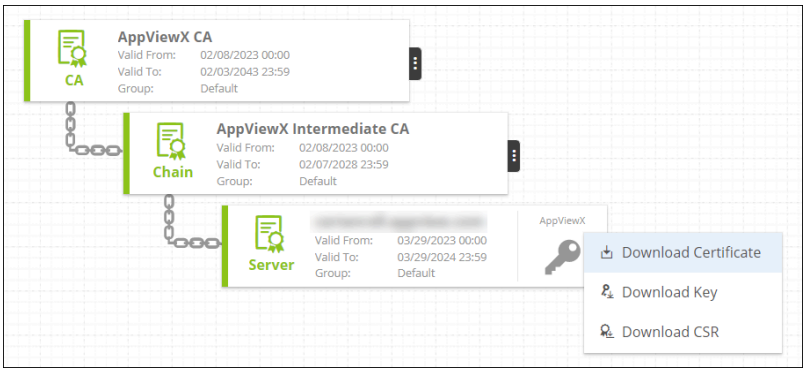
Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

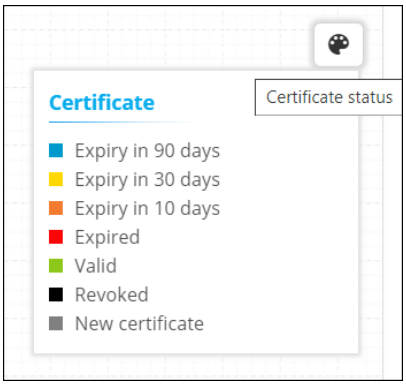
6. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



8. Hover your mouse over  to view the **Certificate status**.



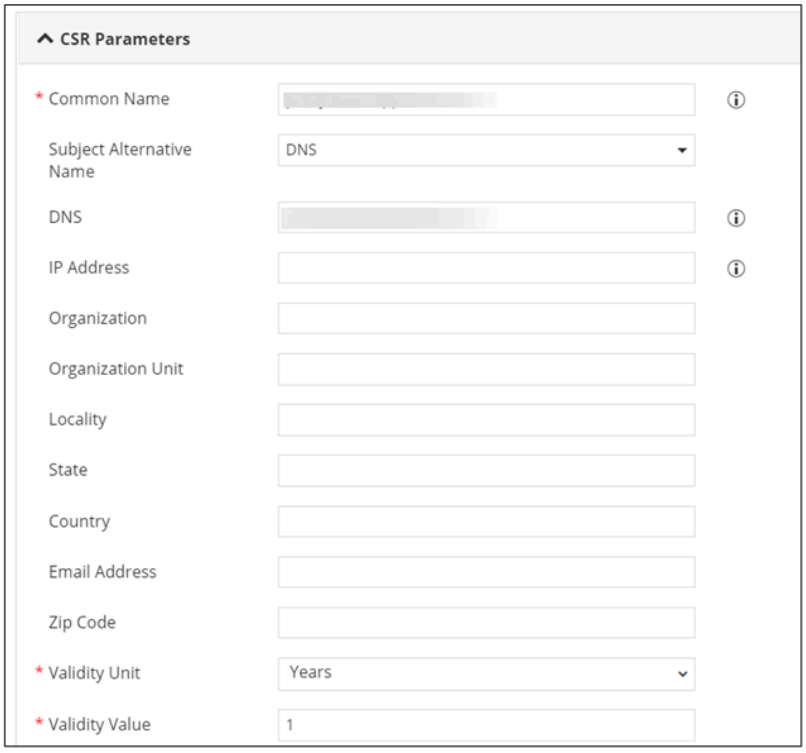
Policy Based

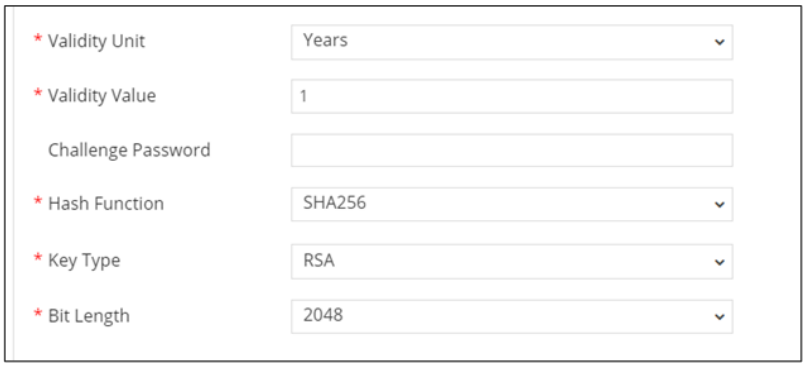
After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter the field information as described in the table below.

> **Note:** Some **CSR Parameters** will be auto-populated based on the policy associated with the **Certificate Group**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

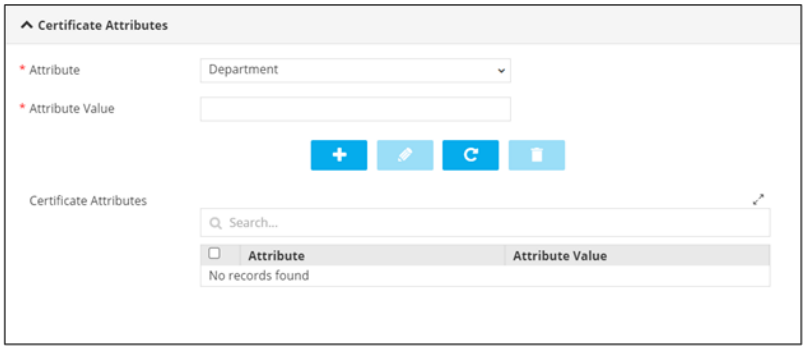




Note: For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

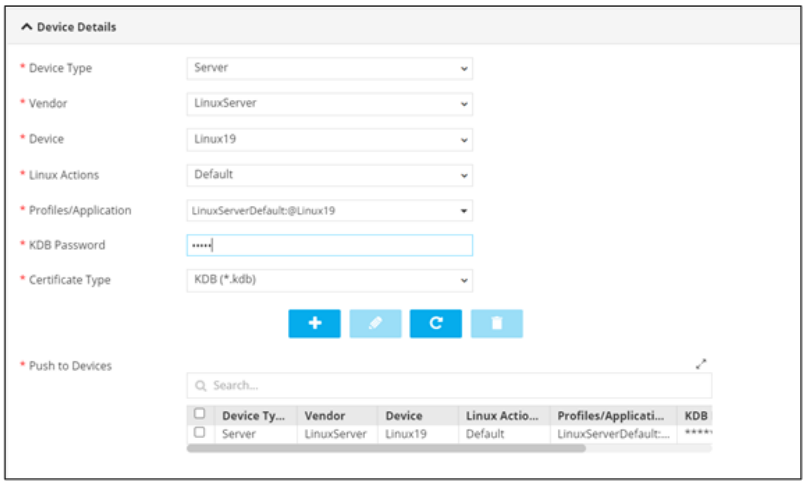
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Device Details** section, enter or select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field description for Device Details section

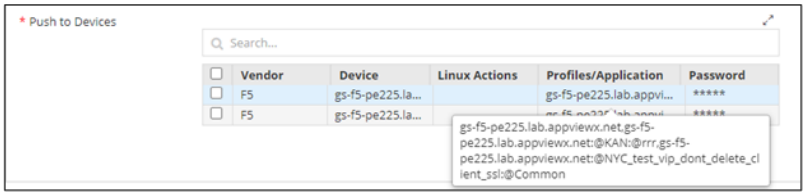
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click  .

   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

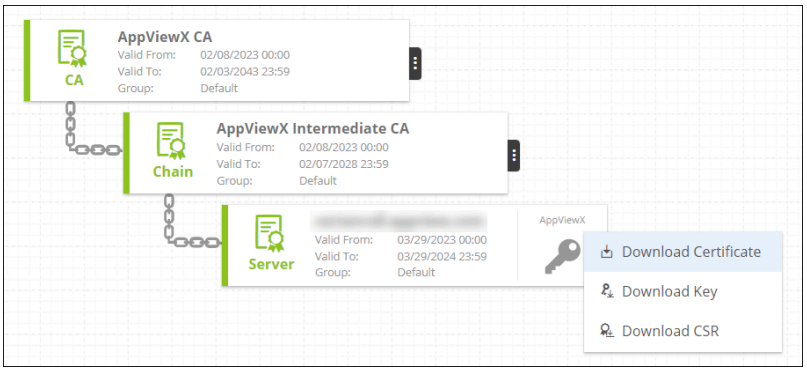


Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

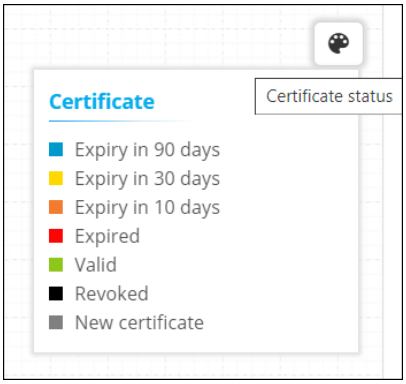
6. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

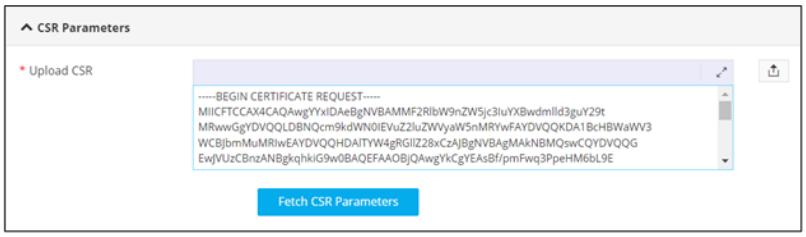
8. Hover your mouse over  to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click  .

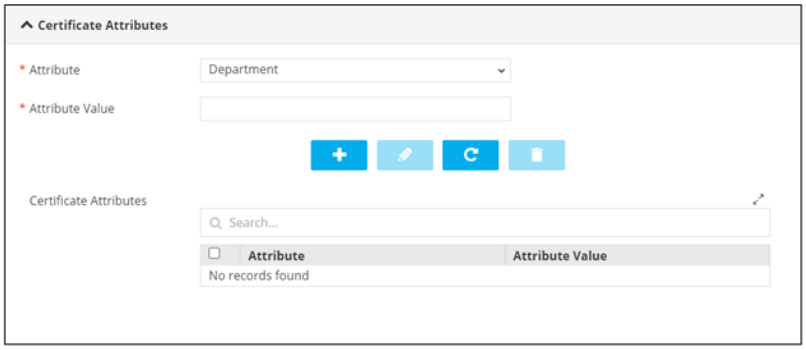


2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Policy Based section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



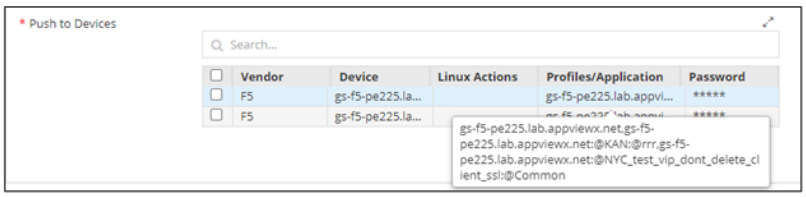
Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. To add the selected profile/application to the grid, click  .
   The **Profile/Application** is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

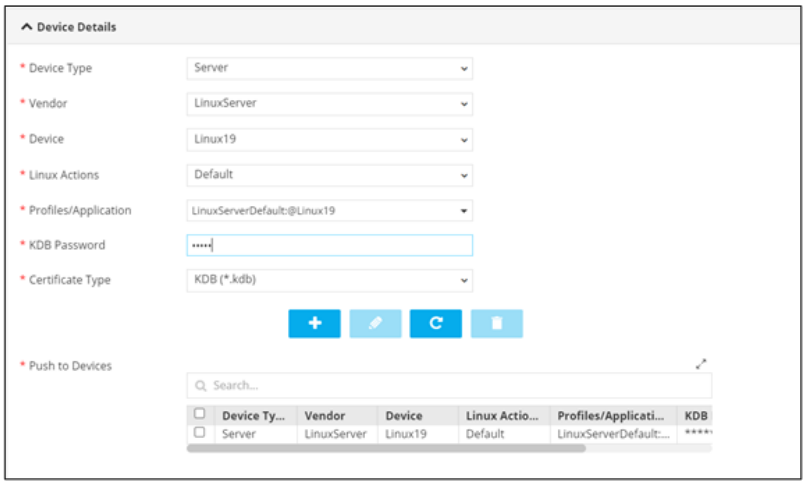


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Under the **Device Details** section, enter or select the requested field information as described in the table below.



Field description for Device Details section

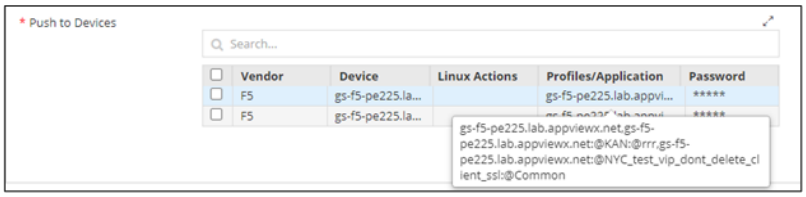
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

7. To add the selected profile/application to the grid, click  .
   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

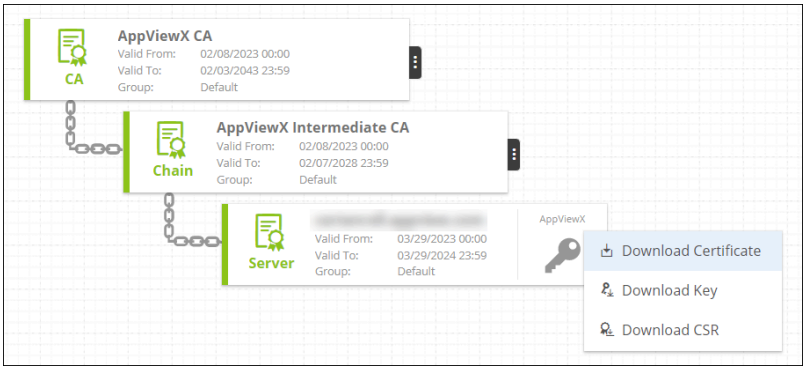
Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

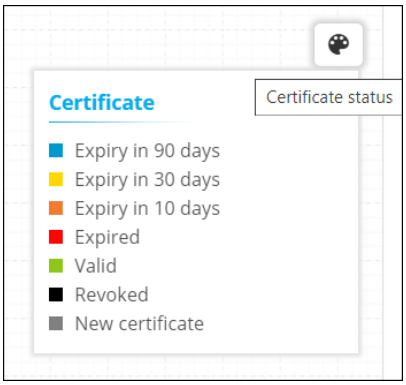
Action	Description
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

8. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



10. Hover your mouse over  to view the **Certificate status**.



Renew Certificate Workflows

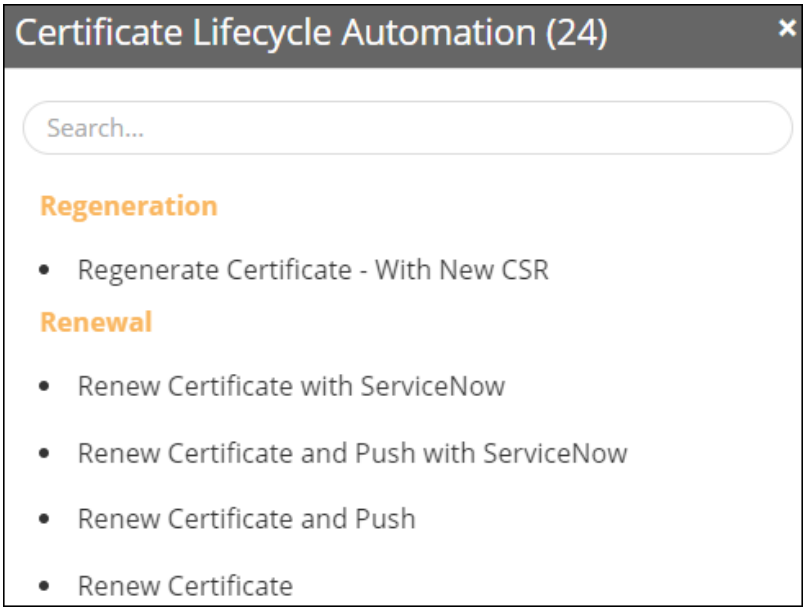
- Overview
- Renew Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Regenerate Certificate with New CSR
- Renew Certificate and Push
- Renew Certificate with ServiceNow
- Renew Certificate and Push with ServiceNow

Overview

This section lists and describes the workflows that can be used to renew and regenerate certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Renewal with Incident Automation. These workflows are available in the **Certificate Lifecycle Automation** catalog under the **Regeneration** and **Renewal** categories.



Renew Certificate

This workflow allows you to renew a certificate based on the certificate group and certificate authority.

To trigger this workflow:

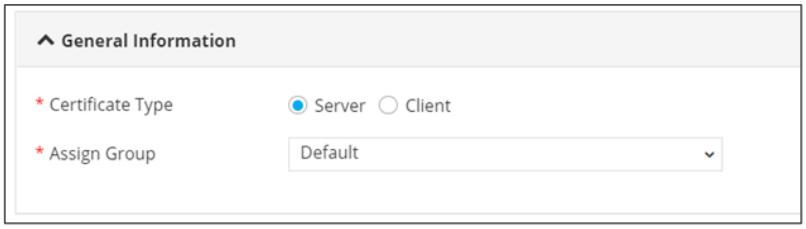
1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

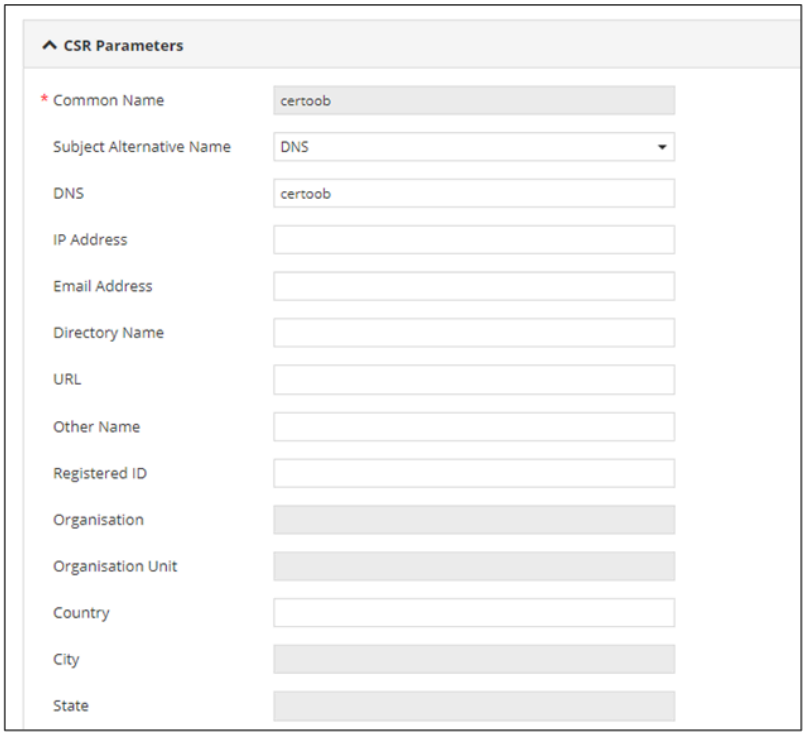
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



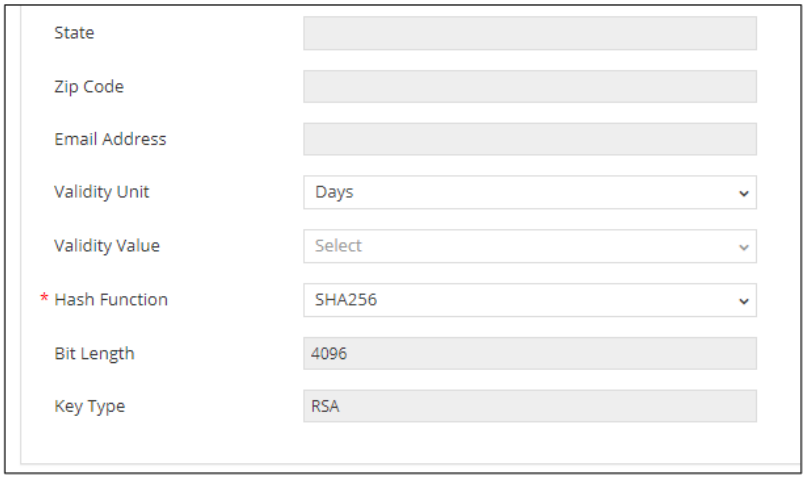
4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
5. Under the **CA Details** section, add a description for the certificate being renewed (optional).



6. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.
7. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.



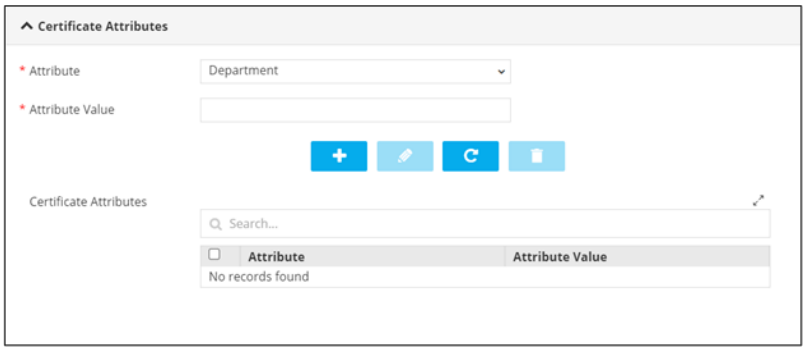
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
Search bar	Allows you to search for a particular attribute in the grid.

10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

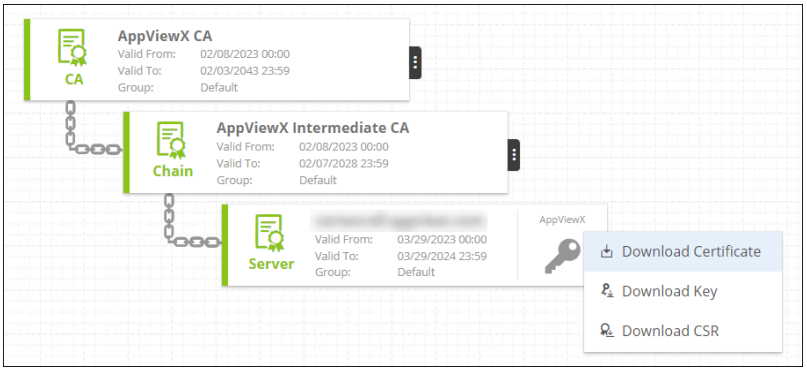
> **Note:** This section is displayed only when DigiCert, EJBCA, or Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

11. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

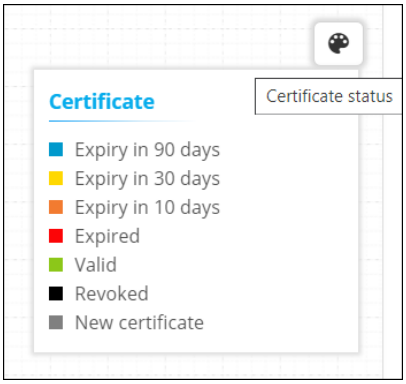
12. Click **Submit**.
    Certificate is renewed successfully.

13. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

14. Hover your mouse over to view the Certificate status.



Regenerate Certificate with New CSR

This workflow allows you to regenerate a certificate with a new CSR.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Regenerate Certificate with New CSR** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the **Certificate Type** (mandatory).
3. Under the **Certificate Details** section, select the **Assign Group** (mandatory).
4. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Field Description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

What to do next:

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

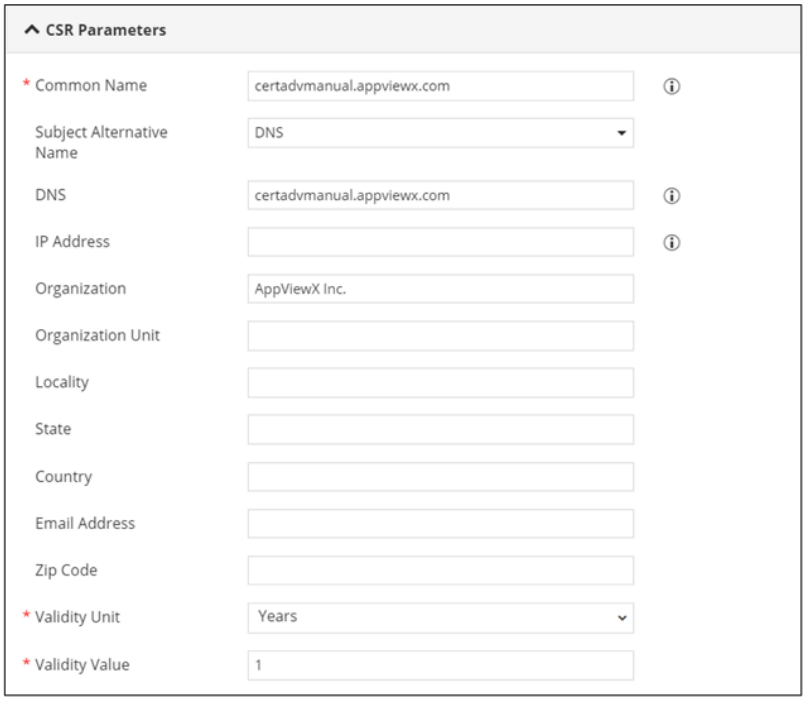
- Manual
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.





Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.

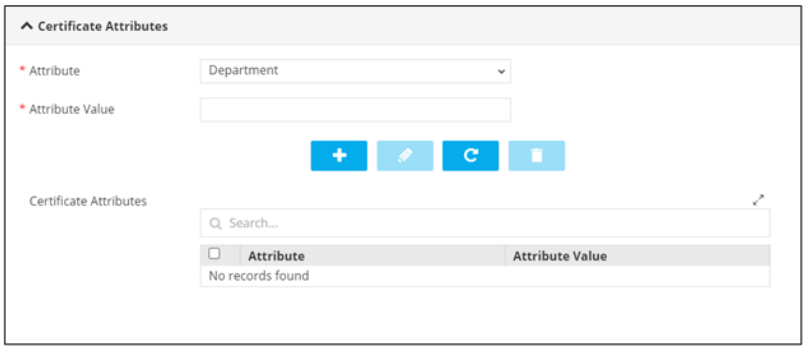
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name** • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

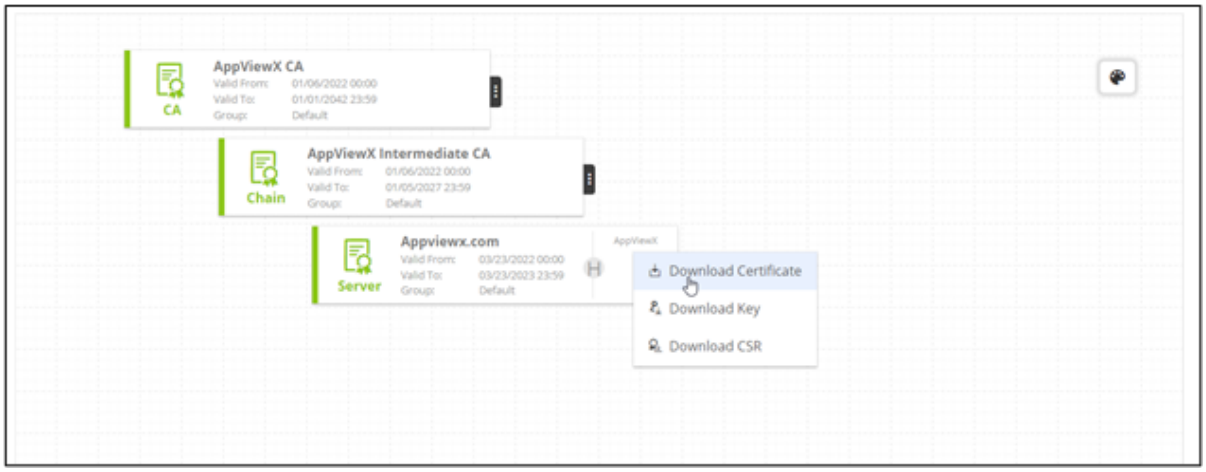
> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

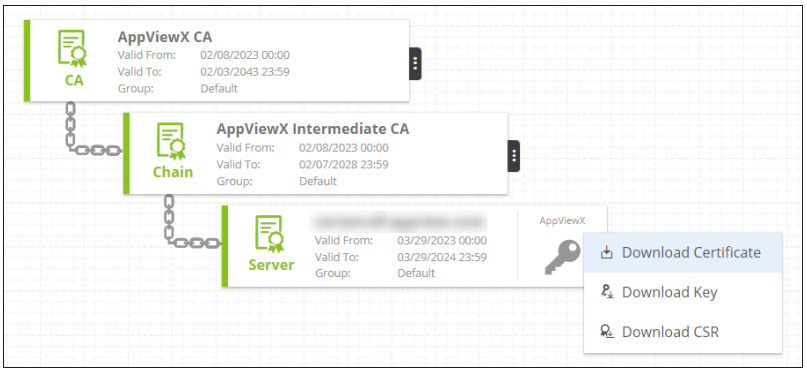
6. Click **Submit**.
   Certificate is regenerated successfully.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.

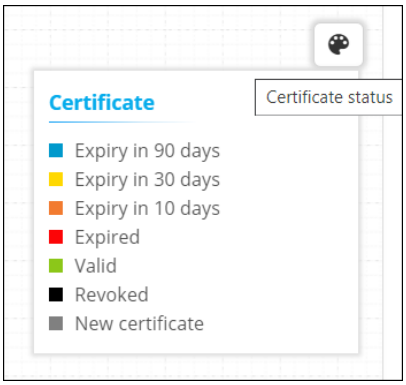


8. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



9. Hover your mouse over to view the Certificate status.



Upload CSR

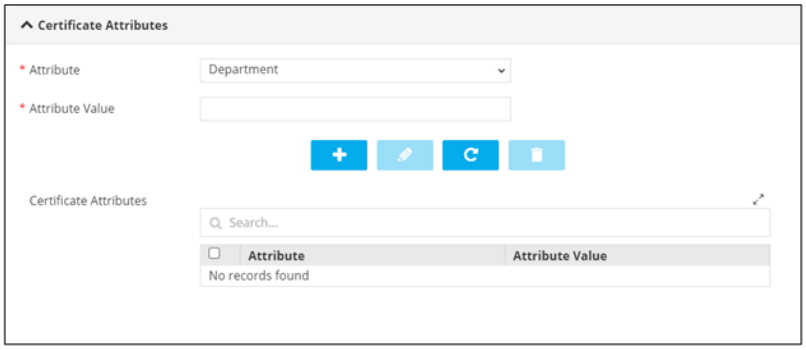
After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click .
2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

6. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

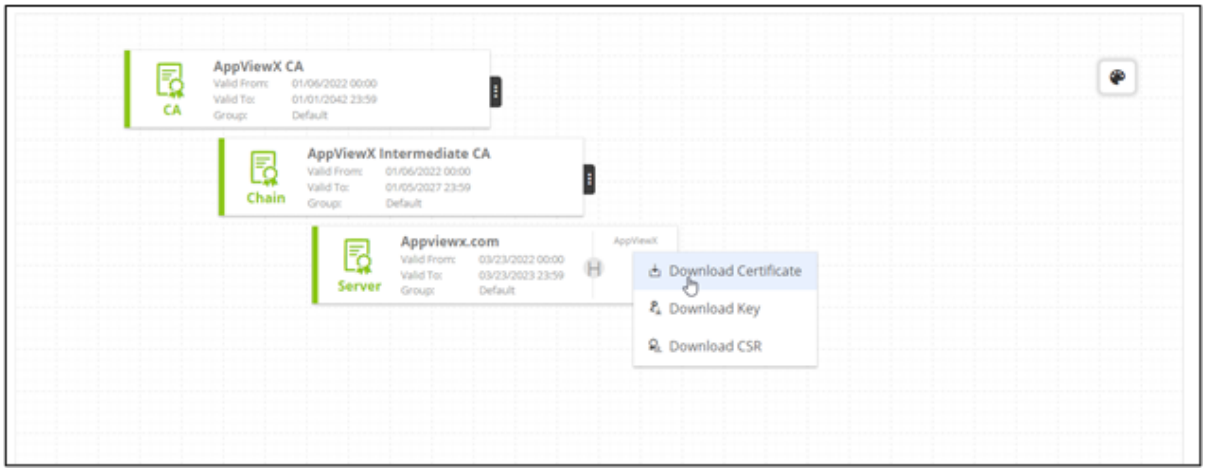
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.

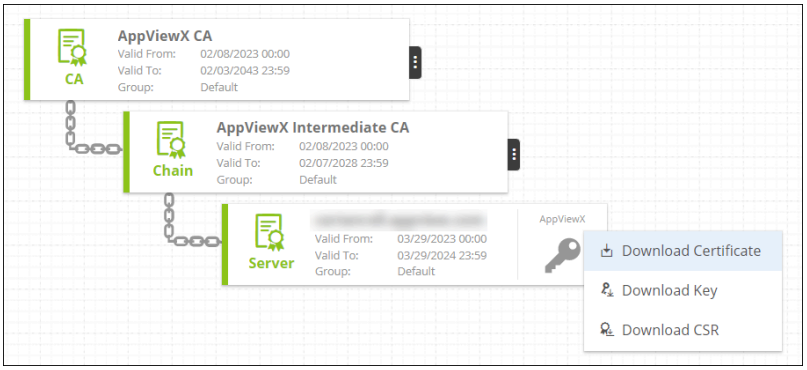
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Certificate is regenerated successfully.

8. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



9. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



Renew Certificate and Push

This workflow allows you to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

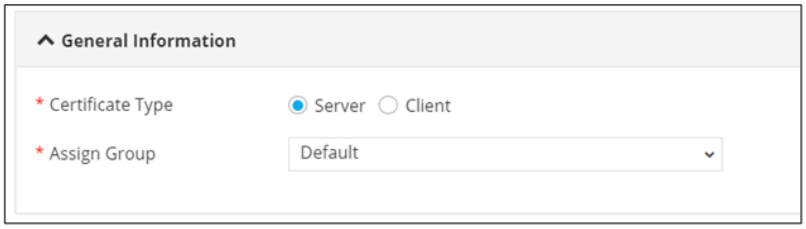
To trigger this workflow:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



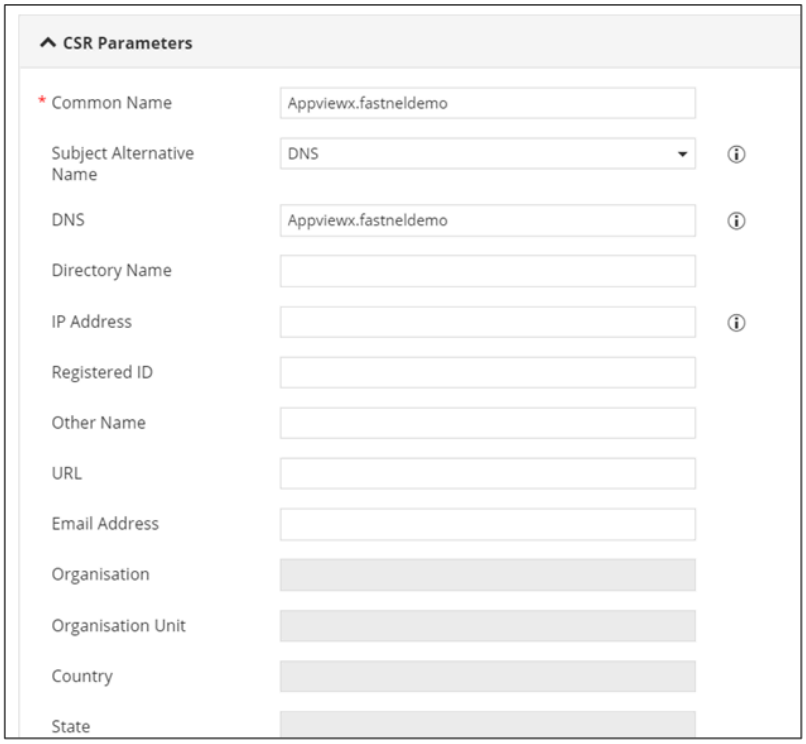
4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory).

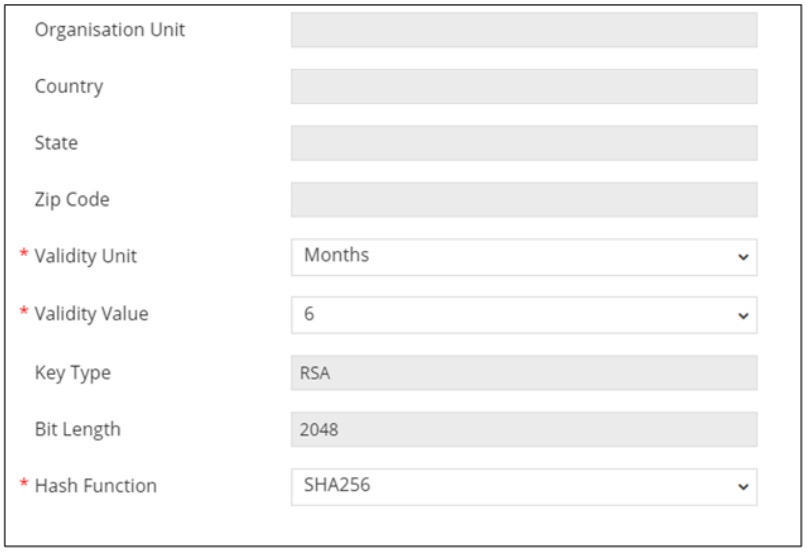
   The **Serial Number** and **CA Account** fields are populated based on the Certificate selected.



6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.

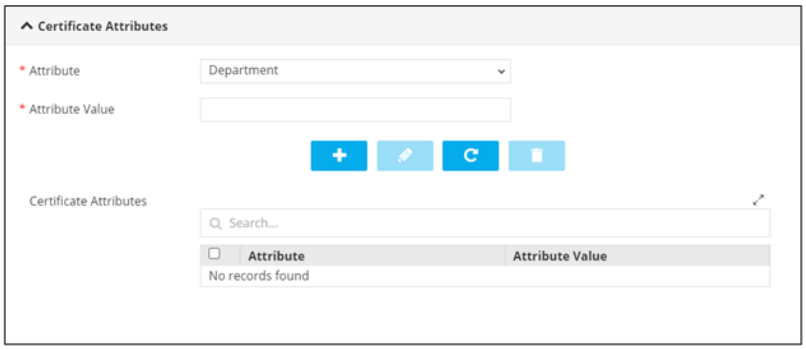
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name** • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email Address	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Country	Enter the name of the country in which the organization is located.
State	Enter the name of the state in which the organization is located.
Zip Code	Enter the zip code.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert, EJBCA, or Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

10. Under the **Device Information** section, select the field information as described in the table below.



Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

11. To add the selected profile/application to the grid, click +.
    The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

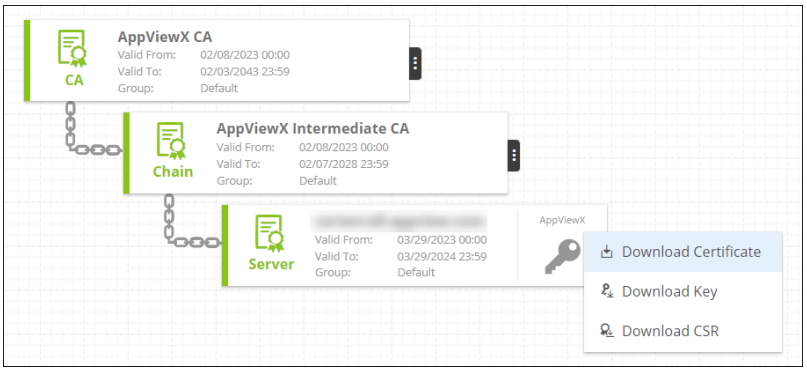
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

12. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

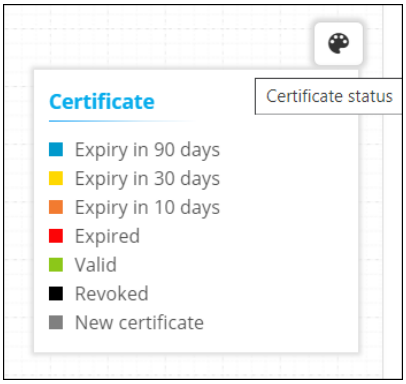
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.
    Certificate is renewed successfully.

14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



15. Hover your mouse over  to view the **Certificate status**.



Renew Certificate with ServiceNow

This workflow allows you to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.

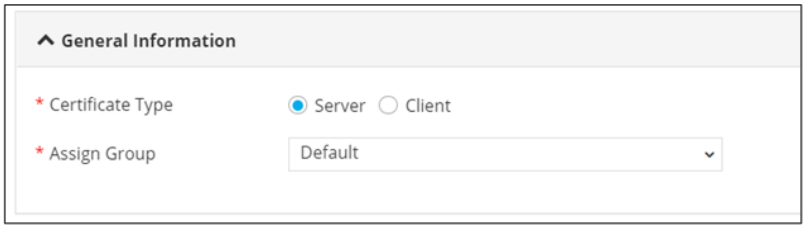
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

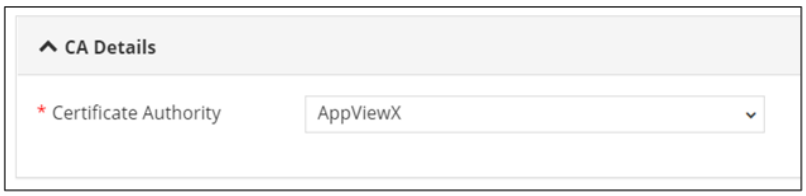
1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate with ServiceNow** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

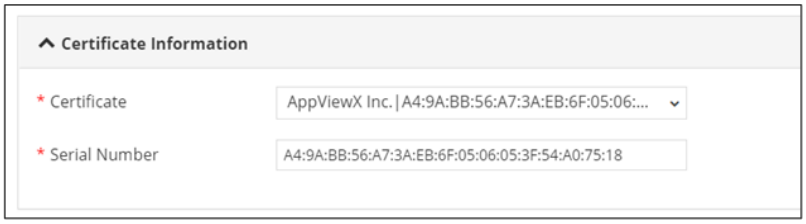
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).

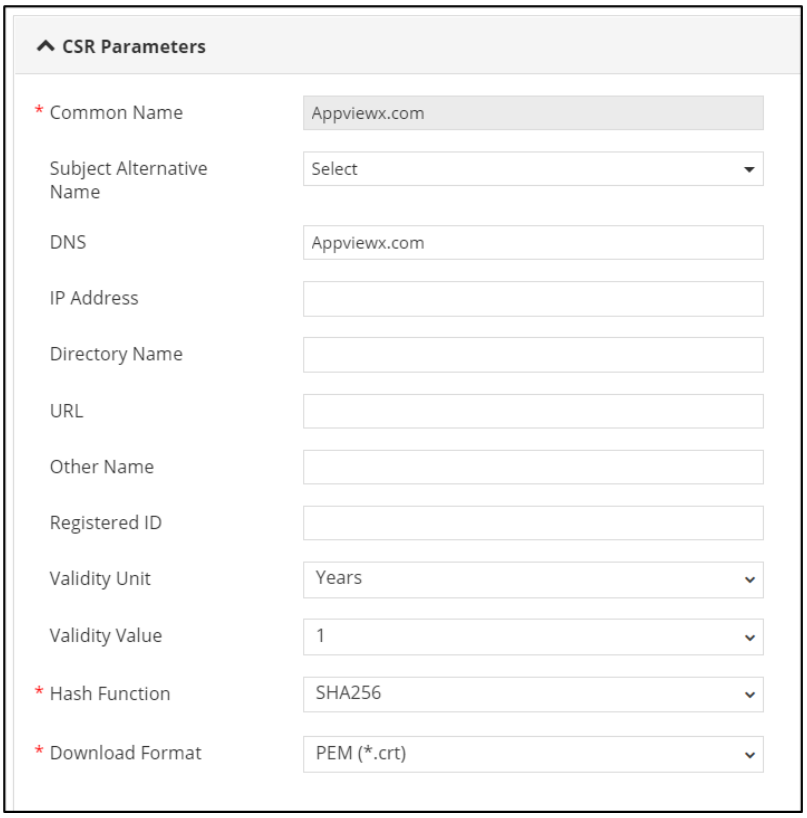


5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.



6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



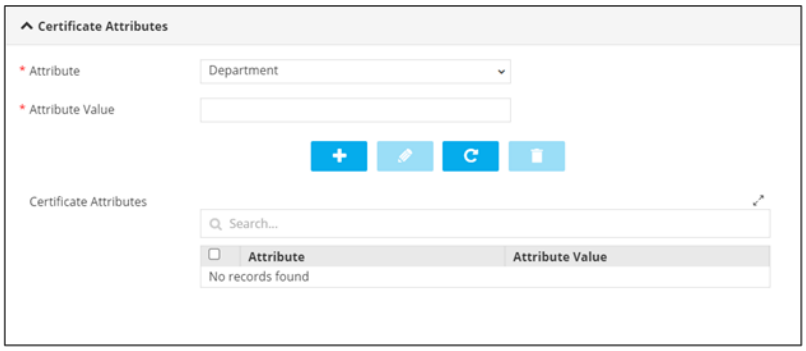
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID** • **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Validity Unit	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
Validity Value	Enter a **Validity Value** based on the selected validity unit.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Download Format**	Select the format for downloading the certificate from the available options.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.



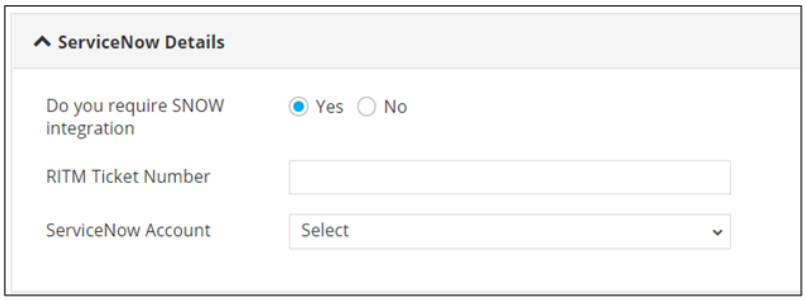
Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **ServiceNow Details** section, enter or select the requested field information as described in the table below.



Field Description for ServiceNow Details section

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

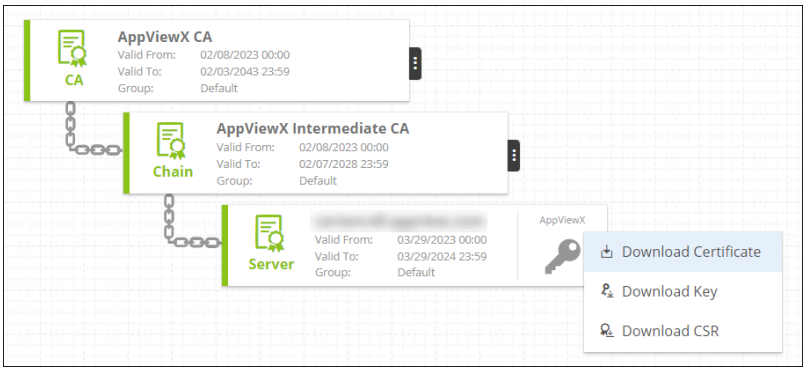
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

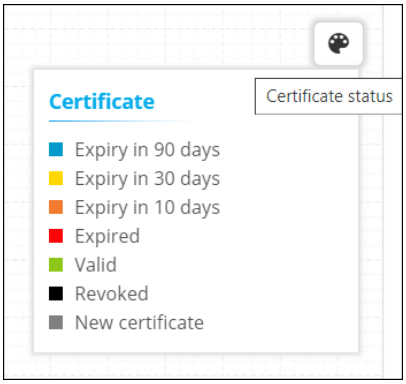
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

11. Click **Submit**.
    Certificate is renewed successfully.

12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



13. Hover your mouse over  to view the **Certificate status**.



Renew Certificate and Push with ServiceNow

This workflow allows you to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.

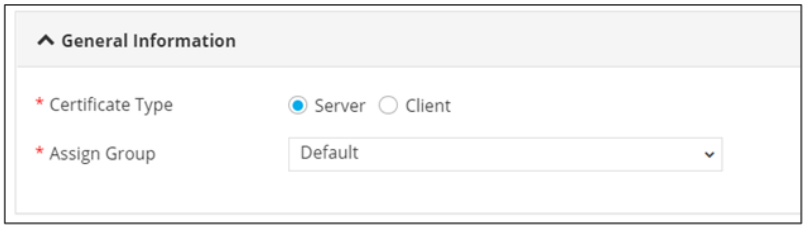
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

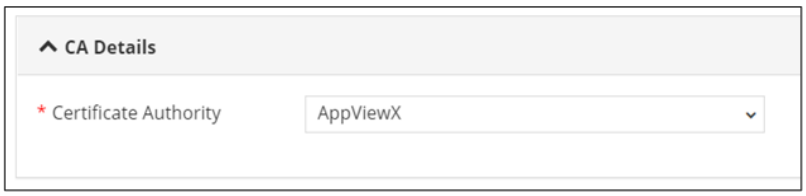
1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push with ServiceNow** workflow and click  .

   > **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).

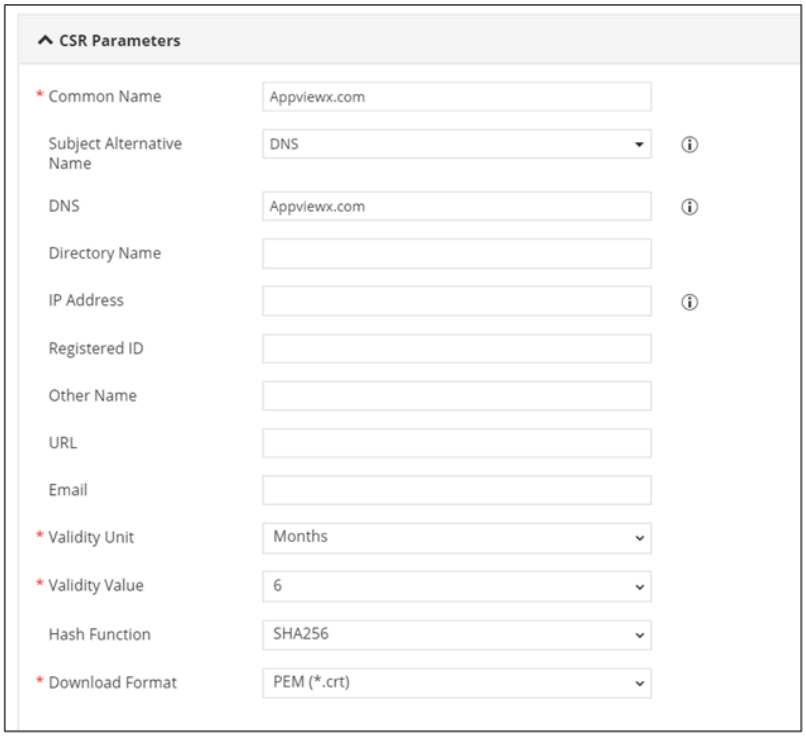


5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.



6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



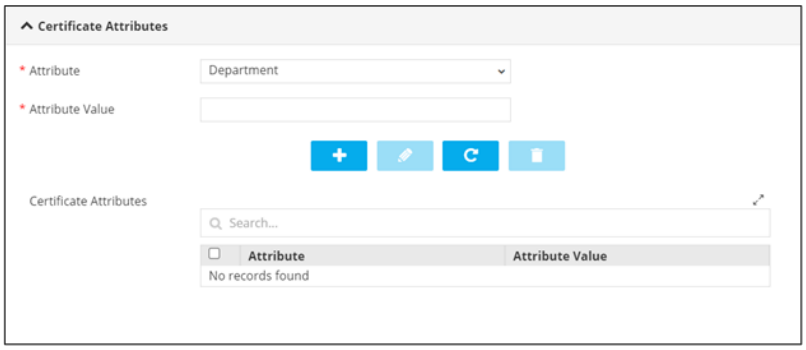
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID** • **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email	Enter a valid Email address if you select the **Email** option in the **SAN** field.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
***Download Format**	Select the format for downloading the certificate from the available options.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.



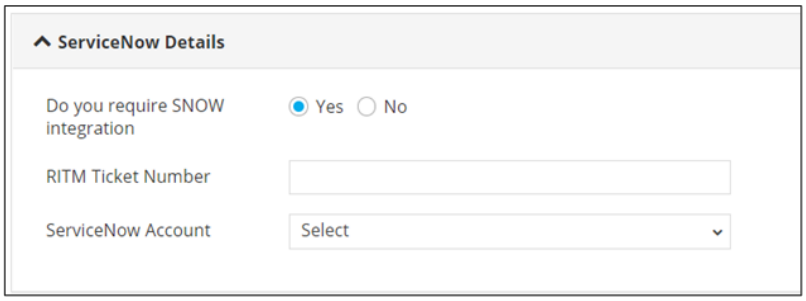
Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click  , enter the new value for the attribute, and click  again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **ServiceNow Details** section, enter or select the requested field information as described in the table below.



Field Description for ServiceNow Details section

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

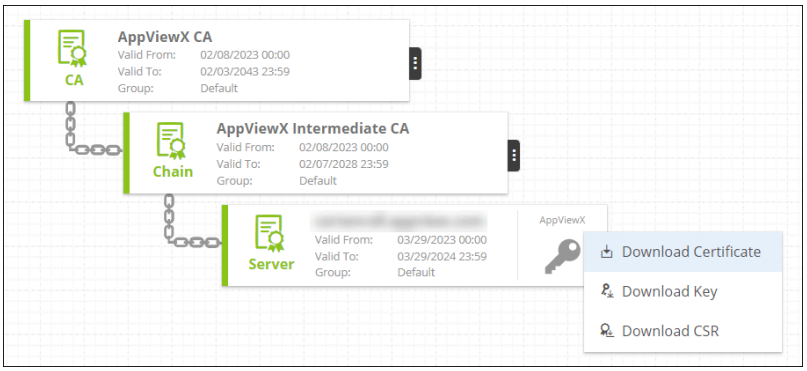
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

10. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

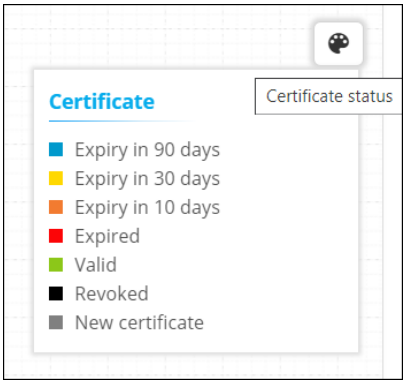
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

11. Click **Submit**.
    Certificate is renewed successfully.

12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



13. Hover your mouse over  to view the **Certificate status**.



Automation Workflow Tasks

- Overview
- Expiry Task

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Enrollment Tasks
• Renew Tasks
• Push Tasks

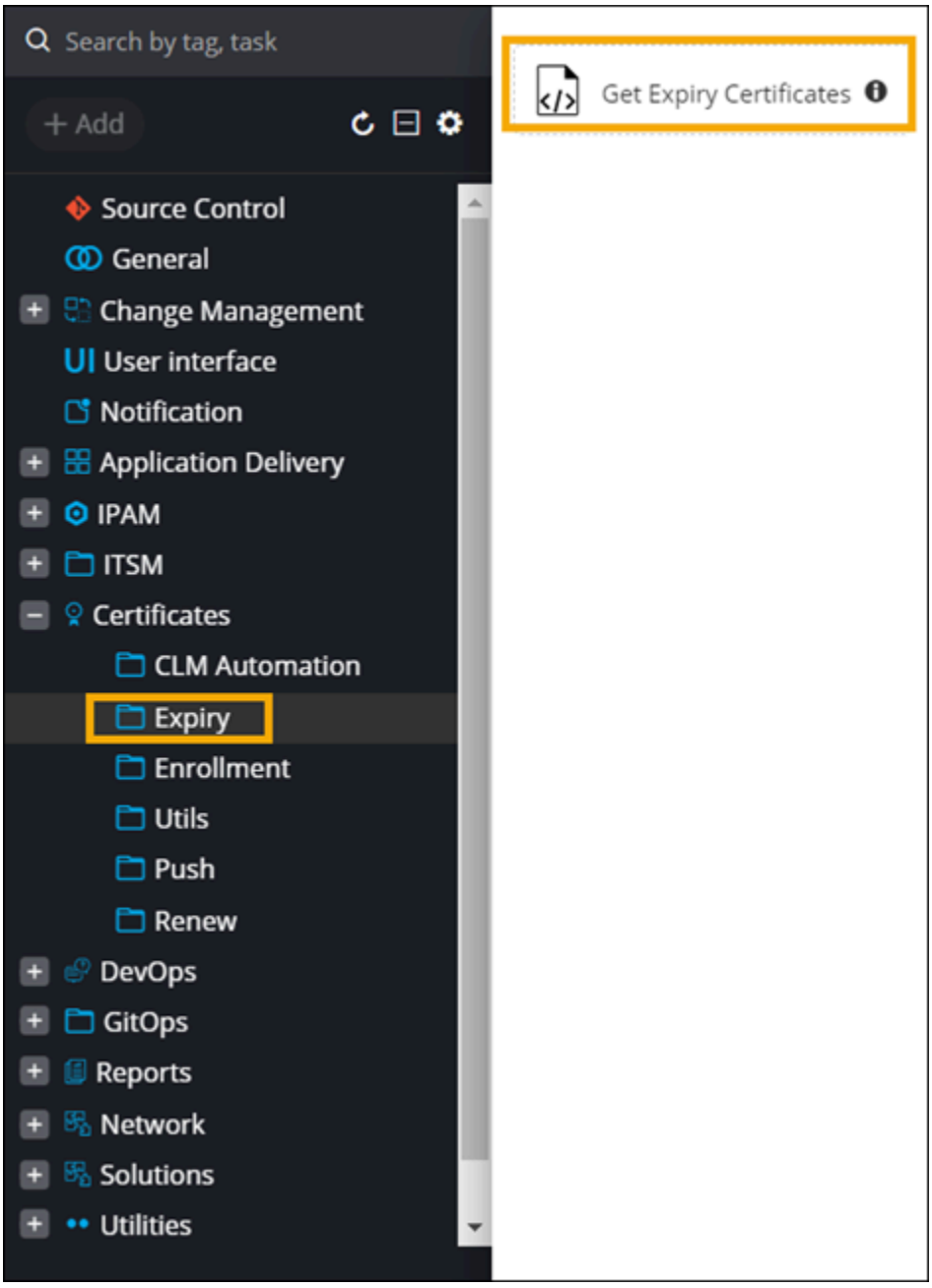
Overview

This section will describe the various OOB tasks available in the Workflow Studio.

Expiry Task

You can design a custom workflow for receiving certificate expiry notifications using the prebuilt task for getting expiry certificates available in the **Automation** module. The OOB script task for getting expiry certificates can be found under **Certificates**, in the **Expiry** folder.

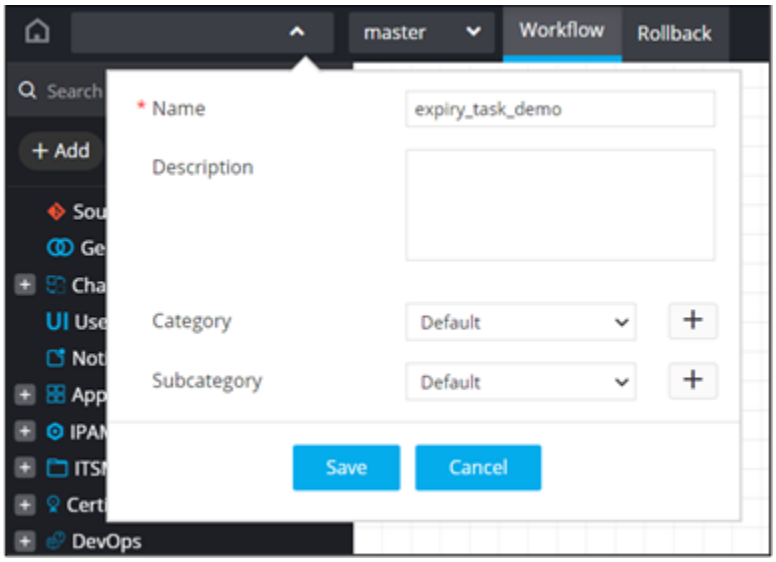
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



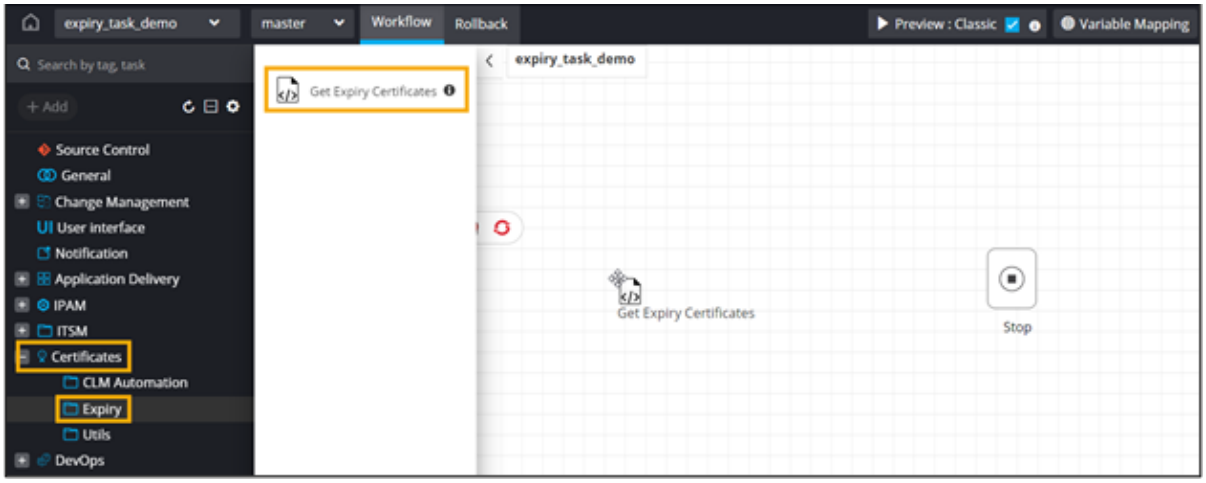
To design a custom workflow using the **Get Expiry Certificates** task

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

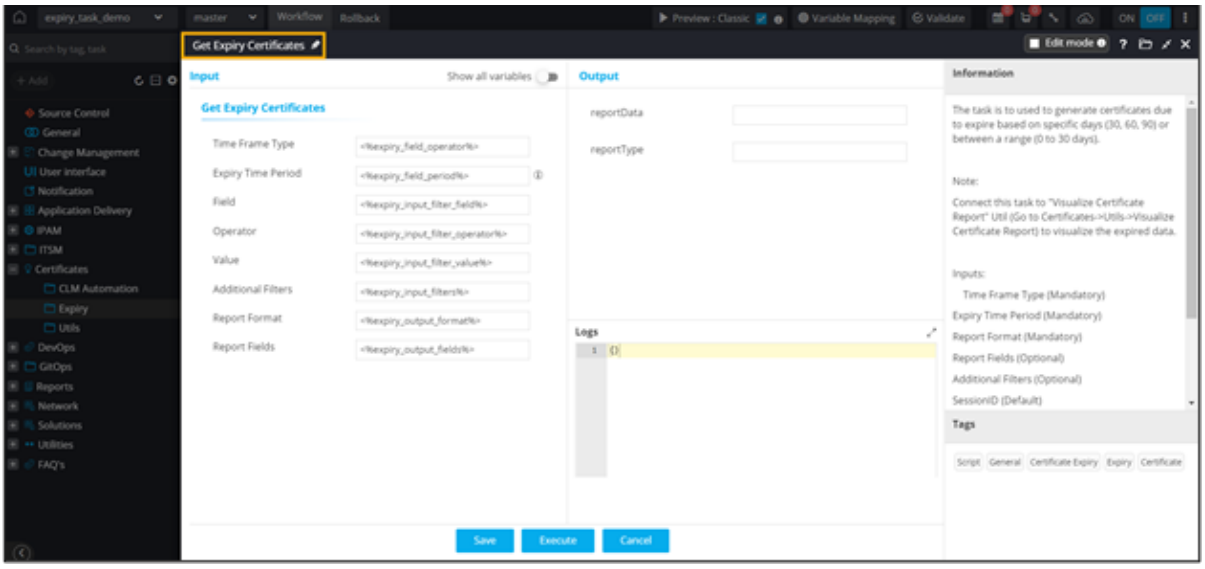


3. From the **Certificates**folder in the left menu, under **Expiry**, drag and drop the **Get Expiry Certificates** task.

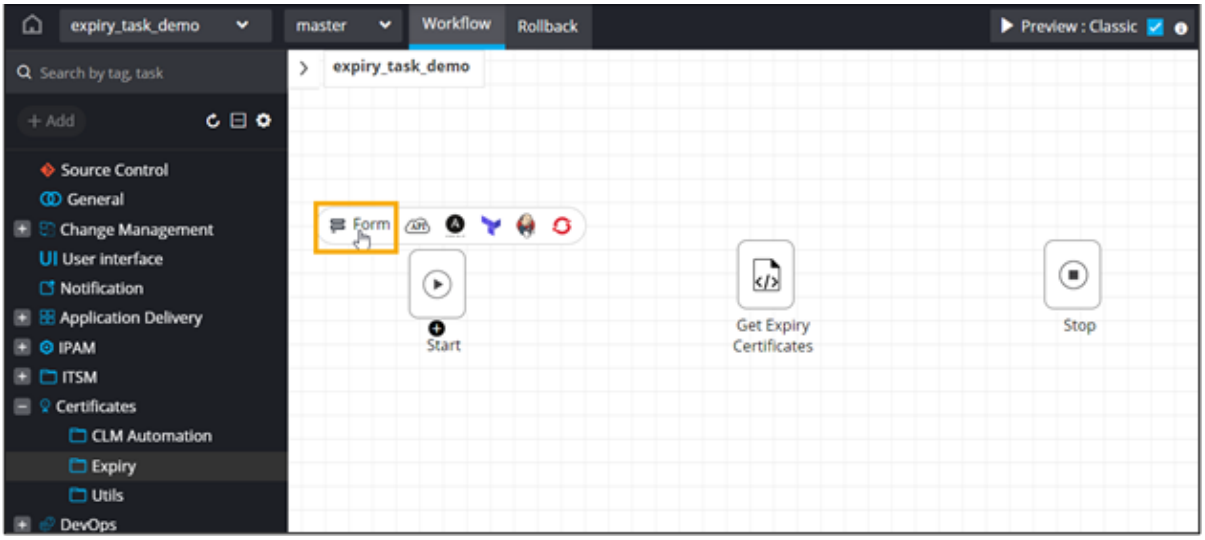


This task can be used to generate a report listing certificates due to expire in a specific number of days.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

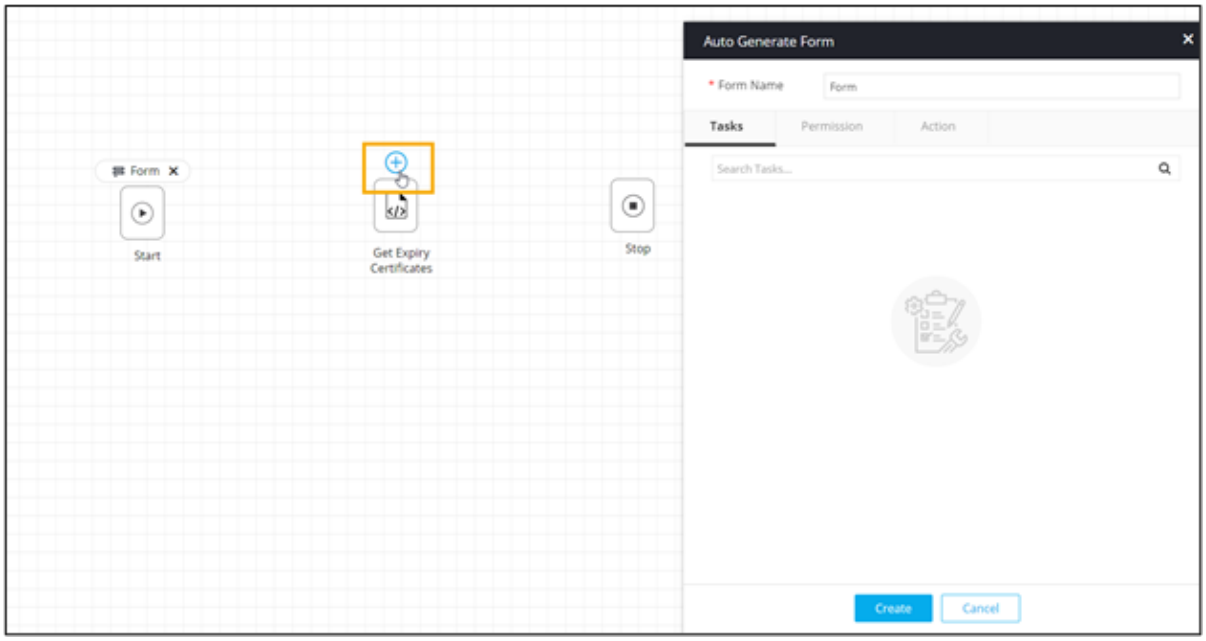


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.



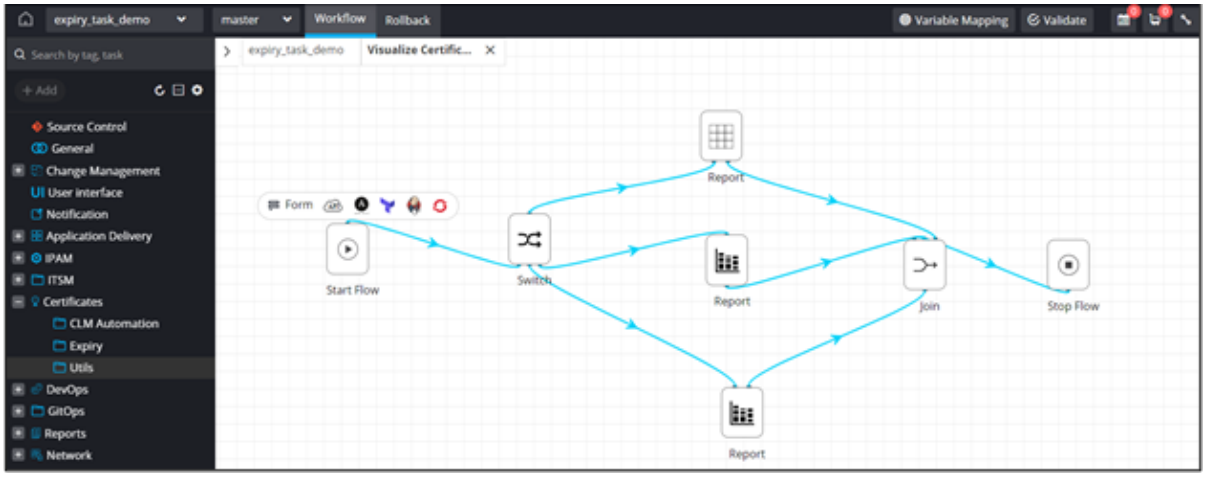
5. Click ⊕ above the **Get Expiry Certificates** task to auto-populate the form fields.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Enter a **Form Name** and click **Create**.
8. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.

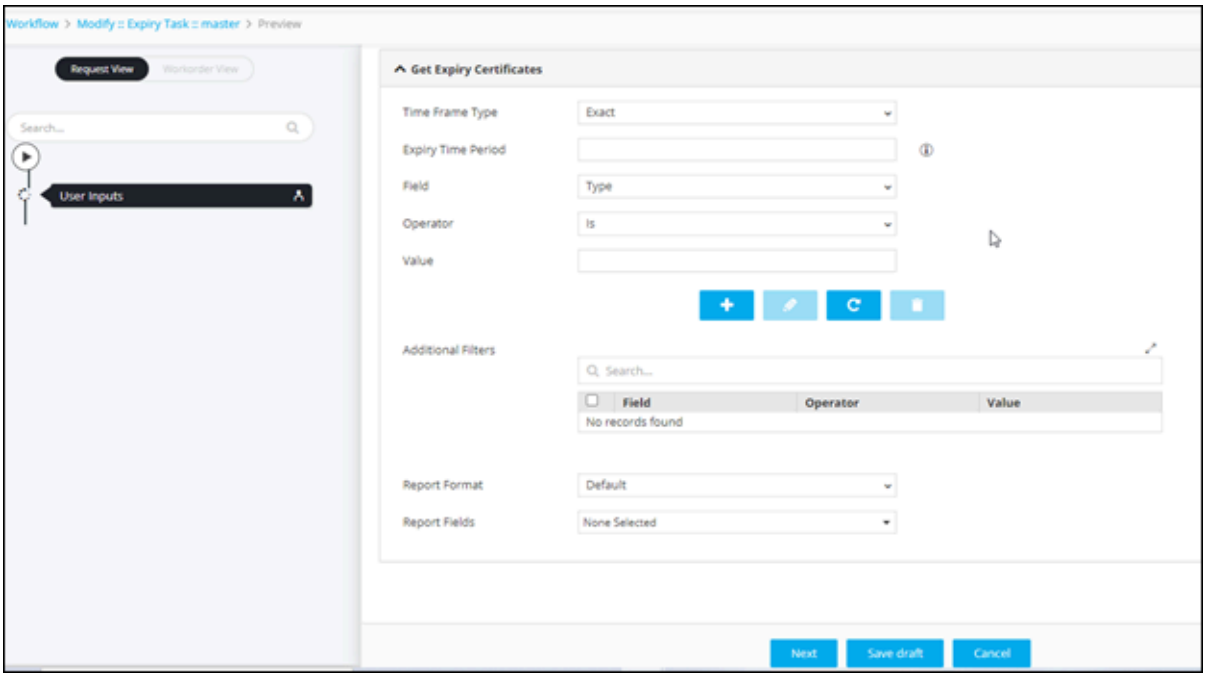
   This subflow includes **User Interface** tasks such as **Grid** and **Chart** (Pie chart and Stacked bar chart). The report generated will be displayed as a grid or a chart based on the inputs provided in the input form.



9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

   User Inputs form is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for User Inputs form

Field	Description
Time Frame Type	Enter the time frame type from the available options: • **Exact** - Allows you to enter the exact value for the expiry time period (30 days). • **Range** - Allows you to give a range for the expiry time period (0 - 30). **Note: Exact** is the default selection.
Expiry Time Period	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Field	Select the field from the options available in the dropdown.
Operator	Select the conditional operator: • **Is** • **Is Not**
Value	Enter a valid value for filtering the certificates.

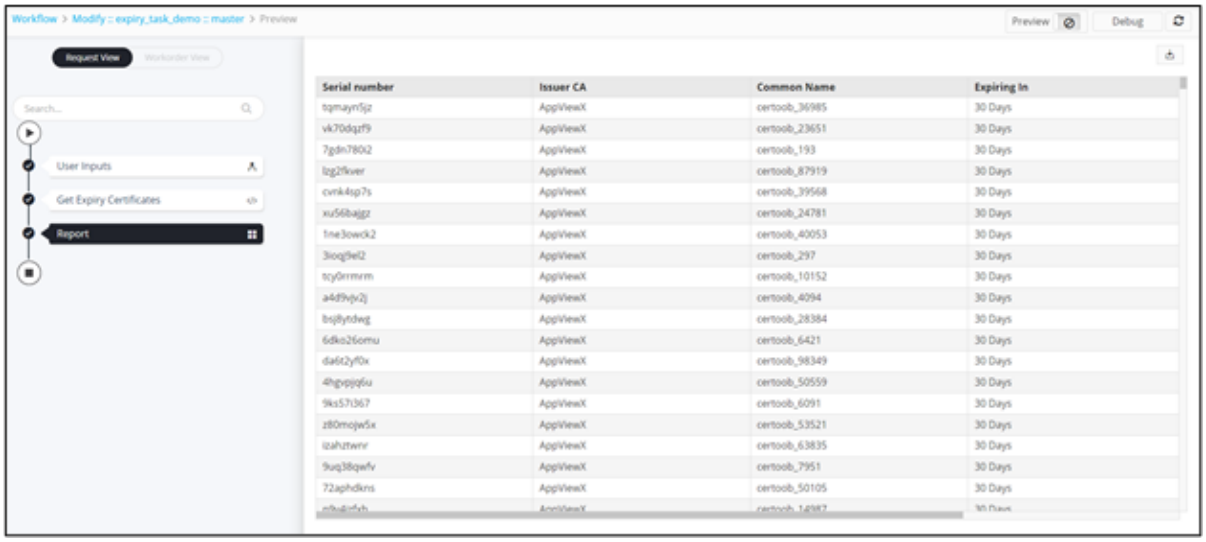
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Additional Filters	This grid displays the values selected in these fields: • **Field** • **Operator** • **Value** **Note:** The steps to apply these additional filters are given below the table.
Report Format	Select the format in which the report is displayed from the available options: • **Default** • **Pie Bar Chart** • **Stacked/Bar Chart**
Report Fields	Select the fields to be displayed in the report from the options available in the dropdown.

10. To add filters to the **Additional Filters** grid, click 
11. To edit the value of a particular filter, select the filter in the grid and click  .
12. Enter the new value(s) for the filters (Field/Operator/Value) and click  again to update the value(s).
13. To delete a filter, select the filter in the grid and click  .
14. To maximize the **Additional Filters** grid, from the top right corner of the grid, click  .
15. Click **Next**.

    Report is generated with expiry certificates data displayed in Grid format.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

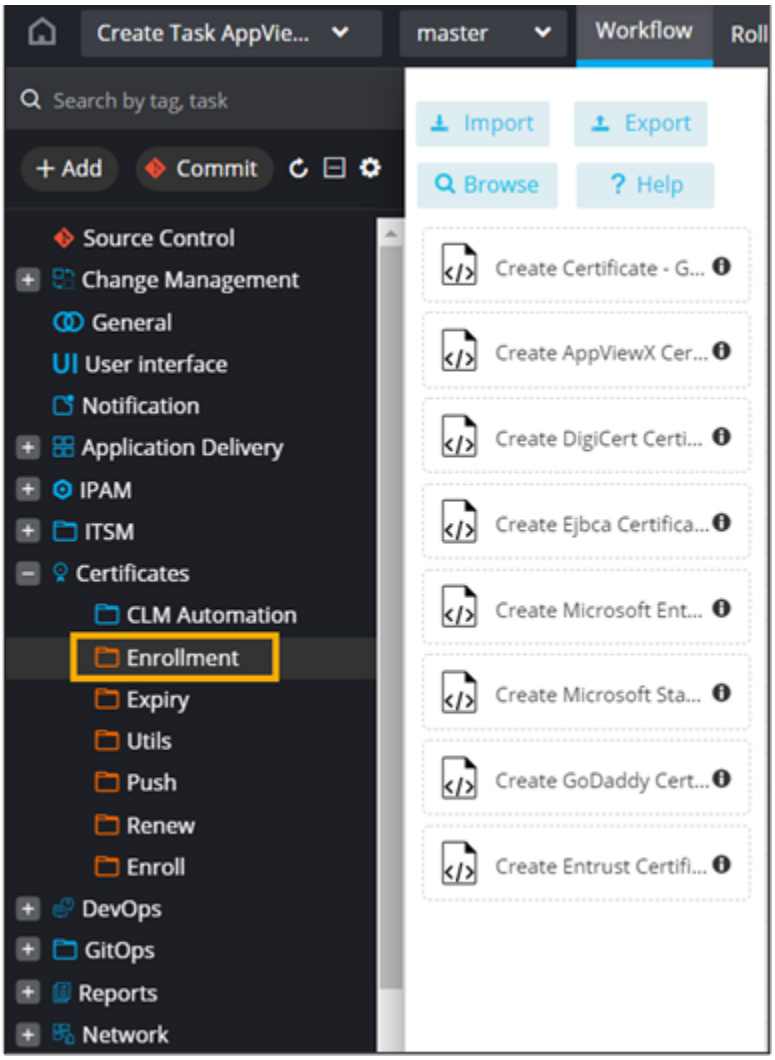


Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Enrollment Tasks

You can design a custom workflow for enrolling a certificate using the prebuilt Create Certificate tasks available in the **Workflow Studio**. The OOB script task for enrolling certificates through different Certificate Authorities can be found under **Certificates**, in the **Enrollment** folder.

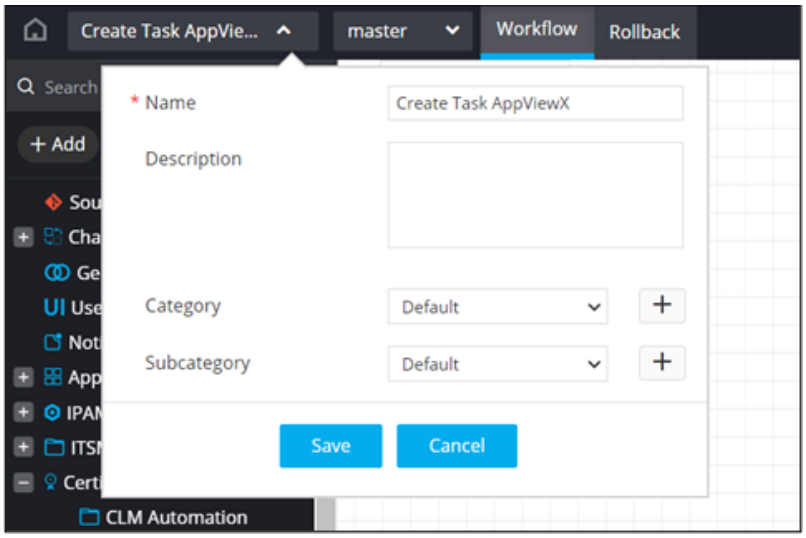
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



To design a custom workflow using **Enrollment** tasks:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

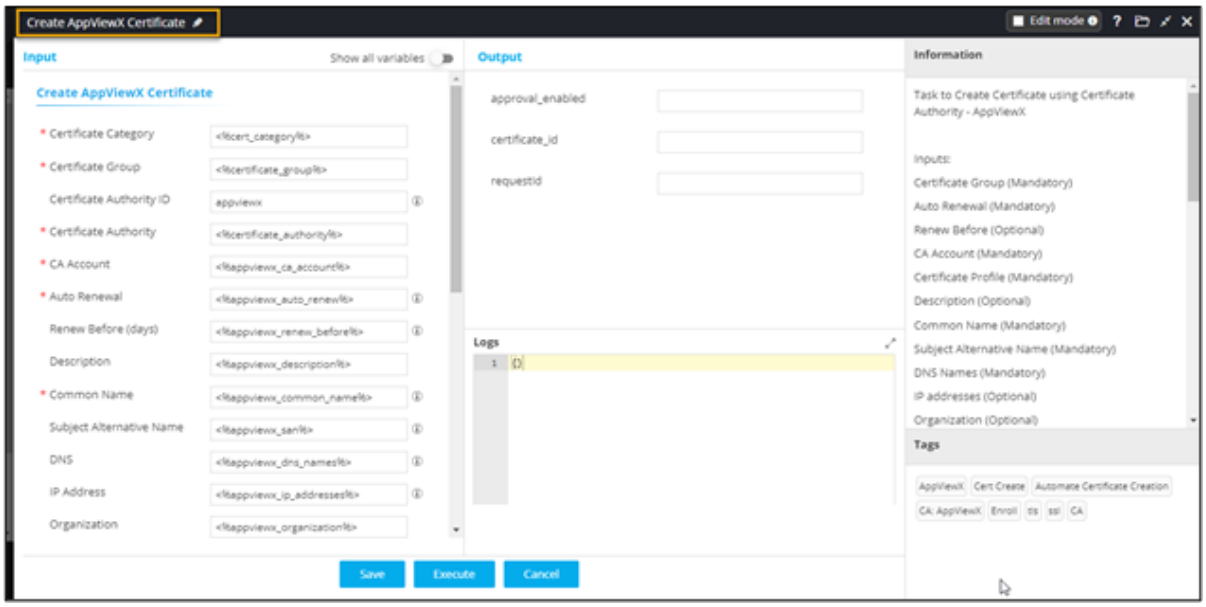


3. From the **Certificates** folder, click **Enrollment**.

   The tasks for the following CAs are available in the **Enrollment** folder:

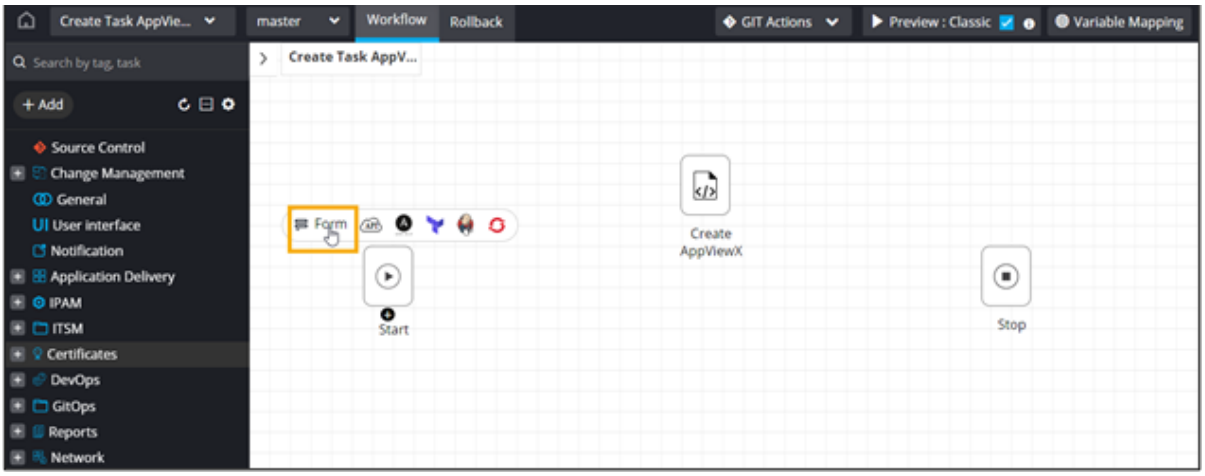
   - Appviewx
   - DigiCert
   - EJBCA
   - Entrust
   - Microsoft Enterprise
   - Microsoft Standalone
   - GoDaddy

4. From the **Enrollment** folder, drag and drop any of the Create Certificate tasks. For example, the **Create AppViewX Certificate** task.

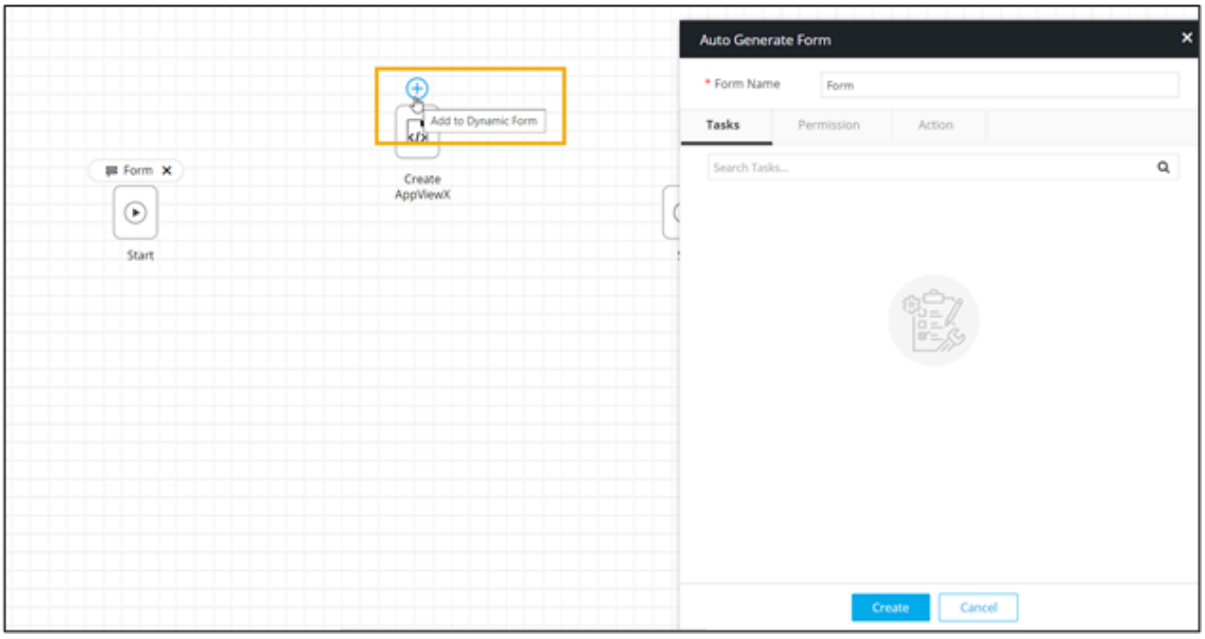


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. Click **Save**.
6. To auto-generate a form for this workflow, click **Form** above the **Start** task.

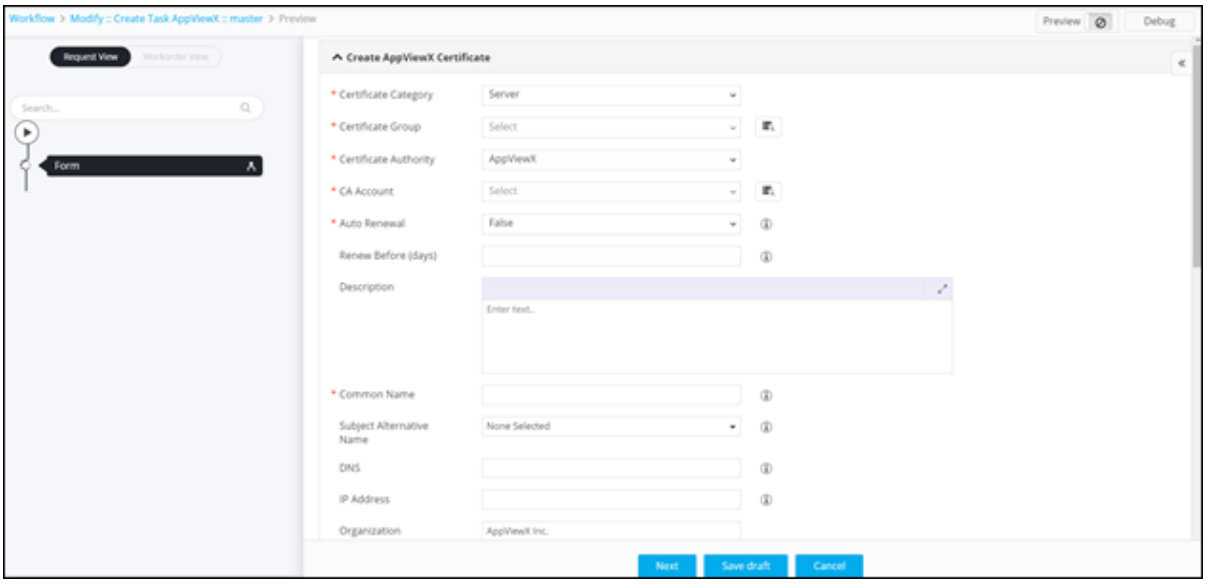


7. Click ⊕ above the **Create AppViewX** task to auto-populate the form fields.



8. Select the fields required in the input form.
9. Enter a **Form Name** and click **Create**.
10. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.
11. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.
    User Inputs form, when the **Create AppViewX Certificate** task is selected, is displayed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Field Description for the User Inputs form

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the **Certificate Group** field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the **CA Account** field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Renew Before (days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date.

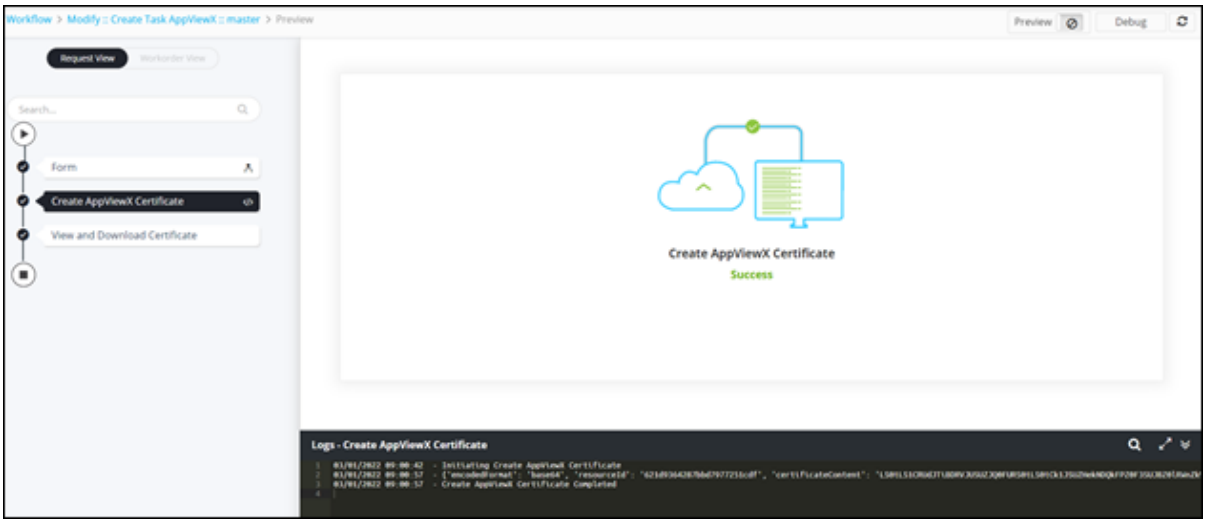
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter the Email Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Enter the challenge password.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

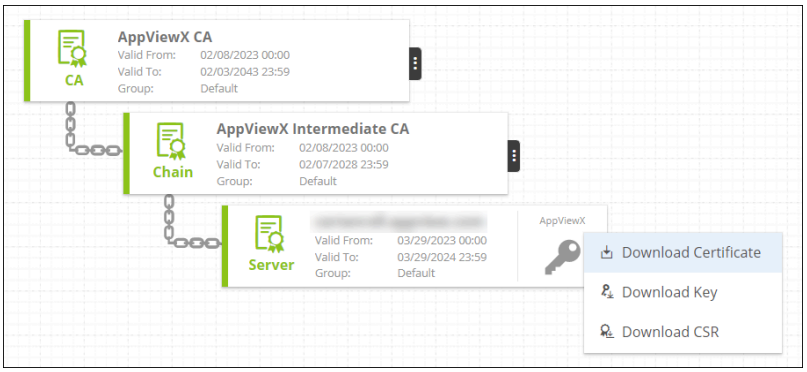
Field	Description
	Note: To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All asterisk (*) marked fields are mandatory.	

12. To add the attribute to the **Certificate Attributes** grid, click .
13. To edit the value of a particular attribute, select the attribute in the grid and click .
14. Enter the new value for the attribute in the **Value** field and click again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.
    AppViewX Certificate is created.

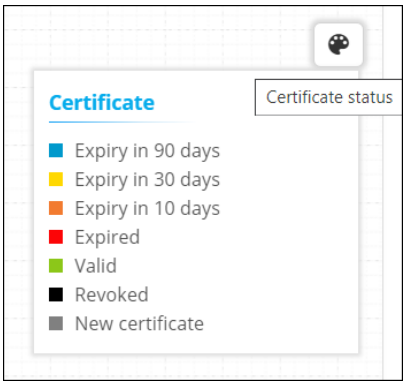


19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



20. Hover your mouse over  to view the **Certificate status**.



Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Renew Tasks

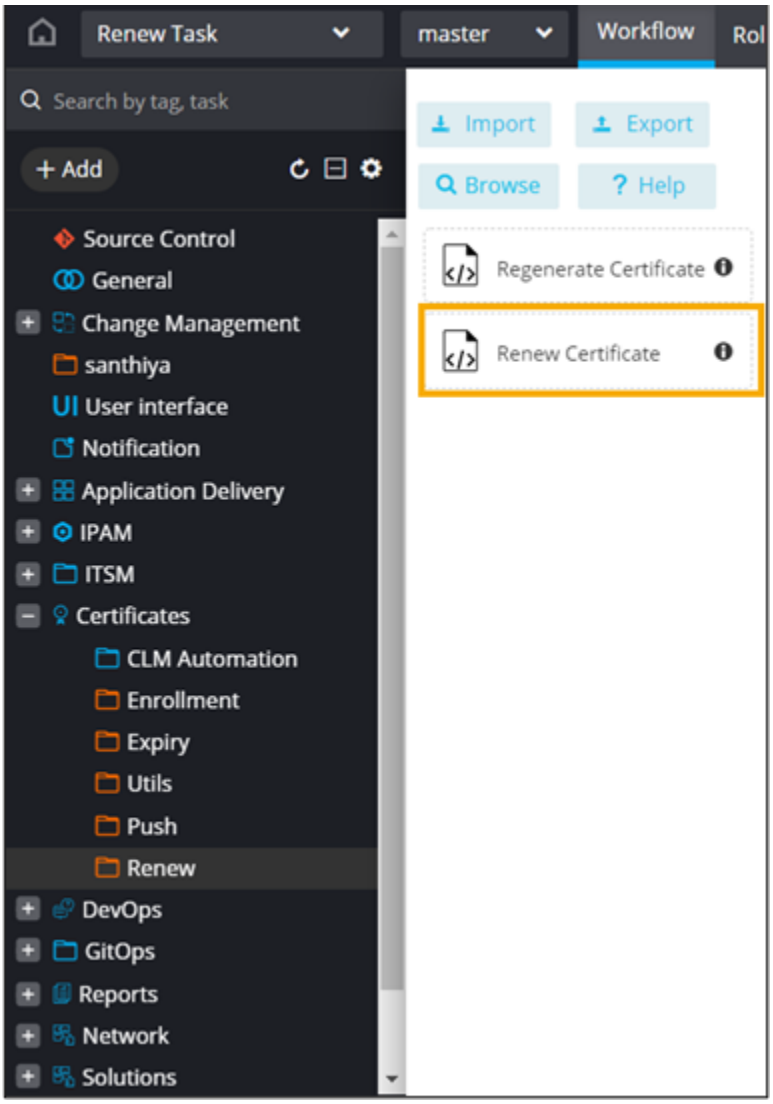
This section describes the **Renew** and **Regenerate** tasks that can be integrated with custom workflows to renew and regenerate certificates.

- Renew Task
- Regenerate Task

Renew Task

The OOB script task for renewing certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.

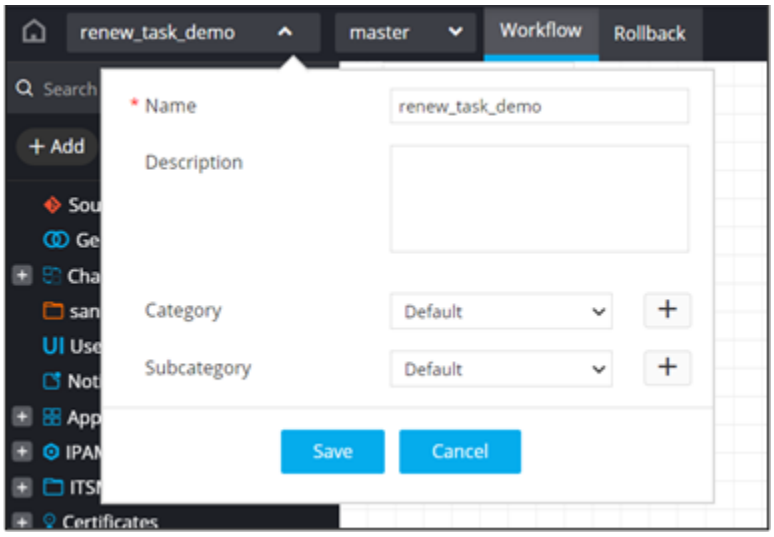
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



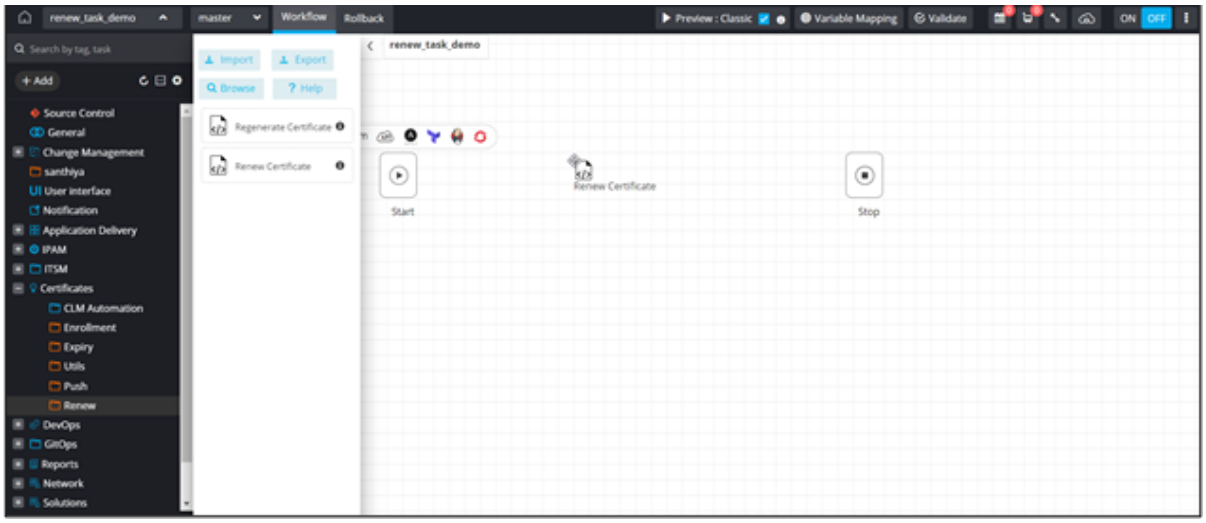
To design a custom workflow using the **Renew** task:

1. Navigate to the WorkflowWorkflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

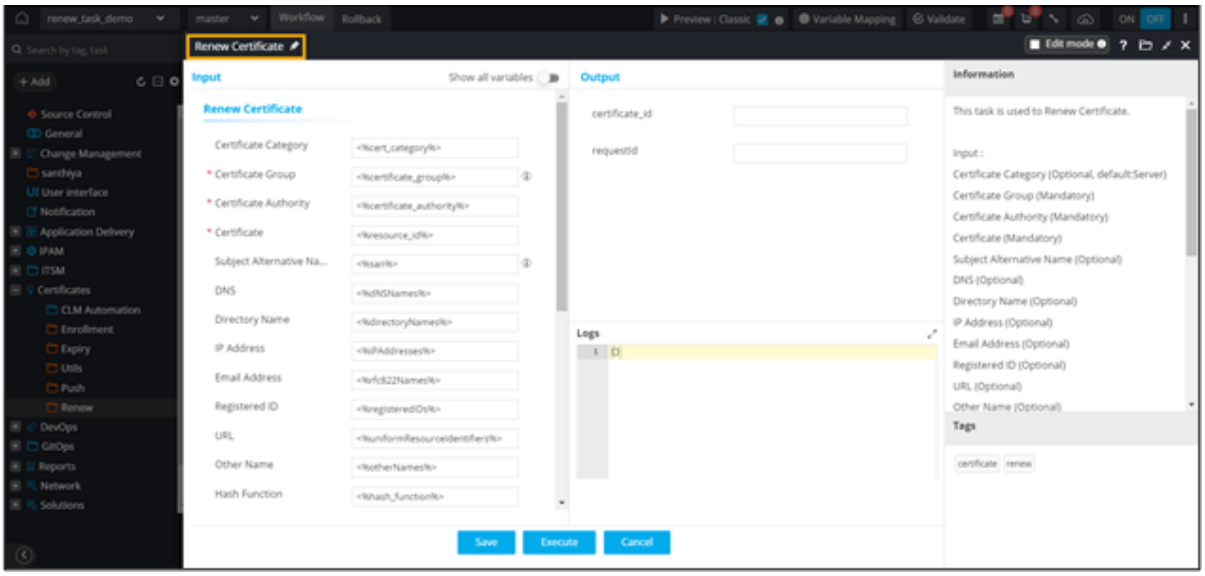


3. From the **Certificates** folder, under **Renew**, drag and drop the **Renew Certificate** task.

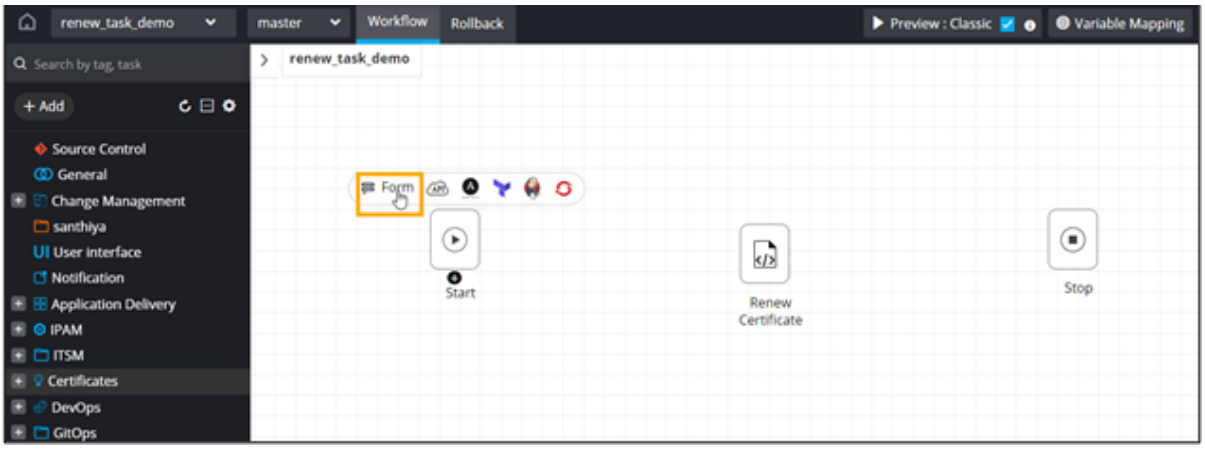


This task can be used to renew certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

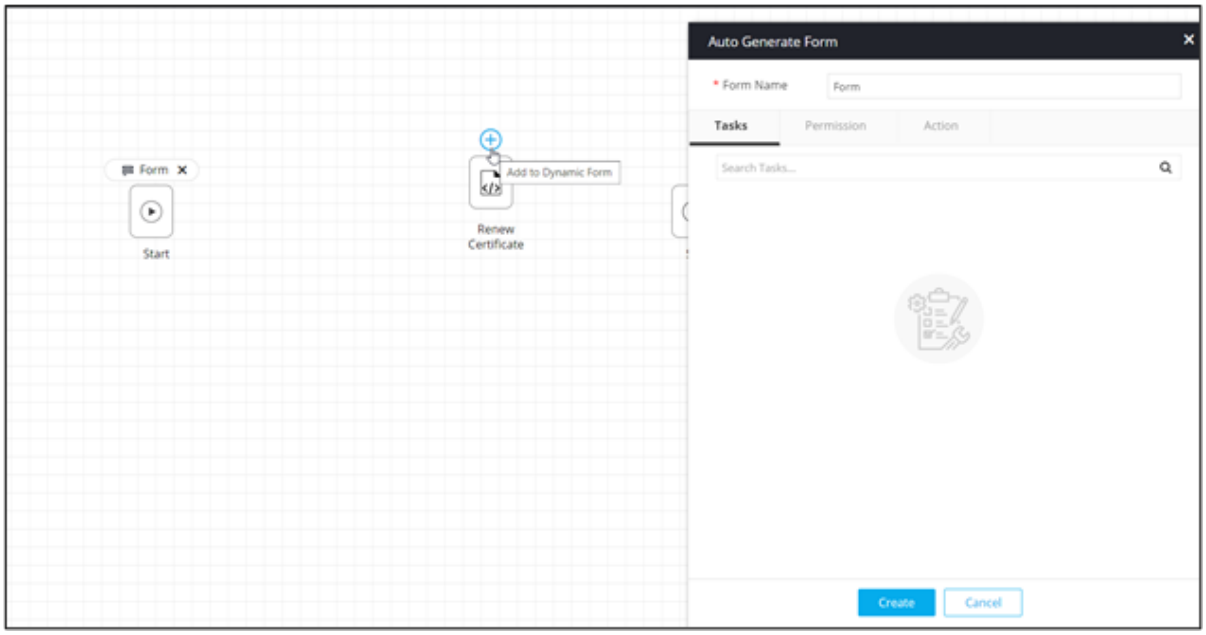


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.



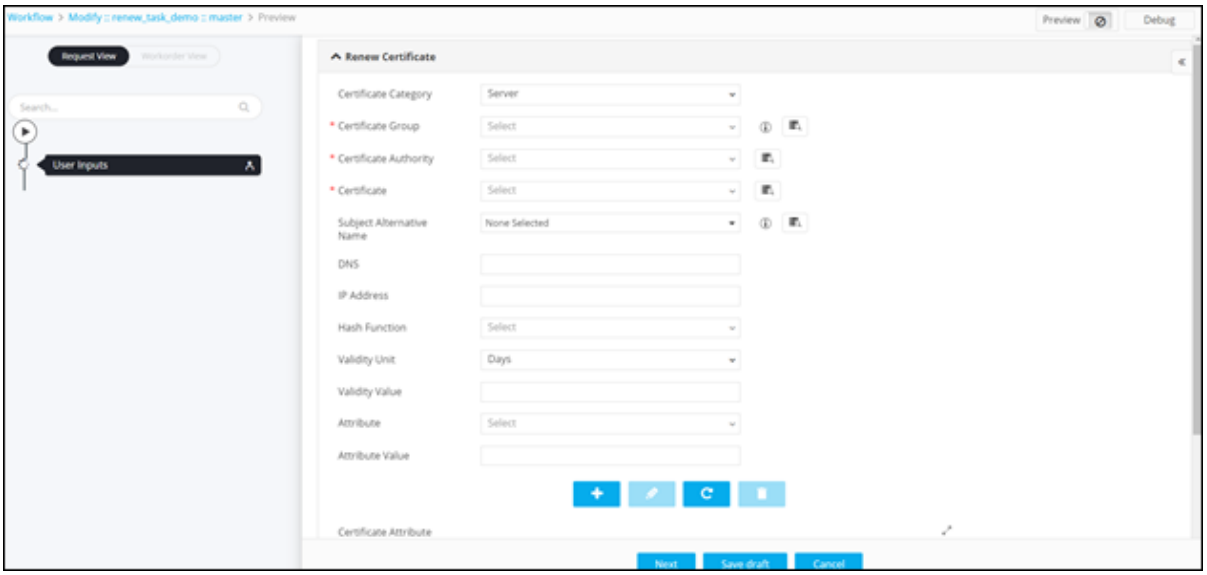
5. Click ⊕ above the **Renew Certificates** task to auto-populate the form fields.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Provide a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

   The **User Inputs** form is displayed on the screen.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

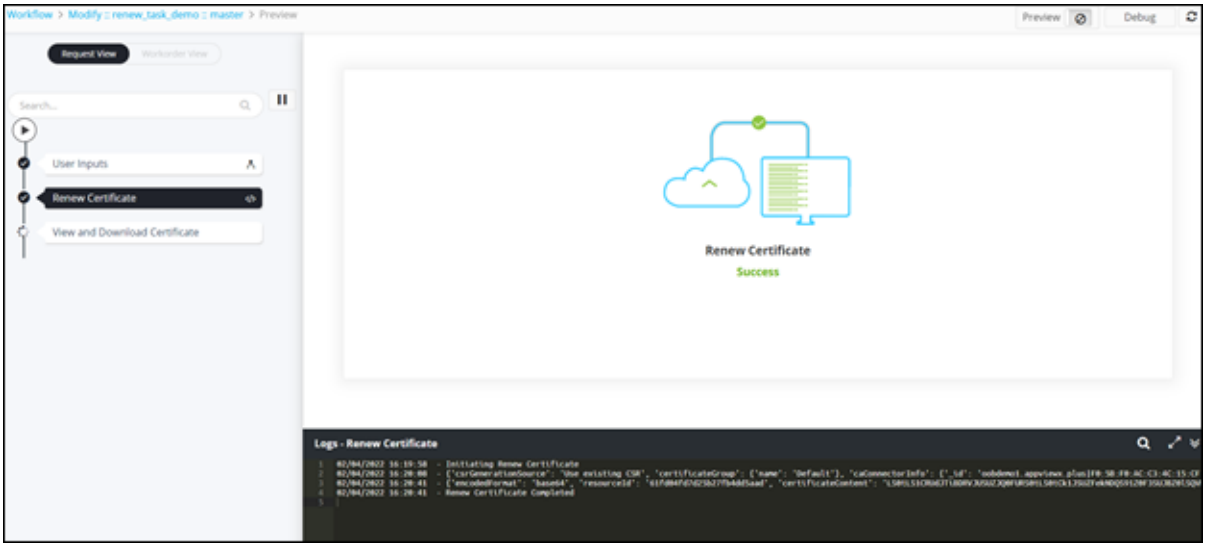
Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
Validity Unit	Select the **Validity Unit** from the options available in the dropdown.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Validity Value	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

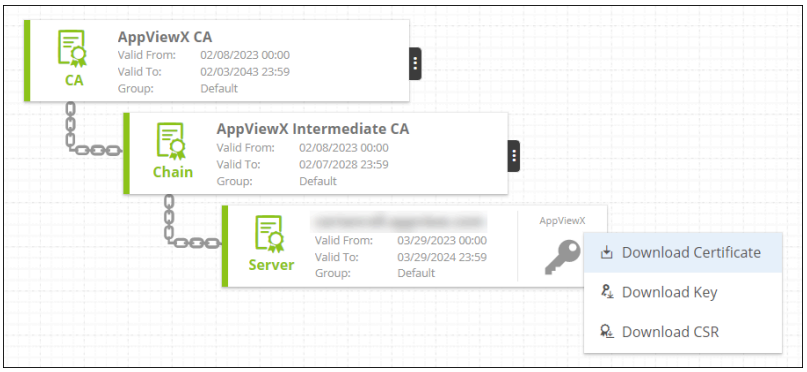
10. To add this attribute to the **Certificate Attributes** grid, click  .
11. To edit the value of a particular attribute, select the attribute in the grid and click  .
12. Enter the new value for the attribute in the **Value** field and click  again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click  .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Click **Next**.

    Certificate renewed successfully.

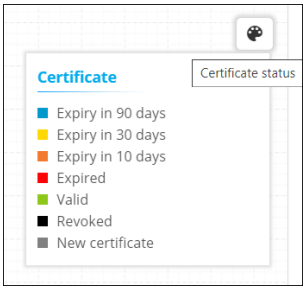


17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



18. Hover your mouse over to view the **Certificate status**.



19. Click on the renewed certificate to view the **Certificate Details**.

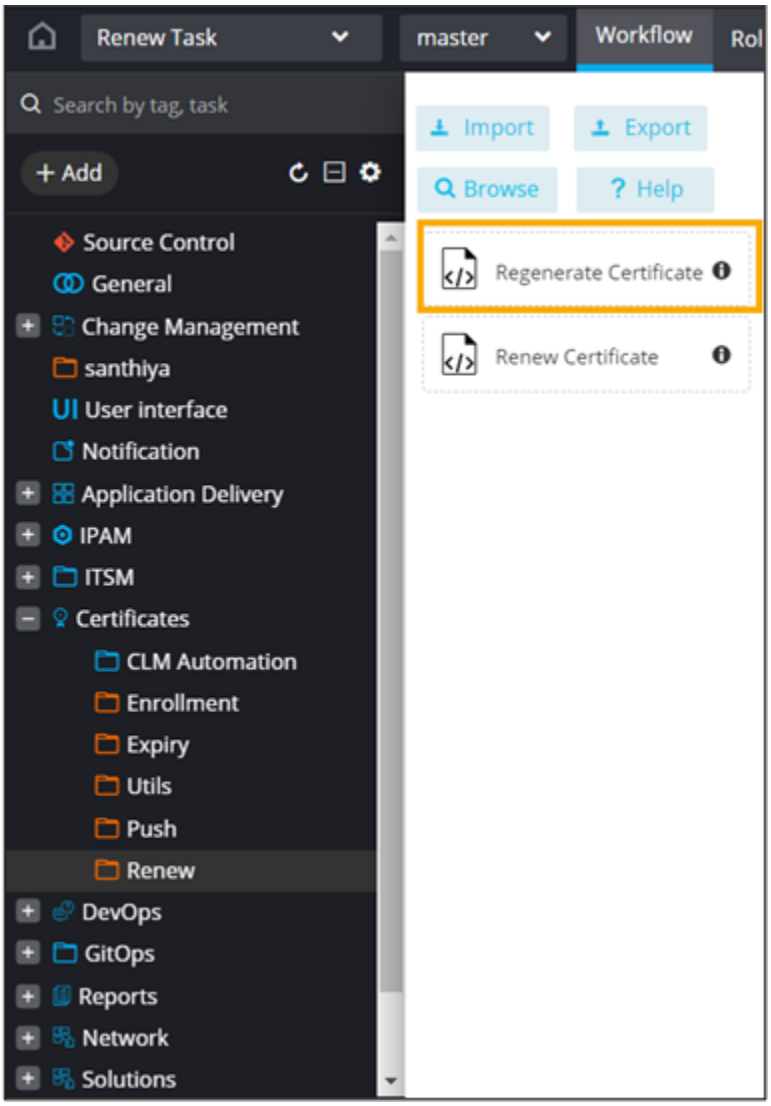


Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Regenerate Task

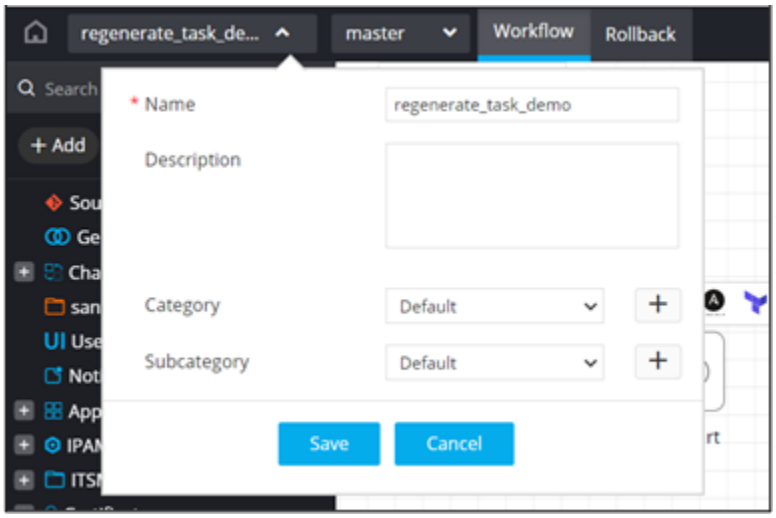
The OOB script task for regenerating certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.



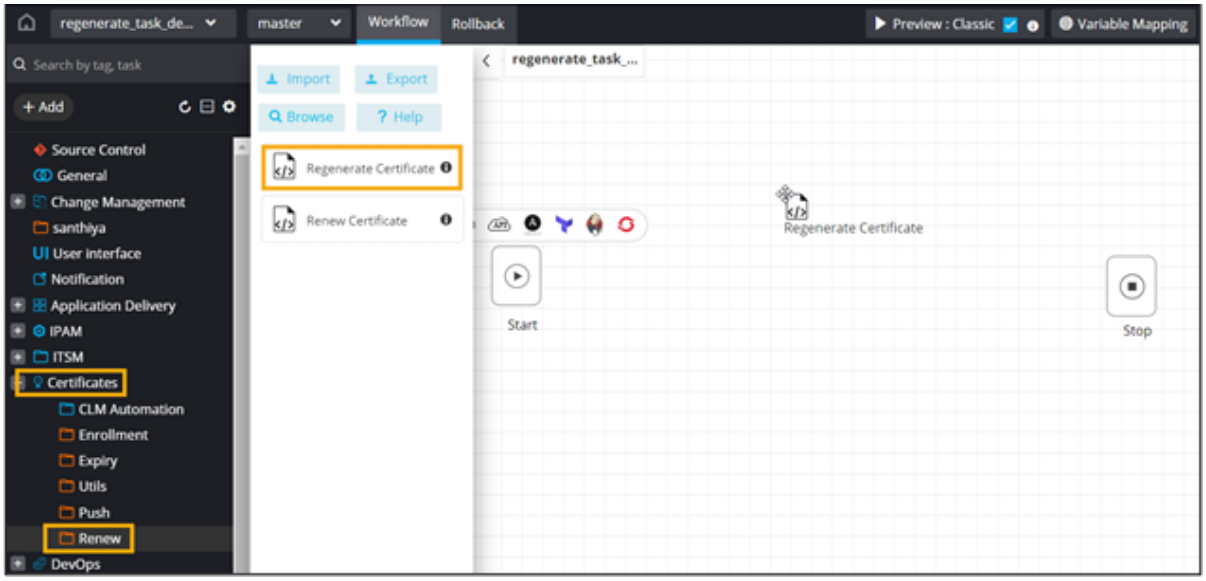
To design a custom workflow using the **Regenerate** task:

1. Navigate to the WorkflowWorkflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

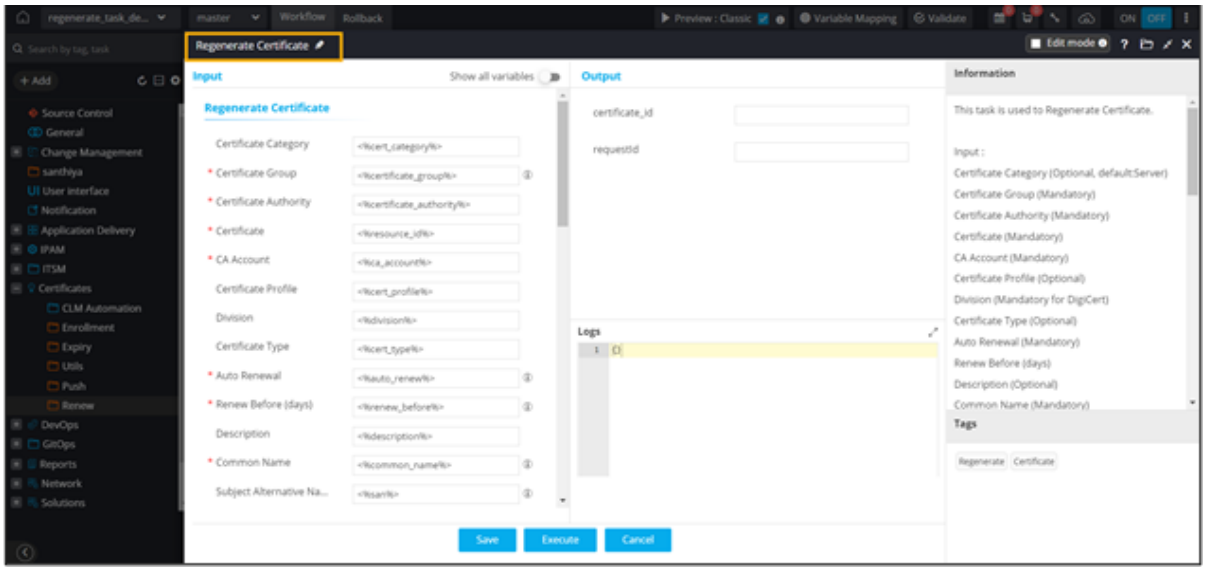


3. From the **Certificates** folder, under **Renew**, drag and drop the **Regenerate Certificate** task.

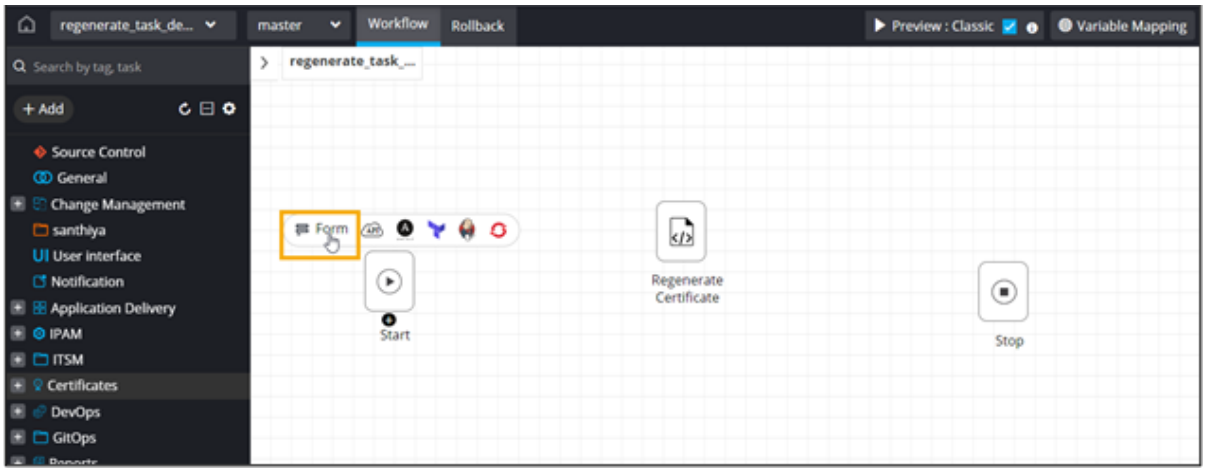


This task can be used to regenerate certificates.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

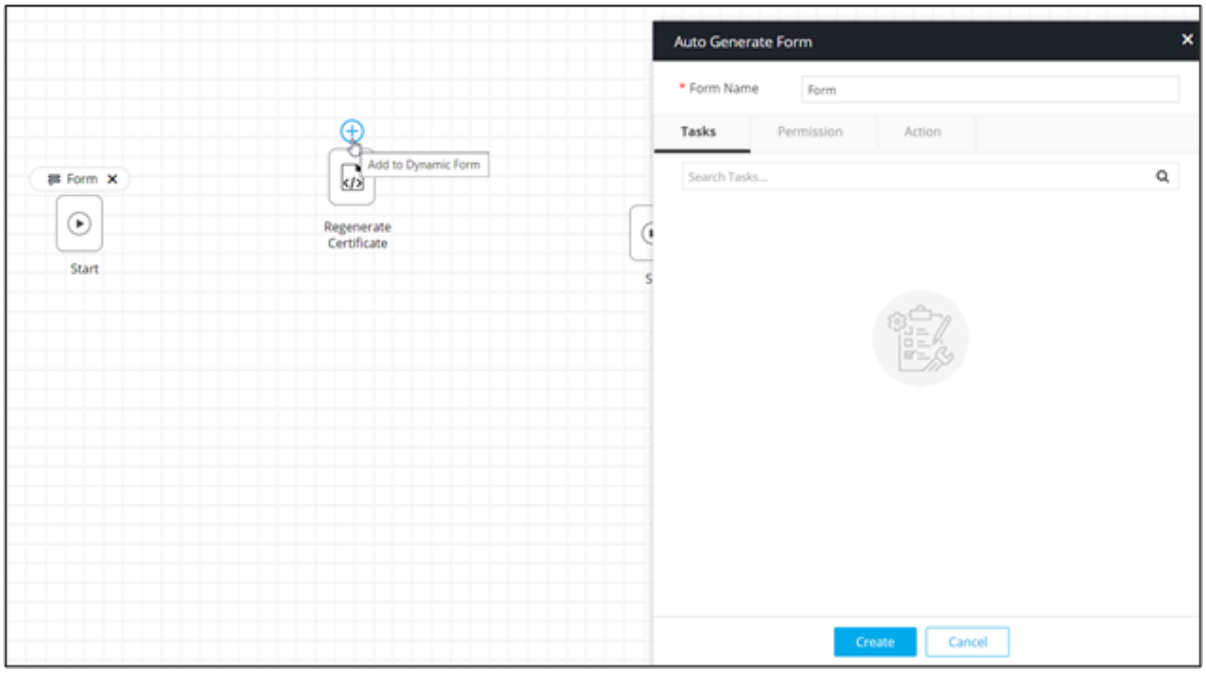


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.

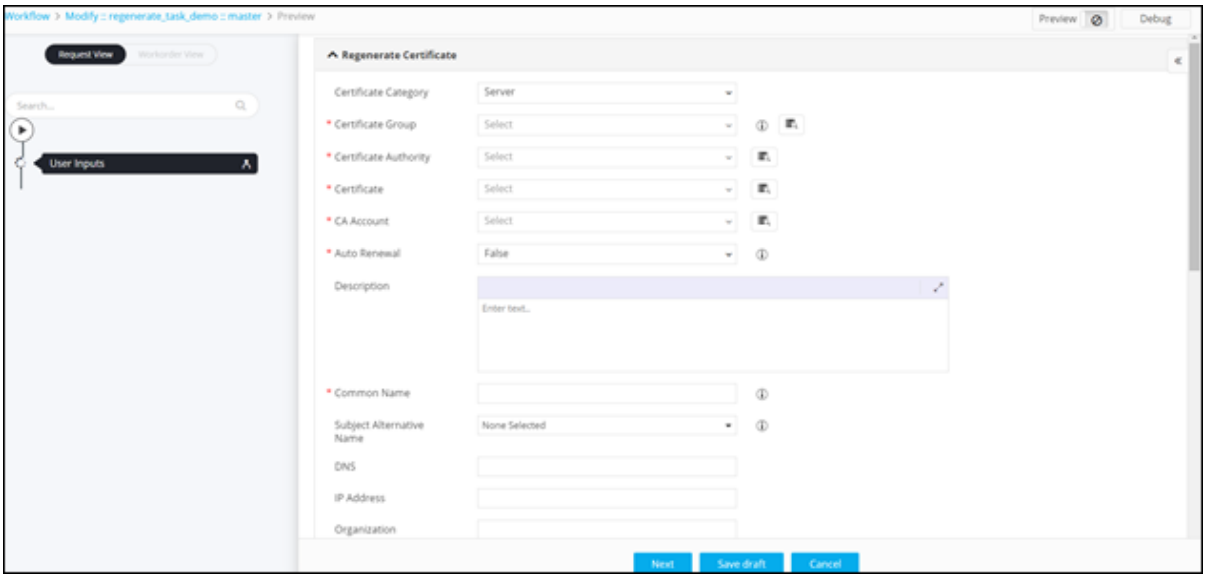


5. Click ⊕ above the **Regenerate Certificates** task to auto-populate the form fields.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Enter a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.
   The **User Inputs** form is displayed on the screen.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the CA Account field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Description	Provide a description for the regenerated certificate.
***Common Name**	This field is populated on the basis of the certificate selected.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
City	Enter the name of the city in which the organization is located.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the organization.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type**from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** To retrieve the values in the Bit Length field, click .
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

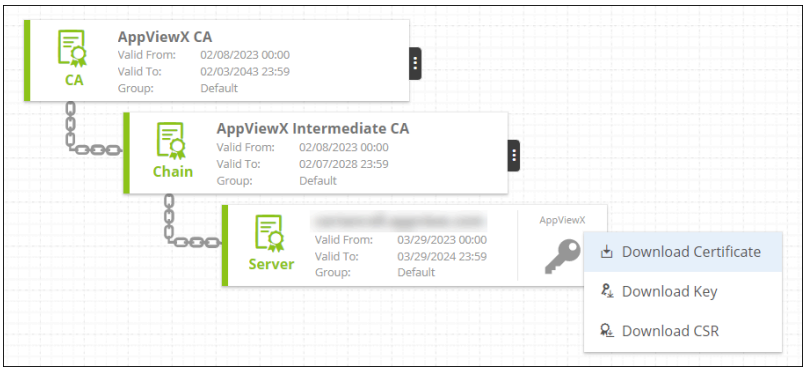
10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

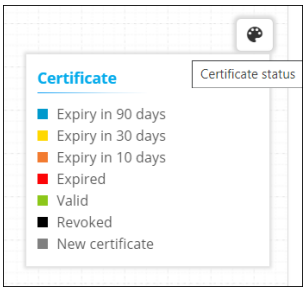
16. Click **Next**.

    Certificate is regenerated successfully.

17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



18. Hover your mouse over 🎨 to view the **Certificate status**.



19. Click on the regenerated certificate to view the **Certificate Details**.

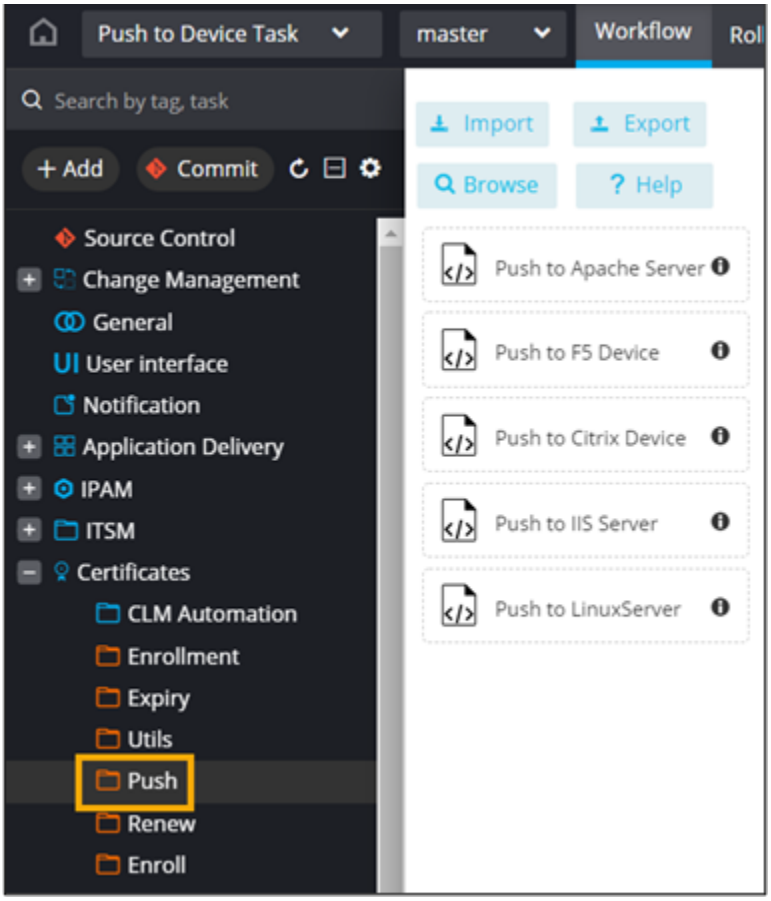


Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

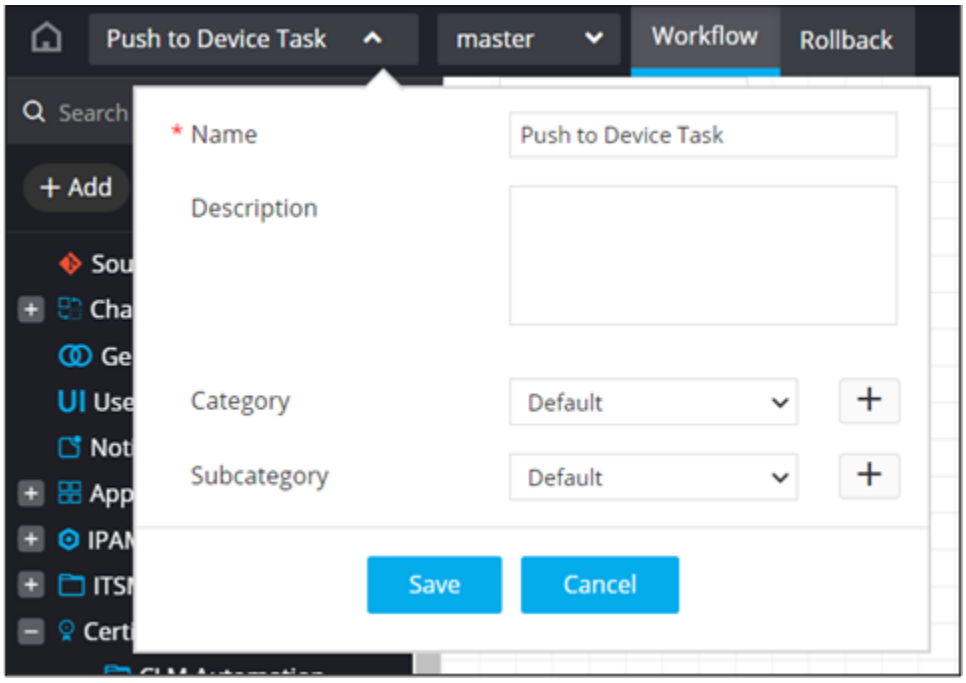
Push Tasks

You can design a custom workflow for pushing a certificate to a device(s) or a server(s) using the prebuilt Push tasks available in the **Workflow Studio**. The OOB script task for pushing certificates to devices/ servers can be found under **Certificates**, in the **Push** folder.



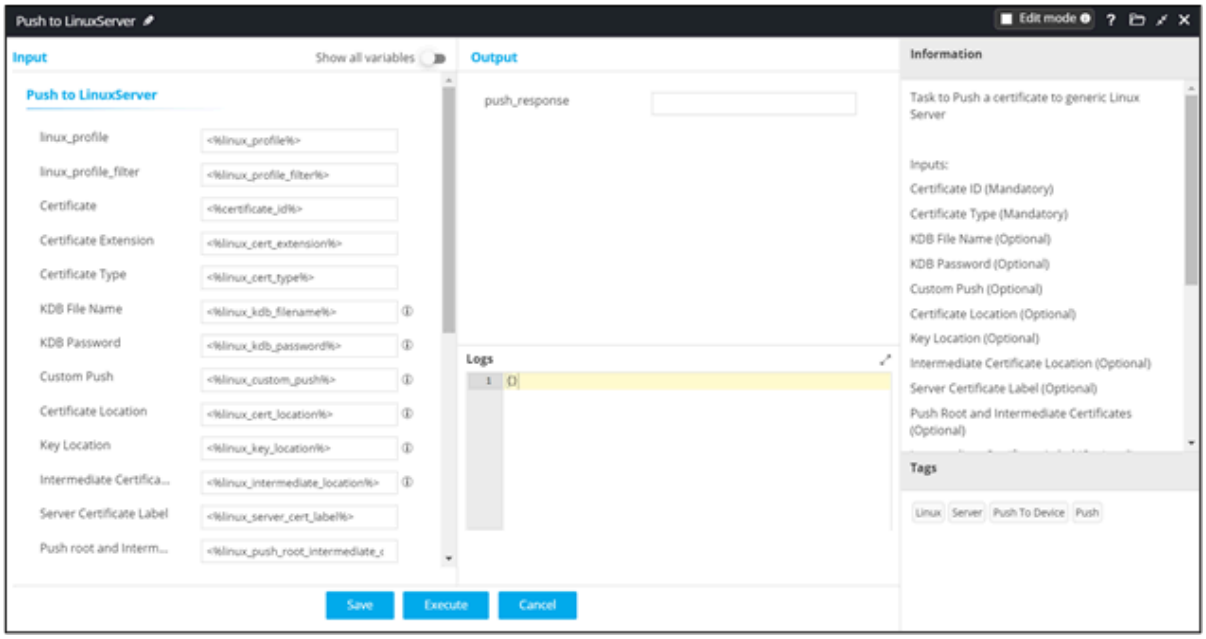
1. Navigate to the WorkflowWorkflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

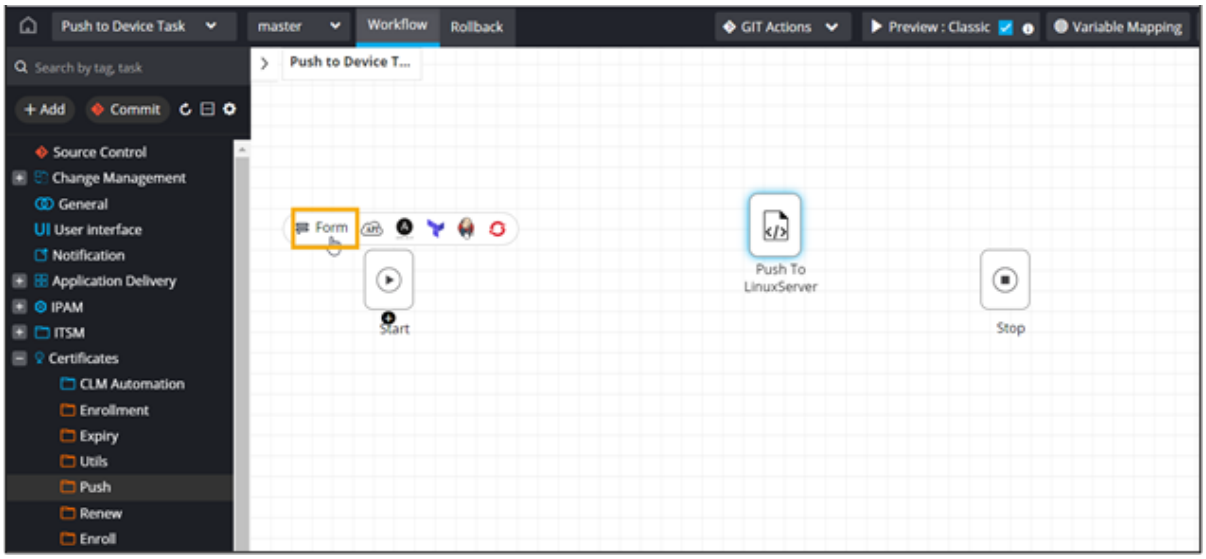


3. From the **Certificates** folder, click **Push**.
   The following tasks for pushing certificates are available in the **Push** folder:
   - Push to Apache Server
   - Push to F5 device
   - Push to Citrix Device
   - Push to IIS Server
   - Push to Linux Server
4. From the **Push** folder, drag and drop any of the Push tasks. For example, the **Push to Linux Server** task.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

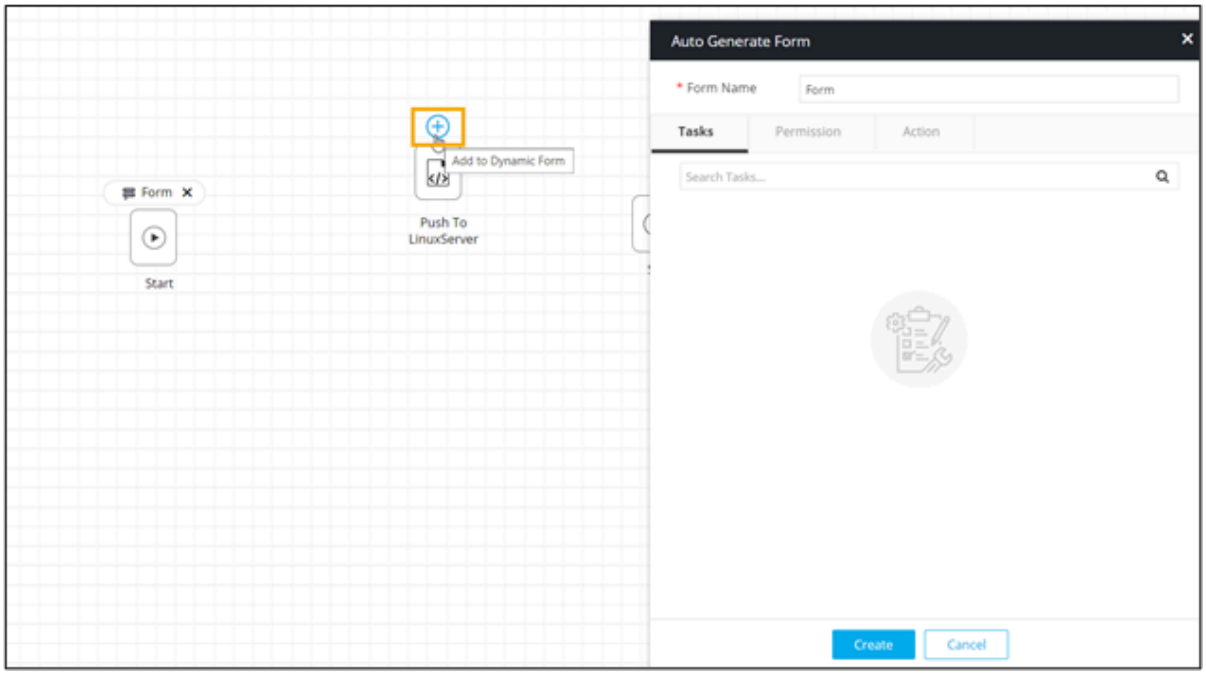


5. Click **Save**.
6. To auto-generate a form for this workflow, click **Form** above the **Start** task.



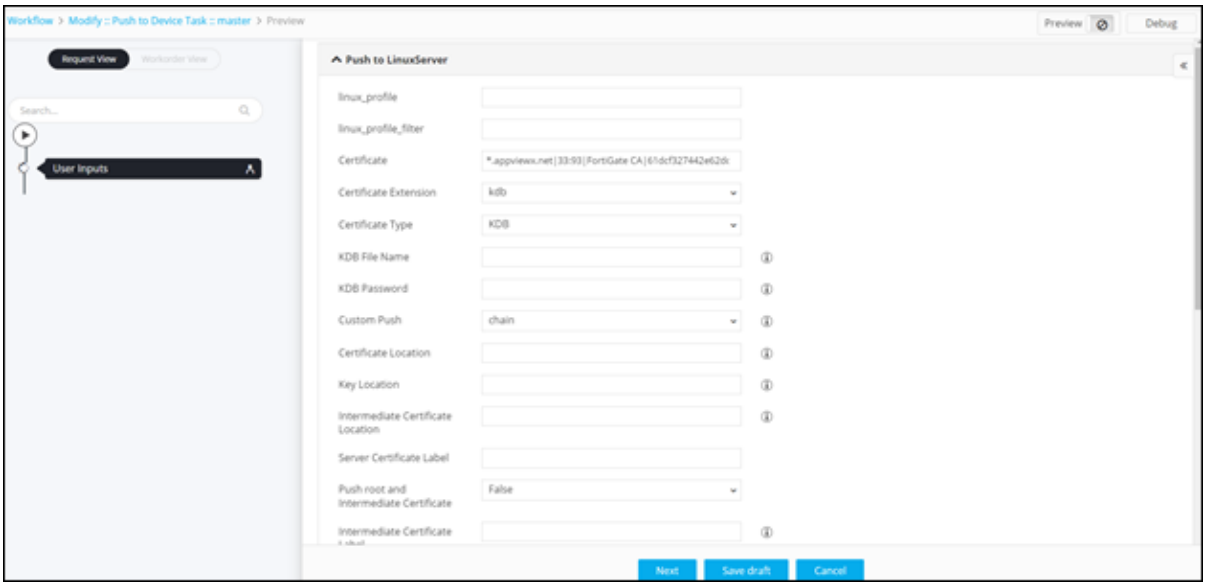
7. Click ⊕ above the **Push to LinuxServer** task to auto-populate the form fields.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



8. Select the fields required in the input form.
9. Provide a **Form Name** and click **Create**.
10. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.
11. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

    User Inputs form when the **Push to LinuxServer** task is selected is displayed.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: The fields displayed in the User Inputs form will vary depending on the Push task selected from the Push folder while designing the workflow.

Field Description for the User Inputs form

Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note**: This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note**: Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note**: This field is displayed only when the **Auto Renewal** field is enabled.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter the Email Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown. **Note:** To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.

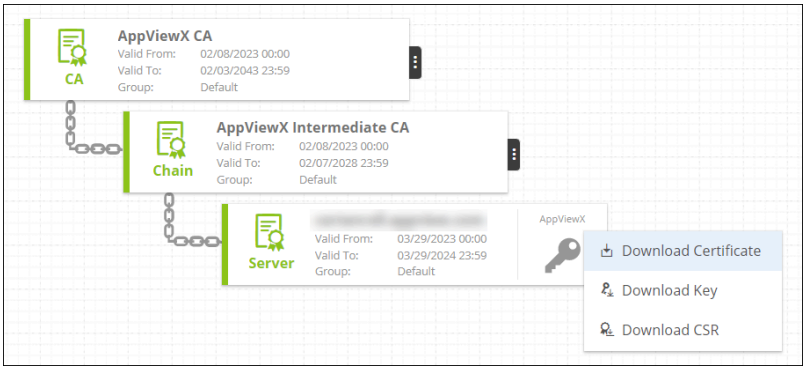
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
All Asterisk (*) marked fields are mandatory.	

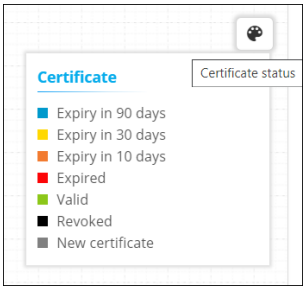
12. To add this attribute to the **Certificate Attributes** grid, click  .
13. To edit the value of a particular attribute, select the attribute in the grid and click  .
14. Enter the new value for the attribute in the **Value** field and click  again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click  .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.

    Certificate created successfully.

19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



20. Hover your mouse over  to view the **Certificate status**.



Note: For more information on how to design custom workflows, refer to the Automation User Guide.

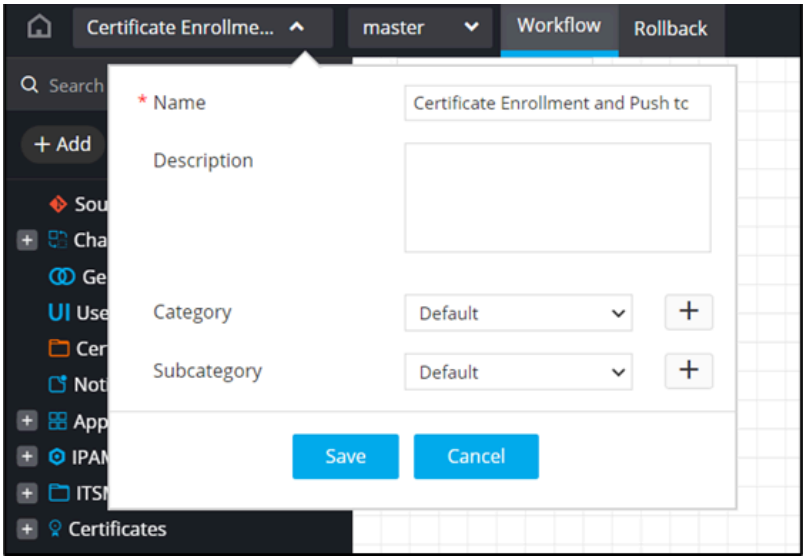
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Designing a Custom Workflow using OOB Tasks

You can use the OOB tasks and subflows available in the Automation module to build custom workflows for enrolling and renewing certificates. You can also add the OOB Push to Device subflow to push the certificates to a selected device.

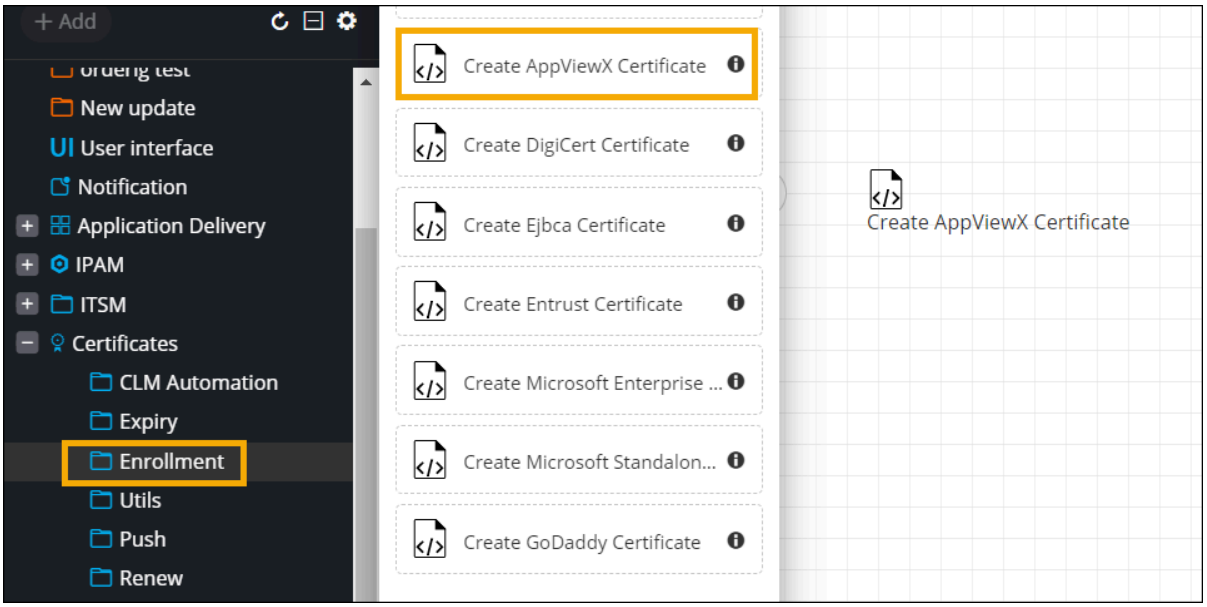
To design a custom workflow to enroll a certificate and push it to a device:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

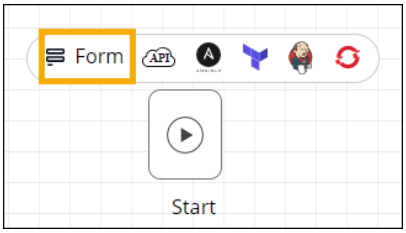


3. To access the OOB workflow tasks, from the left menu, click **Certificates**.
4. Under **Certificates**, from the **Enrollment** folder, drag and drop the required OOB task for enrolling a certificate, for example, the **Create AppViewX Certificate** task.

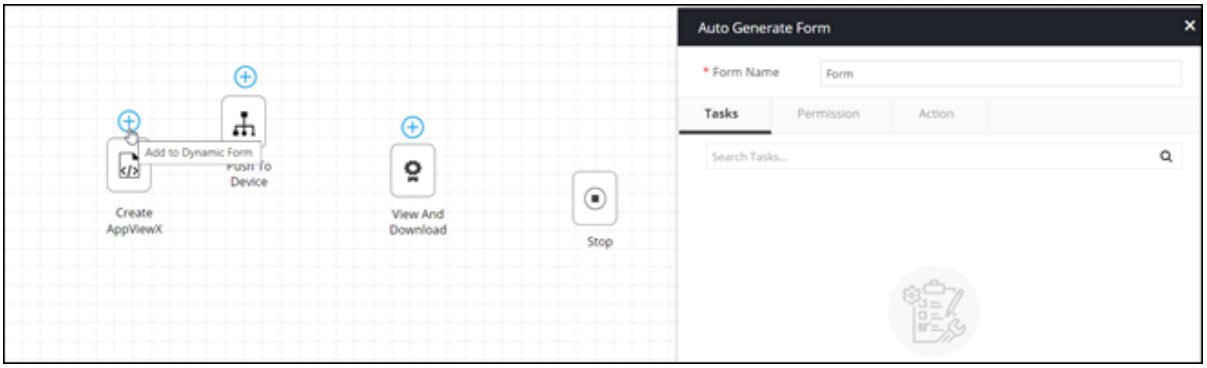
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



5. Click **Save**.
6. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **Push to Device** subflow.
7. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **View and Download Certificate** task.
8. To generate a form for this workflow, click **Form** above the **Start** task.



9. Click ⊕ above the **Create AppViewX Certificate** task to auto-populate the form fields.



10. Connect all workflow tasks and enable the workflow.
11. Trigger the workflow from the Request :: View/Run page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The workflow execution page is displayed with the workflow inputs requested at the first stage.

Field Description for the User Inputs form

Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note:** Server is the default selection. :
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**.

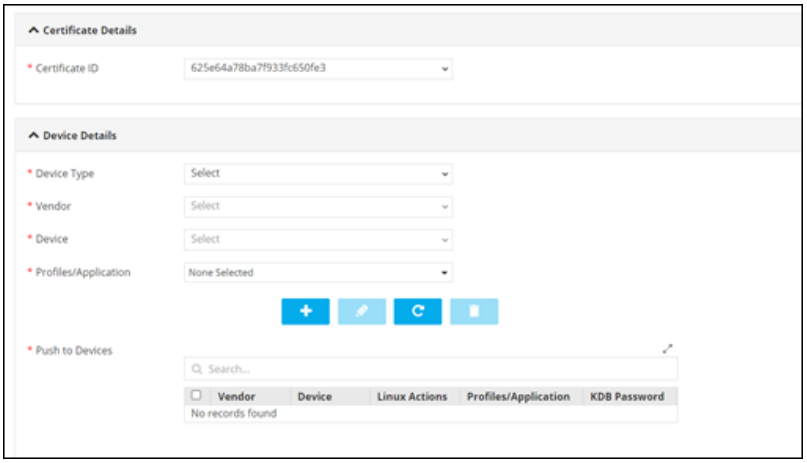
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
Description	Enter a description for the certificate to be created.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field	Description
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
Attribute	Select the **Attribute** from the available options.
Attribute Value	Enter a value for the selected attribute.
All Asterisk (*) marked fields are mandatory.	

12. To add this attribute to the **Certificate Attributes** grid, click .
13. To edit the value of a particular attribute, select the attribute in the grid and click .
14. Enter the new value for the attribute in the **Value** field and click again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.
    AppViewX Certificate is created successfully.
19. At the **Device Inputs** stage of workflow execution, under **Device Details**, select the requested field information as described in the table below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

This table describes the field information in this section:

Field Description for Device Details section

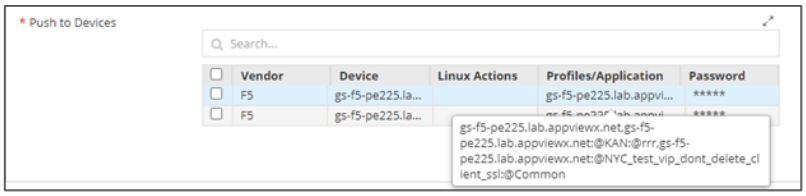
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

20. To add the selected profile/application to the grid, click  .

    The **Profile/Application** is added to the **Push to Devices** grid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

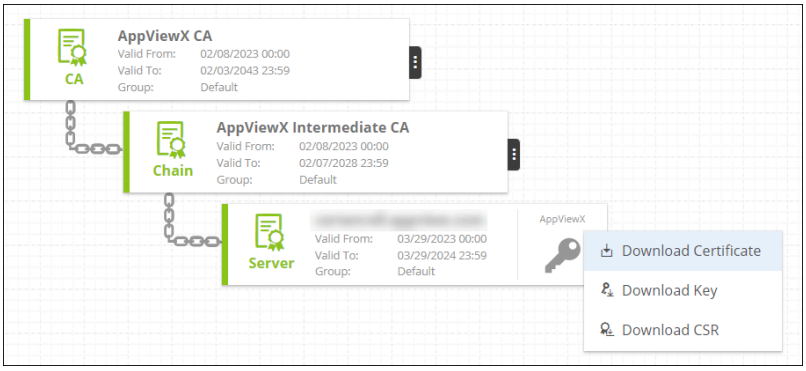
Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

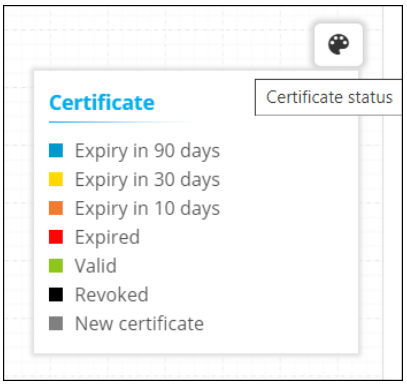
Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

21. Click **Submit**.
    Certificate is pushed to the selected device.
22. To download the certificate, at the **View | Download Certificate** stage of the workflow, hover your mouse over , and from the options displayed, click **Download Certificate**.



23. Hover your mouse over to view the Certificate status.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Note: For more information on how to design workflows, refer to the Automation User Guide.

Scheduling an OOB workflow

You can also schedule these OOB workflows to be triggered at specific time intervals (once or repeat daily, weekly, monthly, yearly) as per your requirement.

Note: For more information on scheduling workflows, refer to the Automation User Guide.

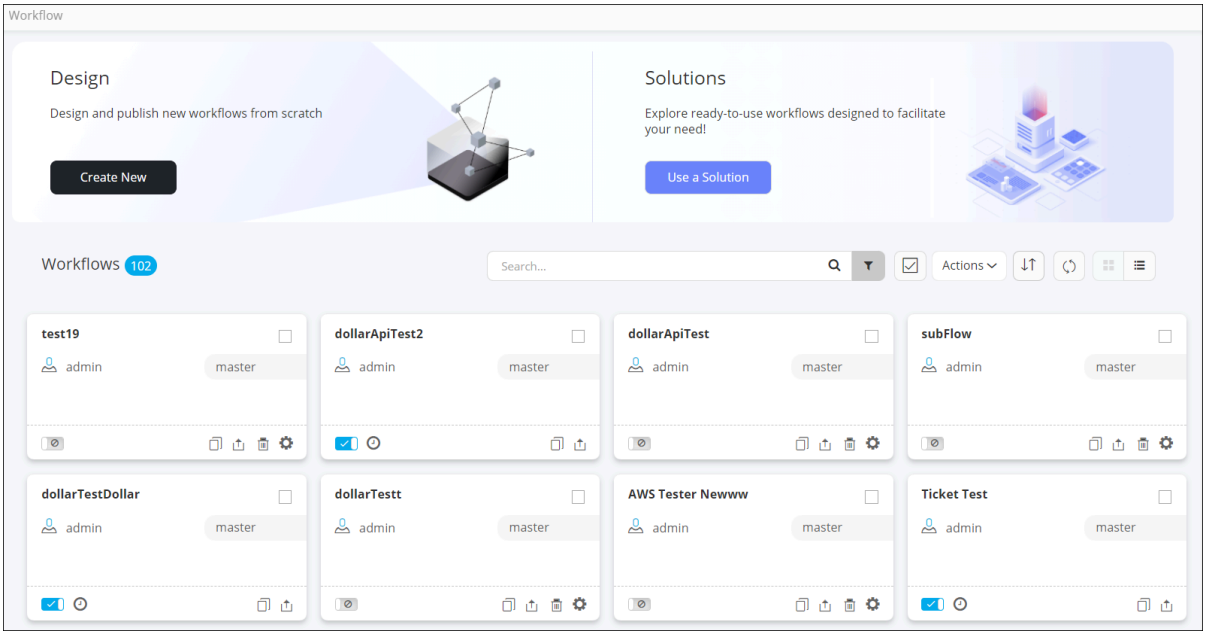
Customizing an OOB Workflow

You can customize any of these OOB workflows by modifying individual tasks within the workflow.

To customize a workflow:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Navigate to the **Workflow** page in the **Automation** module.



2. On the **Workflow** page, search for the workflow you want to customize by typing the keyword in the search bar.
3. Disable the workflow by turning off the toggle on the workflow card.
4. Click on the workflow to open it in the design space.
5. Modify the required tasks.
6. Once the tasks have been modified as required, validate and enable the workflow.
7. Trigger the workflow from the Request :: View/Run page.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 8: CERT+ Automation Workflows API Guide

This guide informs you about the APIs to be used for executing different Cert+ Automation workflows.

- Getting Started
- Enroll Certificate and Download
- Easy Certificate Provisioning
- Enroll Certificate and Push
- Enroll Certificate with ServiceNow
- Enroll Certificate and Push with ServiceNow Integration
- Renew Certificate and Push
- Renew Certificate with ServiceNow Integration
- Renew Certificate and Push With ServiceNow Integration
- Regenerate Certificate - With New CSR
- Get Request Summary/Log

Getting Started

This guide informs you about the APIs to be used for executing different Cert+ Automation workflows.

- Before you Begin
- Login to retrieve active SessionId

Before you Begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer to the Automation User Guide.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Login to retrieve active SessionId

- Overview
- Request Structure
- Response Structure
- Response
- Status Codes
- Sample Request/Response

Overview

This API retrieves the sessionId. This sessionId retrieved can be used for another api that ensures a valid session.

Request Structure

URL:`/acctmgmt-perform-login`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`username`	Header	AppViewX login username.	`String`	NA
`password`	Header	AppViewX login password.	`String`	NA
`Content-Type`	Header	Specifies the nature of the data in the payload.	`String`	Value of param should be `application-json`
`gwkey`	Query	Tenant Key. Needed only in case of multi tenant installations.	`String`	NA
`gwsource`	Query	Source from which the request is triggered. (For example: web, external)	`String`	NA
`payload`	Body	Contains an empty payload.	NA	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More information in case of failure response.	NA

Response

Name	Description	Field Type
status	Status of the request.	String
appStatusCode	appStatusCode	String
statusDescription	Description of the status.	String
sessionId	Session ID to be retrieved.	String
availableLoginAttemptCount	Count of login attempts	Integer

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK	NA	Login successful.	NA
400 Bad Request	NA	Username or password cannot be null or empty.	Check and ensure if a non-null/non-empty value is given in the header field for.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Status Code	appStatusCode	Message	Possible Remediation
401 Unauthorized	NA	Login failed. Invalid credentials.	Check and ensure if the username and password provided are valid and correct.

Sample Request/Response

Use Case: Submit a request for the sessionId retrieval.

Sample Request

```
{
  "payload": {
    }
}
```

Sample Response

```
{
    "response": {
        "status": "SUCCESS",
        "appStatusCode": null,
        "statusDescription": null,
        "sessionId": "dea911-f342-440b-8bce-fe7fbc204g6c",
        "availableLoginAttemptCount": "10"
    },
    "message": null,
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```

Enroll Certificate and Download

- Overview
- Request Structure
- Payload
- Response Structure

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Status Codes
• Sample Request/Response

Overview

This API is used to create and download certificates based on the certificate group.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA
`payload`	Body	Contains all the params to be sent in the request body for the post request.	`payload`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Mandatory	Description	Field Type	Constraints
cert_category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of certificate authority.	String	NA
division	Yes	Division values for DigiCert.	String	Required only if DigiCert is selected as the CA.
cert_type	Yes	Cert Type values for DigiCert and Entrust.	String	Required only if DigiCert is selected as the CA.
description	No	Description of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values**: DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus).	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		Multiple values must be separated by comma (,).		
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
organization	No	Name of the organization requesting the certificate.	String	Required only if AppViewX, EJBCA, Microsoft Enterprise is selected as the CA.
digicert_entrust_organization	Yes	Name of the organization.	String	Required only if DigiCert, Entrust is selected as the CA.
organization_unit	No	Organization unit requesting the certificate.	String	NA
locality	No	Locality in which the organization is situated.	String	NA
state	No	State in which the organization is located.	String	NA
country	No	Country in which the organization is located.	String	Required only if AppViewx, EJBCA, Entrust, Digicert, Microsoft Enterprise is selected as the CA.
entrust_country	Yes	Country in which the organization is located.	String	Required only if Entrust is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
digicert_postal_code	No	Postal code of the organization.	String	Required only if DigiCert is selected as the CA.
mail_address	No	Email address of the organization.	String	NA
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA
key_type	Yes	Key type for the certificate. **Possible values**: RSA, DSA, EC.	String	Required only when the input_method is selected as Manual or Policy Based.
bit_length	Yes	Bit length for the certificate. **Possible values**: 4096, 2048.	String	Required only when the input_method is selected as Manual or Policy Based.
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
elliptic_curve	Yes	Elliptic curve value for the certificate.	String	Required only if key_type is selected as EC.
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The cert_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA

• cert_attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
atrribute	No	Certificate attribute names.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
attribute_value	No	Attribute values.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

• Response

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK	NA	Success	NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	NA

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate and Download"
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
},
"data": {
  "input": {
    "requestData": [
      {
        "sequenceNo": 1,
        "scenario": "scenario",
        "fieldInfo": {
          "info": "",
          "cert_category": "Server,Client,Code Signing",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
          "ca_account": "<mandatory field>",
          "division": "<mandatory field>",
          "cert_type": "<mandatory field>",
          "description": "",
          "common_name": "<mandatory field>",
          "san": "DNS, IP Address",
          "dns_names": "",
          "ip_addresses": "",
          "organization": "",
          "digicert_entrust_organization": "<mandatory field>",
          "organization_unit": "",
          "organization_address": "",
          "locality": "",
          "state": "",
          "country": "",
          "entrust_country": "<mandatory field>",
          "digicert_postal_code": "",
          "mail_address": "",
          "validity_unit": "Days,Months,Years",
          "validity_value": "<mandatory field>",
          "key_type": "RSA,DSA,EC",
          "bit_length": "<mandatory field>",
          "hash_function": "<mandatory field>",
          "elliptic_curve": "<mandatory field>",
          "check_attribute": "true",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "certificates_attributes": [
             {
               "attributes": "",
               "value": ""
             }
            ],
            "digicert_server_type": "<mandatory field>",
            "ejbca_end_entity_profile_name": "<mandatory field>",
            "ejbca_end_entity_user_mame": "",
            "ejbca_issuer_common_name": "<mandatory field>",
            "ejbca_certificate_profile_name": "<mandatory field>",
            "microsoft_enterprise_template_name": "<mandatory field>",
            "entrust_additional_emails": "",
            "user_email": "(~get_logged_user_email_id~)"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    "message": "Success",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


Easy Certificate Provisioning

• Overview
• Request Structure
• Payload
• Response Structure
• Response
• Status Codes
• Sample Request/Response

Overview

This API is used to create an AppViewX certificate and push to a device available in the instance.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
				can be ignored in other types of installations.
gwsource	Query	Source from which the request is triggered. (For example: external)	String	NA
payload	Body	Contains all the params to be sent in the request body for the post request.	payload	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
appviewx_common_name	Yes	Common name of the certificate. Fully qualified domain name (FQDN) of the server for which certificate is requested.	String	NA
appviewx_dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
device_type	Yes	Type of device to which the certificate will be pushed. **Possible Values**: ADC, Server.	String	NA
push_devices	Yes	Contains all push details.	Tabular	NA
device_vendor	Yes	Device vendor type based on selection of device type. **Possible Values**: F5, LinuxServer, Citrix.	String	NA
device	Yes	Device name for selected device_vendor.	String	NA
linux_actions	Yes	Linux action for the selected device_vendor. **Possible Values**:	String	Required only if the device vendor

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb).		is selected as Linux Server.
selected_profiles	Yes	Profile name for device.	String	NA
apache_custom_push	Yes	Provision to opt for pushing the certificate to a custom location. **Possible Values**: Yes, No.	String	Required only if the device vendor is selected as Apache.
apache_certificate_location	Yes	Certificate path created by the user.	String	Required only if apache_custom_push is selected as Yes.
apache_key_location	Yes	Certificate Key path created by the user.	String	Required only if apache_custom_push is selected as Yes.
password	Yes	Password to access the KDB file.	String	Required only if linux_actions is selected as Default.
email_id	No	Email address of the organization. **Possible values**: Default value configured in the policy.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More information in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Status Code	appStatusCode	Message	Possible Remediation
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Easy Certificate Provisioning"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "appviewx_common_name": "<mandatory field>",
              "appviewx_dns_names": "",
              "device_type": "ADC,Server",
              "push_devices": [
                {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
                "device_vendor": "<mandatory field>",
                "device": "<mandatory field>",
                "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
                "selected_profiles": "<mandatory field>",
                "password": "<mandatory field>"
              }
            ],
            "email_id": "<mandatory field>"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "306",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 306 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Enroll Certificate and Push

- Overview
- Request Structure
- Payload
- Response Structure
- Response
- Status Codes
- Sample Request/Response

Overview

This API is used to create a certificate and push it to the selected device.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
payload	Body	Contains all the params to be sent in the request body for the post request.	payload	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
cert_category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of certificate authority.	String	NA
division	Yes	Division values for DigiCert.	String	Required only if DigiCert is selected as the CA.
cert_type	Yes	Cert Type values for DigiCert and Entrust.	String	Required only if DigiCert is selected as the CA.
auto_renew	Yes	If enabled, renewal will be scheduled to trigger before expiry based on renew_before days.	String	NA
renew_before	Yes	The renewal request will be triggered prior to the expiry date	String	Required only if auto_renew is selected.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		as per the selected renew_before days.		
auto_regenerate	Yes	If enabled, regenerate will be scheduled to trigger before expiry based on regenerate_before days.	String	NA
regenerate_before	Yes	The regenerate request will be triggered prior to the expiry date as per the selected regenerate_before days.	String	Required only if auto_regenerate is selected.
input_method	Yes	Certificate creation method. **Possible Values**: Manual, Policy Based, Upload CSR.	String	NA
upload_csr	Yes	CSR for the new certificate.	NA	Required only if the input_method selected is upload_csr.
description	No	Description of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values:**DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus).	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		Multiple values must be separated by comma (,).		
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
directory_names	No	Directory names for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
rfc822names	No	Email address(es) of the user(s) to whom the certificate is issued.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
registered_ids	No	Registered id of the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
uris	No	Uniform Resource Identifier for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
othernames	No	Other names for the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
				is selected as the CA.
organization	No	Name of the organization requesting the certificate.	String	Required only if AppViewX, EJBCA, Microsoft Enterprise is selected as the CA.
organization_unit	No	Organization unit requesting the certificate.	String	NA
locality	No	Locality in which the organization is situated.	String	NA
state	No	State in which the organization is located.	String	NA
country	No	Country in which the organization is located.	String	Required only if AppViewx, EJBCA, Entrust, Digicert, Microsoft Enterprise is selected as the CA.
mail_address	No	Email address of the organization.	String	NA
challenge_password	No	Password to access the certificate.	String	NA
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
key_type	Yes	Key type for the certificate. **Possible values**: RSA, DSA, EC.	String	Required only when the input_method is selected as Manual or Policy Based.
bit_length	Yes	Bit length for the certificate. **Possible values**: 4096, 2048.	String	Required only when the input_method is selected as Manual or Policy Based.
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
elliptic_curve	Yes	Elliptic curve value for the certificate.	String	Required only if key_type is selected as EC.
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA
device_type	Yes	Type of device to which the certificate will be pushed. **Possible Values**: ADC, Server.	String	NA
push_devices	Yes	Contains all device fields.	Array of attributes	NA

- Atrributes
- cert_atrributes

Atrributes

Name	Mandatory	Description	Field Type	Constraints
device_vendor	Yes	Device vendor type based on selection of device type. **Possible Values**: F5, LinuxServer, Citrix.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
device	Yes	Device name for selected device_vendor.	String	NA
linux_actions	Yes	Linux action for the selected device_vendor. For example: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb).	String	Required only if the device vendor is selected as Linux Server.
selected_profiles	Yes	Profile name for device.	String	NA
apache_custom_push	Yes	Provision to opt for pushing the certificate to a custom location. **Possible Values**: Yes, No.	String	Required only if the device vendor is selected as Apache.
apache_certificate_location	Yes	Certificate path created by the user.	String	Required only if apache_custom_push is selected as Yes.
apache_key_location	Yes	Certificate Key path created by the user.	String	Required only if apache_custom_push is selected as Yes.
password	Yes	Password to access the KDB file.	String	Required only if linux_actions is selected as Default.
push_cert_type	Yes	Certificate type being pushed.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

cert_atrributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attribute names.	String	NA
attribute_value	No	Attribute values.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Certificate Create and Push"
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
},
"data": {
  "input": {
    "requestData": [
      {
        "sequenceNo": 1,
        "scenario": "scenario",
        "fieldInfo": {
          "info": "",
          "cert_category": "Server,Client,Code Signing",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "DigiCert,Entrust,Ejbca,Microsoft Enterprise,Microsoft Standalone",
          "ca_account": "<mandatory field>",
          "division": "<mandatory field>",
          "cert_type": "",
          "auto_renew": "Off,On",
          "renew_before": "<mandatory field>",
          "auto_regenerate": "Off,On",
          "regenerate_before": "<mandatory field>",
          "input_method": "Manual,Policy Based,Upload CSR",
          "upload_csr": "<mandatory field>",
          "common_name": "<mandatory field>",
          "san": "DNS,IP Address",
          "directory_names": "",
          "dns_names": "",
          "rfc822names": "",
          "ip_addresses": "",
          "registered_ids": "",
          "uris": "",
          "othernames": "",
          "organization": "",
          "organization_unit": "",
          "locality": "",
          "state": "",
          "country": "",
          "mail_address": "",
          "postal_code": "",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
        "validity_unit": "Days,Months,Years",
        "validity_value": "1",
        "challenge_password": "",
        "hash_function": "<mandatory field>",
        "key_type": "EC",
        "bit_length": "<mandatory field>",
        "elliptic_curve": "<mandatory field>",
        "attributes_available": "true",
        "cert_attributes": [
         {
           "attribute": "",
           "attribute_value": ""
         }
        ],
        "digicert_server_type": "<mandatory field>",
        "ejbca_end_entity_profile_name": "<mandatory field>",
        "ejbca_end_entity_user_name": "",
        "ejbca_issuer_common_name": "<mandatory field>",
        "ejbca_certificate_profile_name": "<mandatory field>",
        "entrust_additional_emails": "",
        "microsoft_enterprise_template_name": "<mandatory field>",
        "device_type": "ADC,Server",
        "push_devices": [
         {
           "device_vendor": "<mandatory field>",
           "device": "<mandatory field>",
           "linux_action": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
           "selected_profiles": "<mandatory field>",
           "password": "<mandatory field>",
           "push_cert_type": "<mandatory field>"
         }
        ],
        "user_email": ""
      }
    }
  ]
},
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Enroll Certificate with ServiceNow

- Overview
- Request Structure
- Payload
- Response Structure
- Response
- Status Codes
- Sample Request/Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

This API is used to create a certificate corresponding to the ticket raised on ServiceNow (RITM).

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA
`payload`	Body	Contains all the params to be sent in the request body for the post request.	`payload`	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
`cert_category`	Yes	Specifies the certificate category. **Possible values**: Server, Client	`String`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of certificate authority.	String	NA
division	Yes	Division values for DigiCert.	String	Required only if DigiCert is selected as the CA.
cert_type	Yes	Cert Type values for DigiCert and Entrust.	String	Required only if DigiCert is selected as the CA.
description	No	Description of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values:**DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
organization	No	Name of the organization requesting the certificate.	String	Required only if AppViewX, EJBCA, Microsoft Enterprise is selected as the CA.
digicert_entrust_organization	Yes	Name of the organization.	String	Required only if DigiCert, Entrust is selected as the CA.
organization_unit	No	Organization unit requesting the certificate.	String	NA
locality	No	Locality in which the organization is situated.	String	NA
state	No	State in which the organization is located.	String	NA
country	No	Country in which the organization is located.	String	Required only if AppViewx, EJBCA, Entrust, Digicert, Microsoft Enterprise is selected as the CA.
entrust_country	Yes	Country in which the organization is located.	String	Required only if Entrust is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
digicert_postal_code	No	Postal code of the organization.	String	Required only if DigiCert is selected as the CA.
mail_address	No	Email address of the organization.	String	NA
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA
key_type	Yes	Key type for the certificate. **Possible values**: RSA, DSA, EC.	String	Required only when the input_method is selected as Manual or Policy Based.
bit_length	Yes	Bit length for the certificate. **Possible values**: 4096, 2048.	String	Required only when the input_method is selected as Manual or Policy Based.
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
elliptic_curve	Yes	Elliptic curve value for the certificate.	String	Required only if key_type is selected as EC.
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA
snow_integration	Yes	Provision to opt for ServiceNow integration. **Possible Values:** Yes, No	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
snow_account	No	ServiceNow account	String	Required only if ServiceNow integration is selected.
download_format	Yes	Download format for certificate type	String	Required only if ServiceNow integration is selected.

• cert_attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attributes names.	String	NA
attribute_value	No	Attribute value.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Status Code	appStatusCode	Message	Possible Remediation
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate with ServiceNow"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "cert_category": "Server,Client,Code Signing",
              "certificate_group": "<mandatory field>",
              "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
              "ca_account": "<mandatory field>",
              "division": "<mandatory field>",
              "cert_type": "<mandatory field>",
              "description": "",
              "common_name": "<mandatory field>",
              "san": "DNS, IP Address",
              "dns_names": "",
              "ip_addresses": "",
              "organization": "",
              "digicert_entrust_organization": "<mandatory field>",
              "organization_unit": "",
              "organization_address": "",
              "locality": "",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
          "state": "",
          "country": "",
          "entrust_country": "<mandatory field>",
          "digicert_postal_code": "",
          "mail_address": "",
          "validity_unit": "Days,Months,Years",
          "validity_value": "<mandatory field>",
          "key_type": "RSA,DSA,EC",
          "bit_length": "<mandatory field>",
          "hash_function": "<mandatory field>",
          "elliptic_curve": "<mandatory field>",
          "download_format": "(~get_certificate_download_format~)",
          "check_attribute": "true",
          "certificates_attributes": [
           {
             "attributes": "",
             "value": ""
           }
          ],
          "digicert_server_type": "<mandatory field>",
          "ejbca_end_entity_profile_name": "<mandatory field>",
          "ejbca_end_entity_user_name": "",
          "ejbca_issuer_common_name": "<mandatory field>",
          "ejbca_certificate_profile_name": "<mandatory field>",
          "microsoft_enterprise_template_name": "<mandatory field>",
          "entrust_additional_emails": "",
          "snow_integrations": "Yes,No",
          "ritm": "<mandatory field>",
          "snow_account": "",
          "user_email": ""
        }
      }
    ]
  },
  "globalData": {},
  "task_action": 1
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
 }
}
```

Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
   },
   "message": "Success",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```


Enroll Certificate and Push with ServiceNow Integration

- Overview
- Request Structure
- Payload
- Response Structure
- Response
- Status Codes
- Sample Request Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

This API is used to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA
`payload`	Body	Contains all the params to be sent in the request body for the post request.	`payload`	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
`cert_category`	Yes	Specifies the certificate category. **Possible values**: Server, Client	`String`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of certificate authority.	String	NA
division	Yes	Division values for DigiCert.	String	Required only if DigiCert is selected as the CA.
description	No	Description of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values:**DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
organization	No	Name of the organization requesting the certificate.	String	Required only if AppViewX, EJBCA, Microsoft Enterprise is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
digicert_entrust_organization	Yes	Name of the organization.	String	Required only if DigiCert, Entrust is selected as the CA.
organization_unit	No	Organization unit requesting the certificate.	String	NA
locality	No	Locality in which the organization is situated.	String	NA
state	No	State in which the organization is located.	String	NA
country	No	Country in which the organization is located.	String	Required only if AppViewx, EJBCA, Entrust, Digicert, Microsoft Enterprise is selected as the CA.
entrust_country	Yes	Country in which the organization is located.	String	Required only if Entrust is selected as the CA.
digicert_postal_code	No	Postal code of the organization.	String	Required only if DigiCert is selected as the CA.
mail_address	No	Email address of the organization.	String	NA
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA
key_type	Yes	Key type for the certificate. **Possible values**: RSA, DSA, EC.	String	Required only when the input_method is selected as Manual or Policy Based.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
bit_length	Yes	Bit length for the certificate. **Possible values**: 4096, 2048.	String	Required only when the input_method is selected as Manual or Policy Based.
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
elliptic_curve	Yes	Elliptic curve value for the certificate.	String	Required only if key_type is selected as EC.
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA
snow_integration	Yes	Provision to opt for ServiceNow integration. **Possible Values:** Yes, No	String	NA
snow_account	No	ServiceNow account	String	Required only if ServiceNow integration is selected.
download_format	Yes	Download format for certificate type	String	Required only if ServiceNow integration is selected.
device_type	Yes	Type of device to which the certificate will be pushed. **Possible Values**: ADC, Server.	String	NA
push_devices	Yes	Contains all device fields.	Array of attributes	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• cert_attributes
• Attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attributes names.	String	NA
attribute_value	No	Attribute value.	String	NA

Attributes

Name	Mandatory	Description	Field Type	Constraints
device_vendor	Yes	Device vendor type based on selection of device type. **Possible Values**: F5, LinuxServer, Citrix.	String	NA
device	Yes	Device name for selected device_vendor.	String	NA
linux_actions	Yes	Linux action for the selected device_vendor. For example: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb).	String	Required only if the device vendor is selected as Linux Server.
selected_profiles	Yes	Profile name for device.	String	NA
apache_custom_push	Yes	Provision to opt for pushing the certificate to a	String	Required only if the device vendor

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		custom location. **Possible Values**: Yes, No.		is selected as Apache.
apache_certificate_location	Yes	Certificate path created by the user.	String	Required only if apache_custom_push is selected as Yes.
apache_key_location	Yes	Certificate Key path created by the user.	String	Required only if apache_custom_push is selected as Yes.
password	Yes	Password to access the KDB file.	String	Required only if linux_actions is selected as Default.
push_cert_type	Yes	Certificate type being pushed.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

HTTP Status Code	appStatusCode	Message	Possible Remediation
500 Internal Server Error	NA	Error while processing	

Sample Request Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate and Push with ServiceNow"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "cert_category": "Server,Client,Code Signing",
              "certificate_group": "<mandatory field>",
              "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
              "ca_account": "<mandatory field>",
              "division": "<mandatory field>",
              "cert_type": "<mandatory field>",
              "description": "",
              "common_name": "<mandatory field>",
              "san": "DNS, IP Address",
              "dns_names": "",
              "ip_addresses": "",
              "organization": "",
              "digicert_entrust_organization": "<mandatory field>",
              "organization_unit": "",
              "organization_address": "",
              "locality": "",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"state": "",
"country": "",
"entrust_country": "<mandatory field>",
"digicert_postal_code": "",
"mail_address": "",
"validity_unit": "Days,Months,Years",
"validity_value": "<mandatory field>",
"key_type": "RSA,DSA,EC",
"bit_length": "<mandatory field>",
"hash_function": "<mandatory field>",
"elliptic_curve": "<mandatory field>",
"download_format": "<mandatory field>",
"check_attribute": "true",
"certificates_attributes": [
 {
  "attributes": "",
  "value": ""
 }
],
"digicert_server_type": "<mandatory field>",
"ejbca_end_entity_profile_name": "<mandatory field>",
"ejbca_end_entity_user_name": "",
"ejbca_issuer_common_name": "<mandatory field>",
"ejbca_certificate_profile_name": "<mandatory field>",
"microsoft_enterprise_template_name": "<mandatory field>",
"entrust_additional_emails": "",
"device_type": "ADC,Server",
"push_devices": [
 {
  "device_vendor": "<mandatory field>",
  "device": "<mandatory field>",
  "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
  "selected_profiles": "<mandatory field>",
  "password": "<mandatory field>",
  "push_cert_type": "<mandatory field>"
 }
],
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "snow_integrations": "Yes,No",
            "ritm": "<mandatory field>",
            "snow_account": "",
            "user_email": ""
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
    "response": {
        "workorderId": "0",
        "requestType": "default",
        "requestId": "867",
        "workflowVersion": "master",
        "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
        "status": "In Progress",
        "statusCode": 0
    },
    "message": "Success",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


Renew Certificate and Push

- Overview
- Request Structure

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Payload
• Response Structure
• Response
• Status Codes
• Sample Request/Response

Overview

This API is used to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA
`payload`	Body	Contains all the params to be sent in the request body for the post request.	`payload`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Payload

Name	Mandatory	Description	Field Type	Constraints
cert_category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
serial_number	Yes	Serial Number of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values:**DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		be separated by comma(,).		
directory_names	No	Directory names for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
rfc822names	No	Email address(es) of the user(s) to whom the certificate is issued.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
registered_ids	No	Registered id of the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
uris	No	Uniform Resource Identifier for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
othernames	No	Other names for the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
orderId		Order id of DigiCert certificate.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA
push_devices	Yes	Contains all push details.	Array of attributes	NA

- cert_attributes
- Attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attribute names.	String	NA
attribute_value	No	Attribute values.	String	NA

Attributes

Name	Mandatory	Description	Field Type	Constraints
device_type	Yes	Type of device to which the certificate will be pushed. **Possible Values**: ADC, Server.	String	NA
device_vendor	Yes	Device vendor type based on selection of device type. **Possible Values**:	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		F5, LinuxServer, Citrix.		
device	Yes	Device name for selected device_vendor.	String	NA
linux_actions	Yes	Linux action for the selected device_vendor. **Possible Values**: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb).	String	Required only if the device vendor is selected as Linux Server.
selected_profiles	Yes	Profile name for device.	String	NA
apache_custom_push	Yes	Provision to opt for pushing the certificate to a custom location. **Possible Values**: Yes, No.	String	Required only if the device vendor is selected as Apache.
apache_certificate_location	Yes	Certificate path created by the user.	String	Required only if apache_custom_push is selected as Yes.
apache_key_location	Yes	Certificate Key path created by the user.	String	Required only if apache_custom_push is selected as Yes.
password	Yes	Password to access the KDB file.	String	Required only if linux_actions is selected as Default.
push_cert_type	Yes	Certificate type being pushed.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate and Push"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"scenario": "scenario",
"fieldInfo": {
 "info": "",

 "cert_category": "Server,Client",
 "certificate_group": "<mandatory field>",
 "certificate_authority": "Microsoft Enterprise,DigiCert,Ejbca,Entrust",
 "serial_number": "<mandatory field>",
 "common_name": "<mandatory field>",
 "san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
 "dNSNames": "",
 "directoryNames": "",
 "iPAddresses": "",
 "registeredIDs": "",
 "otherNames": "",
 "uniformResourceIdentifiers": "",
 "rfc822Names": "",
 "validity_unit": "<mandatory field>",
 "validity_value": "<mandatory field>",
 "hash_function": "<mandatory field>",
 "attributes_available": "true",
 "cert_attributes": [
  {
   "attribute": "",
   "attribute_value": ""
  }
 ],
 "orderId": "",
 "digicert_server_type": "<mandatory field>",
 "ejbca_End_Entity_Profile_Name": "<mandatory field>",
 "ejbca_End_Entity_User_Name": "",
 "ejbca_Issuer_Common_Name": "<mandatory field>",
 "ejbca_Certificate_Profile_Name": "<mandatory field>",
 "microsoft_enterprise_template_name": "<mandatory field>",
 "entrust_additional_emails": "",
 "push_devices": [
  {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "device_type": "ADC,Server",
            "device_vendor": "<mandatory field>",
            "device": "<mandatory field>",
            "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
            "selected_profiles": "<mandatory field>",
            "password": "<mandatory field>",
            "push_cert_type": "<mandatory field>"
          }
        ],
        "user_email": "(~get_logged_user_email_id~)"
      }
    }
  ]
 },
 "globalData": {},
 "task_action": 1
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
}
```

Renew Certificate with ServiceNow Integration

• Overview

• Request Structure

• Payload

• Response Structure

• Response

• Status Codes

• Sample Request/Response

Overview

This API is used to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
gwsource	Query	Source from which the request is triggered. (For example: external)	String	NA
payload	Body	Contains all the params to be sent in the request body for the post request.	payload	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
group_name	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of Selected CA	String	NA
certificate	Yes	Universal Unique Identifier (UUID) of the certificate.	String	NA
serial_number	Yes	Serial Number of the certificate	String	NA
common_name	Yes	Common Name of the certificate	String	NA
san_type	No	Subject Alternative Name of the certificate. **Possible Values:**DNS, IP Address	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
iPAddresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
directory_names	No	Directory names for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
uniformResourceIdentifiers	No	Uniform Resource Identifier for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
otherNames	No	Other names for the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
registeredIDs	No	Registered id of the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
validity	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
cert_attributes	No	Details of certificate attributes.	Array of attrib_details	NA
email_id	No	Email address of the organization. **Possible Values**: Default value configured in the policy	String	NA
snow_integration	Yes	Provision to opt for ServiceNow integration. **Possible Values:** Yes, No	String	NA
ritm	Yes	RITM ticket number for ServiceNow ticket	String	Required only if ServiceNow integration is selected.
snow_account	No	ServiceNow account	String	Required only if ServiceNow integration is selected.
download_format	Yes	Format in which the certificate will be downloaded.	String	Required only if ServiceNow integration is selected.
show_validity	Yes	Hidden field inside the form. Default value is **'1'**	String	NA

• attrib_details

attrib_details

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attributes names.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
attribute_value	No	Attribute Value.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"scenario": "scenario",
"fieldInfo": {
  "info": "",
  "category": "Server,Client",
  "group_name": "<mandatory field>",
  "policy_hidden": "",
  "certificate_authority": "<%certificate_authority%>",
  "certificate": "",
  "ca_account": "",
  "comman_name": "<mandatory field>",
  "san_type": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
  "dNSNames": "",
  "iPAddresses": "",
  "rfc": "",
  "directory_names": "",
  "uniformResourceIdentifiers": "",
  "otherNames": "",
  "registeredIDs": "",
  "division": "",
  "organisation": "",
  "organisation_unit": "",
  "country": "",
  "city": "",
  "state": "",
  "postalcode": "",
  "mailaddress": "",
  "validity": "",
  "validity_value": "",
  "hash_function": "<mandatory field>",
  "bit_length": "",
  "key_type": "",
  "attrib_details": [
   {
     "cert_attribute_name": "",
     "cert_attribute_value": ""
   }
  ],
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "order_id": "",
            "server_type": "",
            "order_validity": "",
            "order_val_till": "",
            "end_entity_profile_name": "",
            "end_entity_user_name": "",
            "issuer_common_name": "",
            "certificate_profile_name": "",
            "template_name": "",
            "additional_email": "",
            "resource": "",
            "serial_number": "<mandatory field>",
            "email_id": "(~get_logged_user_email_id~)",
            "ca": "",
            "description": ""
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Renew Certificate and Push With ServiceNow Integration

• Overview
• Request Structure
• Payload
• Response Structure
• Response
• Status Codes
• Sample Request/Response

Overview

This API is used to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
gwkey	Query	Tenant Key	String	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
gwsource	Query	Source from which the request is triggered. (For example: external)	String	NA
payload	Body	Contains all the params to be sent in the request body for the post request.	payload	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
cert_category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
serial_number	Yes	Serial Number of the certificate.	String	NA
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible**	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
		Values:DNS, IP Address		
dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
directory_names	No	Directory names for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
rfc822names	No	Email address(es) of the user(s) to whom the certificate is issued.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
registered_ids	No	Registered id of the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
uris	No	Uniform Resource Identifier for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
othernames	No	Other names for the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
orderId		Order id of DigiCert certificate.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA
snow_integration	Yes	Provision to opt for ServiceNow integration. **Possible Values:** Yes, No	String	NA
ritm	Yes	RITM ticket number for ServiceNow ticket	String	Required only if ServiceNow integration is selected.
snow_account	No	ServiceNow account	String	Required only if ServiceNow integration is selected.
download_format	Yes	Download format for the certificate.	String	Required only if ServiceNow integration is selected.
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA

• cert_attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attribute names.	String	NA
attribute_value	No	Attribute values.	String	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate and Push with ServiceNow"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "cert_category": "Server,Client",
              "certificate_group": "<mandatory field>",
              "certificate_authority": "<mandatory field>",
              "serial_number": "<mandatory field>",
              "common_name": "<mandatory field>",
              "san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
              "dNSNames": "",
              "directoryNames": "",
              "iPAddresses": "",
              "registeredIDs": "",
              "otherNames": "",
              "uniformResourceIdentifiers": "",
              "rfc822Names": "",
              "validity_unit": "<mandatory field>",
              "validity_value": "<mandatory field>",
              "hash_function": "",
              "download_format": "(~get_certificate_download_format~)",
              "cert_attributes": [
                {
                  "attributes": "",
                  "attribute_value": ""
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            }
           ],
           "snow_integrations": "Yes,No",
           "ritm": "<mandatory field>",
           "snow_account": "(~get_ServiceNow_accounts~)",
           "user_email": "(~get_logged_user_email_id~)"
         }
       }
     ]
   },
   "globalData": {},
   "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
   },
   "message": "Success",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Regenerate Certificate - With New CSR

- Overview
- Request Structure
- Payload
- Response Structure
- Response
- Status Codes
- Sample Request/Response

Overview

This API is used to regenerate a certificate with a new CSR.

Request Structure

URL: `/visualworkflow-submit-request`

Type: POST

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Param Type	Description	Field Type	Constraints
payload	Body	Contains all the params to be sent in the request body for the post request.	payload	NA

Payload

Name	Mandatory	Description	Field Type	Constraints
cert_category	Yes	Specifies the certificate category. **Possible values**: Server, Client	String	NA
certificate_group	Yes	Specifies the group under which the created certificate needs to be tagged.	String	NA
certificate_authority	Yes	Name of the certificate authority that will issue the certificate.	String	NA
ca_account	Yes	CA account Name of certificate authority.	String	NA
division	Yes	Division values for DigiCert.	String	Required only if DigiCert is selected as the CA.
cert_type	Yes	Cert Type values for DigiCert and Entrust.	String	Required only if DigiCert, Entrust is selected as the CA.
input_method	Yes	Certificate creation method. **Possible Values**: Manual, Policy Based, Upload CSR.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
upload_csr	Yes	CSR for the new certificate.	NA	Required only if the input_method selected is upload_csr.
common_name	Yes	Common Name of the certificate.	String	NA
san	No	Subject Alternative Name of the certificate. **Possible Values:** DNS, IP Address	String	NA
dns_names	No	DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,).	String	NA
ip_addresses	No	IP values (For example: 192.16x.xx.x). Multiple values must be separated by comma(,).	String	NA
directory_names	No	Directory names for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
rfc822names	No	Email address(es) of the user(s) to whom the certificate is issued.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
registered_ids	No	Registered id of the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
uris	No	Uniform Resource Identifier for the certificate.	String	Required only when EJBCA, Microsoft Enterprise, Microsoft Standalone is selected as the CA.
othernames	No	Other names for the certificate.	String	Required only when Microsoft Enterprise, Microsoft Standalone is selected as the CA.
organization	No	Name of the organization requesting the certificate.	String	Required only if AppViewX, EJBCA, Microsoft Enterprise is selected as the CA.
organization_unit	No	Organization unit requesting the certificate.	String	NA
locality	No	Locality in which the organization is situated.	String	NA
state	No	State in which the organization is located.	String	NA
country	No	Country in which the organization is located.	String	Required only if AppViewx, EJBCA, Entrust, Digicert, Microsoft Enterprise is selected as the CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
mail_address	No	Email address of the organization.	String	NA
challenge_password	No	Password to access the certificate.	String	NA
validity_unit	Yes	Unit of validity for the certificate. **Possible Values**: Days, Months, Years.	String	NA
validity_value	Yes	Validity value for the certificate.	String	NA
key_type	Yes	Key type for the certificate. **Possible values**: RSA, DSA, EC.	String	Required only when the input_method is selected as Manual or Policy Based.
bit_length	Yes	Bit length for the certificate. **Possible values**: 4096, 2048.	String	Required only when the input_method is selected as Manual or Policy Based.
hash_function	Yes	Hash function for the certificate. **Possible values**: SHA256.	String	NA
digicert_server_type	Yes	DigiCert server type value.	String	Required only if DigiCert is selected as CA.
ejbca_end_entity_profile_name	Yes	Profile name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.
ejbca_end_entity_user_name	No	User name of the EJBCA end entity.	String	Required only if EJBCA is selected as CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Mandatory	Description	Field Type	Constraints
ejbca_issuer_common_name	Yes	Common name of the EJBCA issuer.	String	Required only if EJBCA is selected as CA.
ejbca_certificate_profile_name	Yes	Profile name associated with the EJBCA certificate.	String	Required only if EJBCA is selected as CA.
entrust_additional_emails	No	Additional email address(es).	String	Required only if Entrust is selected as CA.
microsoft_enterprise_template_name	Yes	Template name for Microsoft Enterprise.	String	Required only if Microsoft Enterprise is selected as CA.
user_email	Yes	Email address for sending notification of the status of certificate creation and push.	String	NA
check_attribute	No	Certificate attribute values. **Possible Values**: true, false.	String	The certificates_attributes field will be passed only if the value is true.
cert_attributes	No	Array of certificate attributes	Array of cert_attributes	NA

• cert_attributes

cert_attributes

Name	Mandatory	Description	Field Type	Constraints
attribute	No	Certificate attribute names.	String	NA
attribute_value	No	Attribute values.	String	NA

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Response Structure

200 OK returns string of type application/json with the following body params:

Name	Description	Field Type
response	Contains the response params for the search object request.	response
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Response

Name	Description	Field Type
requestId	Unique identifier for the request.	String
workflowVersion	Version of the workflow.	String
message	The message with the status and request number for the request.	String
status	Status of the request.	String
stausCode	Status code for the request.	String
requestType	The type of the request.	String
workorderId	The workoderid for the request If there is no workorder the value will be 0.	String

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK		Success	
400 Bad Request	avx-common-028	Invalid/ Incorrect payload	Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized.	Logged-in user is not authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.	Invalid workflow data.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state.	Given workflow is not in enabled state.
500 Internal Server Error	WORKFLOW_1617	Invalid form data Please provide all mandatory data	Check and ensure if a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing	

Sample Request/Response

Sample Request


```
{
 {
 "payload": {
  "header": {
   "workflowName": "Regenerate Certificate - With New CSR"
  },
  "data": {
   "input": {
    "requestData": [
     {
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
"sequenceNo": 1,
"scenario": "scenario",
"fieldInfo": {
  "info": "",
  "cert_category": "Server,Client",
  "certificate_group": "<mandatory field>",
  "certificate_authority": "Ejbca,Microsoft Enterprise,DigiCert,Entrust",
  "ca_account": "<mandatory field>",
  "division": "",
  "cert_type": "",
  "serial_number": "<mandatory field>",
  "input_method": "Manual,Upload CSR",
  "cert_profile": "",
  "upload_csr": "<mandatory field>",
  "fetch_csr_params": "",
  "common_name": "<mandatory field>",
  "csr_common_name": "",
  "san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
  "csr_san": "DNS,Directory Name,IP Address,Registered ,ID,URL,Other Name,Email",
  "csr_dns": "",
  "dNSNames": "",
  "directoryNames": "",
  "iPAddresses": "",
  "registeredIDs": "",
  "otherNames": "",
  "uniformResourceIdentifiers": "",
  "rfc822names": "",
  "organization": "",
  "csr_iPAddresses": "",
  "csr_uniformResourceIdentifiers": "",
  "csr_directoryNames": "",
  "csr_registeredIDs": "",
  "csr_otherNames": "",
  "csr_rfc822names": "",
  "csr_organization": "",
  "organization_unit": "",
  "csr_organization_unit": "",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
      "locality": "",
      "csr_locality": "",
      "state": "",
      "csr_state": "",
      "country": "",
      "csr_email_address": "",
      "mail_address": "",
      "challenge_password": "",
      "csr_challenge_password": "",
      "csr_country": "",
      "digicert_postal_code": "",
      "validity_unit": "<mandatory field>",
      "validity_value": "<mandatory field>",
      "csr_key_type": "EC",
      "key_type": "EC",
      "bit_length": "<mandatory field>",
      "csr_bit_length": "",
      "hash_function": "<mandatory field>",
      "csr_hash_function": "",
      "attributes_available": "true",
      "cert_attributes": [
       {
         "attributes": "",
         "attribute_value": ""
       }
      ],
      "ejbca_End_Entity_Profile_Name": "<mandatory field>",
      "ejbca_End_Entity_User_Name": "",
      "ejbca_Issuer_Common_Name": "<mandatory field>",
      "ejbca_Certificate_Profile_Name": "<mandatory field>",
      "digicert_server_type": "<mandatory field>",
      "microsoft_enterprise_template_name": "<mandatory field>",
      "entrust_additional_emails": "",
      "user_email": "(~get_logged_user_email_id~)"
    }
  }
]
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the Request Structure to identify the changeable values.

Sample Response


```
{
  {
  "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 897 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Get Request Summary/Log

- Overview
- Request Structure
- Response Structure
- Status Codes
- Sample Request/Response

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Overview

After you are done submitting a workflow you can get the request summary/logs details of a particular workflow request. The execution details of the workflow can be viewed from these logs.

Request Structure

URL:`/visualworkflow-request-logs`

Type: GET

Name	Param Type	Description	Field Type	Constraints
`sessionId`	Header	Session Id received after login.	`String`	Required if username and password are not provided.
`username`	Header	AppViewX login username.	`String`	Required if sessionId is not provided.
`password`	Header	AppViewX login password.	`String`	Required if sessionId is not provided.
`content-type`	Header	Specifies the nature of the data in the payload	`String`	Value of the param should be `application/json`
`gwkey`	Query	Tenant Key	`String`	This is required only in case of multi-tenant installations and can be ignored in other types of installations.
`gwsource`	Query	Source from which the request is triggered. (For example: external)	`String`	NA
`ids`	Query	Request IDs	`String`	NA

Response Structure

200 OK returns string of type application/json with the following body params:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Name	Description	Field Type
response	Contains the response object along with the hierarchy of the object mapped in field children.	Key value pair
message	Success message or failure description in case of error.	String
appStatusCode	Application specific status code for the response. Will be non-null for failure response.	String
tags	More info in case of failure response.	NA

Status Codes

HTTP Status Code	appStatusCode	Message	Possible Remediation
200 OK	NA	Success	NA
400 Bad Request	WORKFLOW_1300	Workflow Request Id is Mandatory.	Check and ensure if a valid Request Id is given.
404 Not Found	engine-db-011	Request not found.	Invalid workflow data.

Sample Request/Response

Sample Request

NA

Sample Response


```
{
   "response": {
      "workOrderList": [
         {
            "statusCode": 1,
            "requestId": "410",
             "created_by": "admin",
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
            "status": "Completed",
            "workflowName": "Copy of reviewComponent Test",
             "toolTip": null,
            "workorder_id": null,
             "description": null,
            "ticket_details": null,
            "tasks": [
               {
                  "state": 1,
                 “comments”:null,
                  "task_name": "WorkOrder",
                  "task_id": "startWorkOrder_1",
                  "user": "admin",
                  "task_status": "Success",
                  "task_start_time": 1502696313667,
                  "task_end_time": 1502696729781,

                  "logs": [
                     {
                        "time": 1502696313815,
                        "message": "Child WorkOrder ID: 1, has been created for the Child workflow: WorkOrder"
                     },
                     {
                        "time": 1502696729781,
                        "message": "WorkOrder Completed"
                     }
                  ]
               }
            ],
            "created_time": 1502696305239,
            "rollback_reference_id": "",
            "clone_reference_ids": [],
            "last_updated": 1502696305239,
            "runnning_time": 0
         }
      ]
   },
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    "message": null,
    "appStatusCode": null,
    "tags": null
}
```


Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 9: CERT+ Solution Guides

• EST Client Configuration Guide - Linux and Windows

• EST Server Configuration Guide

• SCEP Configuration Guide

• ACME Configuration Guide

• MSIntune Integration Guide

EST Client Configuration Guide - Linux and Windows

This guide describes the steps to install the EST client agent on a Linux and Windows machine.

• Overview

• Installation Steps

• Downloading and Extracting the EST Client in Linux Machine

• Downloading and Extracting the EST Client in Windows Machine

• Configuring the AppViewX EST Client for Redistribution to End-Users (Linux and Windows)

• Generator And Installer For EST Client in Linux Machine

• Generator and Installer for EST Client in Windows Machine

• Available Commands and Features in EST Client

• Keystore

• Troubleshooting Steps and Common Errors [Linux and Windows]

• Best Practices for Client

Overview

AppViewX EST Client and Server

Enrollment over Secure Transport (EST) is a simple and functional certificate management protocol defined under RFC 7030. EST works in the client-server model. AppViewX offers both EST server and client functionalities with TLS-based authentication between the server and client as per the protocol. This document helps with the configuration of the AppViewX EST Client in Windows, Linux and Mac OS.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Need for an EST Client

Most laptop and desktop systems do not have the capability of generating certificates, but they still require a system or user level or for other purposes, the certificates from a CA for various authentication and signing purposes. Hence, a desktop application like the EST Client is required which enables the system and OS users with certificates.

Values and Benefits of Using the EST Client

EST is one of the automatic enrollment protocols which also supports a wide range of functionalities, such as enrollment, re-enrollment, and server-side key generation. This protocol is used as a base for building this client and also be an interoperable client with other EST-compliant servers.

Some benefits of using the EST Client are

- It is simple to install and use
- It uses the native keystore of the windows keystore and the apple keychain store for Windows and MAC systems, and for Linux, a proprietary keystore is used with the required encryption followed.
- It is available for Windows, Linux, and MAC OS.
- It can be set for automatic enrollment through a set-up in the scheduler and its renewal happens automatically based on the scheduler job.

Certificate Procurement using the EST Client

EST Client provides a mechanism to generate system, OS User, authentication, and other types of certificates.

Installation Steps

This document provides guidance on how to install and configure the EST client agent on both Linux and Windows machines. The installation and configuration process encompasses the following steps:

1. Downloading and extracting the est client in Linux machine and Windows machine (different sections are provided for each operating system)
2. Configuring the AppViewX EST Client for Redistribution to End-Users [Linux and Windows]
3. Generator And Installer EST Client in Linux machine and Windows machine (different sections are provided for each operating system)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Downloading and Extracting the EST Client in Linux Machine

This section covers the configuration procedures for the EST client agent on a Linux machine to perform certificate enrollment tasks.

• Prerequisites for the EST Client Agent Installation on a Linux Machine
• Downloading and Extracting the Agent Software

Prerequisites for the EST Client Agent Installation on a Linux Machine

- Configure EST server in AppViewX.
- Ensure that the firewall configuration permits communication for the EST client. (Port 30021 for both On-Prem and SaaS setup)
- If load balancer is involved in the network infrastructure for the endpoint to communicate with EST agent, please ensure that load balancer does not terminate the client authentication certificate. If it terminates, then EST authentication mode should be set as "**Certificate TLS with HTTP as fallback**" in EST endpoint configuration in AppViewX.
- OS Requirements: Supported OS and their versions are mentioned in the table below.

OS	Versions
Redhat	v8.6 and later
Ubuntu	v20.04 and later
CentOS	v7.9 and later
Debian	v11.0 and later
Mint	v18.2 and later
Opensuse	v15.0 and later

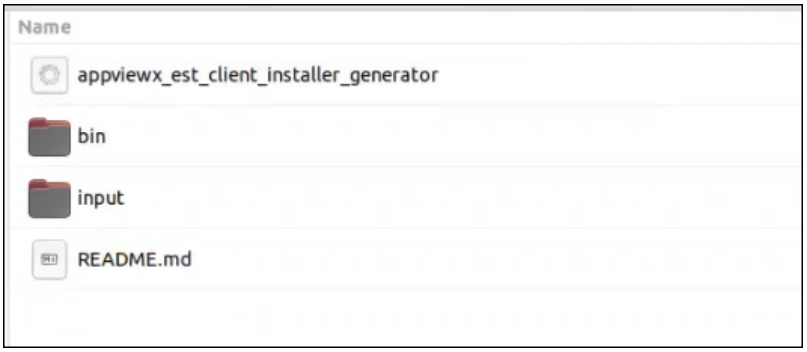
Downloading and Extracting the Agent Software

1. Login to the AppViewX release portal
2. Download the **est-client-linux-1.X.0.zip** file.
3. Extract the above zip file to the desired file location.
   The extracted file contains the following two subfolders:
   - appviewx_est_client_installer
   - appviewx_est_client_installer_generator

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



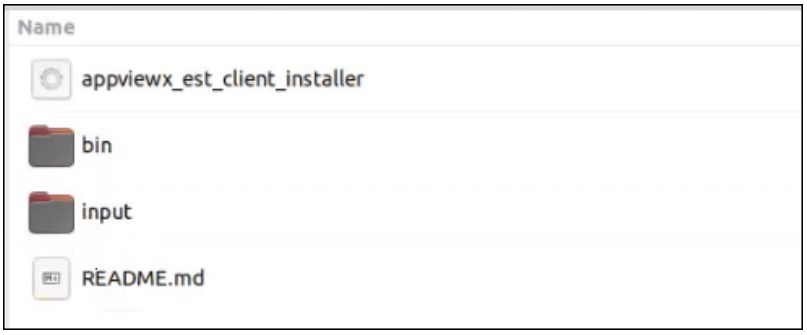
Contents of the **appviewx_est_client_installer_generator** folder:



- appviewx_est_client_installer_generator
- bin
- input

  Contents of this sub-folder:
  - credentials
  - est_auth.crt
  - est_auth.key
  - secure_config.json
- Readme.md

Contents of the **appviewx_est_client_Installer** folder:



- appviewx_est_client_installer
- bin
- input

  Contents of this sub-folder:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



- appviewx_client
- config.json
- Readme.md

Downloading and Extracting the EST Client in Windows Machine

- Prerequisites for the EST Client Agent Installation on a Windows Machine
- Downloading the EST Client

Prerequisites for the EST Client Agent Installation on a Windows Machine

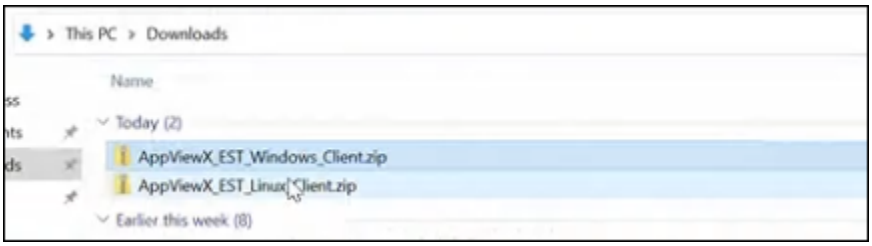
- Configure EST server in AppViewX.
- Admin access is required to run AppViewX EST Client.
- OS Requirements (Windows: v7.0 and above).
- Ensure that the firewall configuration permits communication from the EST client. (Port 30021 for both on-prem and SaaS setup)
- If load balancer is involved in the network infrastructure for the endpoint to communicate with EST agent, please ensure that load balancer does not terminate the client authentication certificate. If it terminates, then EST authentication mode should be set as “**Certificate TLS with HTTP as fallback**” in EST endpoint configuration in AppViewX.

Downloading the EST Client

To download the EST client:

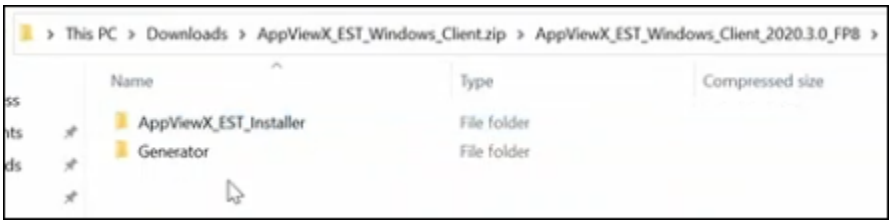
1. Login to the AppViewX release portal.
2. Download the **AppViewX_EST_Windows_Client.zip** file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



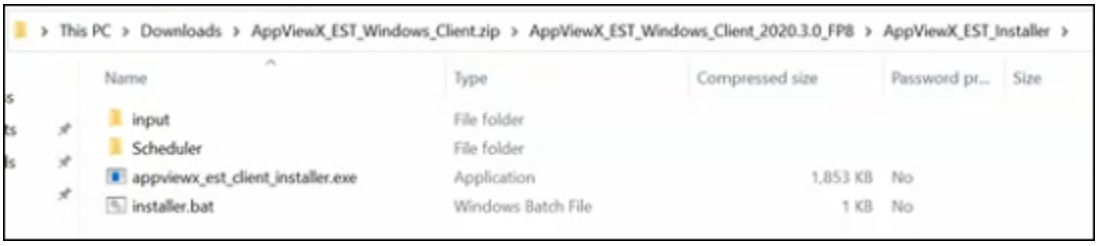
3. Extract the zip file to the desired file location.

   The extracted file contains the following two subfolders:



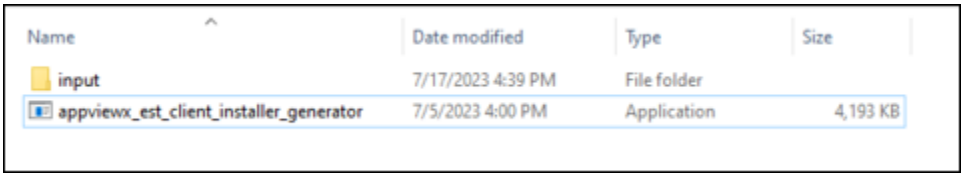
   - AppViewX_EST_Installer
   - Generator

   Contents of the **AppViewX_EST_Installer** folder:



   - input
   - Scheduler
   - appviewx_est_client_installer.exe
   - installer.bat

   Contents of the **Generator** folder:



   - input
   - appviewx_est_client_installer_generator.exe

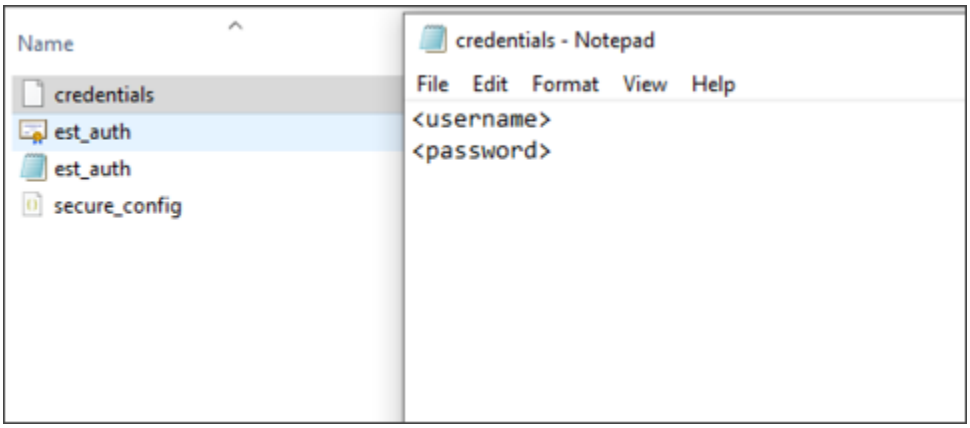
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Configuring the AppViewX EST Client for Redistribution to End-Users (Linux and Windows)

1. Navigate to the following extracted folder:
   - For Linux: **appviewx_est_client_installer_generator → input**
   - For Windows : **AppViewX_EST_Windows_Client → Generator → input**
2. Replace the following files from the input folder with your authentication key and certificate with the same names. Also make sure that the key file is not encrypted and the certificate file is present in ".crt" format. (This certificate needs to be trusted by the EST server. The issuer certificate must be configured in the EST server setting under the option **Client Authentication -> Issuer Certificate**):
   - est_auth.crt
   - est_auth.key
3. Open the **credentials** file in the Notepad editor and add the following details in two separate lines:

```
<username>

<password>
```



Note:
- The username and password are the values which are configured in the agent setting under Client Authentication in EST agent server settings.
- This step is not necessary when the **Authentication Mode** is set to "**Only Certificate TLS**" in AppViewX EST agent setting.
- When the Fallback credentials under Client Authentication is set to "Logged on user credentials" in server side. Enter the AppViewX web username and password (used to login into the AppViewX web page/UI) in the credentials file. (This feature is only available from AppViewX server version "Ganga - 2022.1.0" and later)

4. Open **secure_config.json** and edit the configuration file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

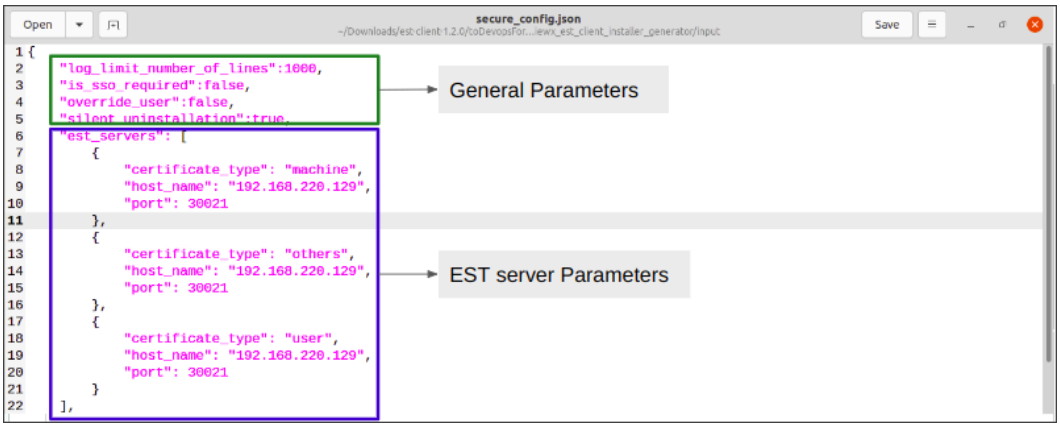
The details of the parameters are described below.

Structure of the **secure_config.json** file:

- **General parameters** - Comprises general configuration parameters such as log limit values and the option for silent uninstallation.
- **EST server parameters** - In this section, you can provide the configuration details of EST server like hostname, port number, and path_seg (which represents the agent name in the server settings) specific to the certificate type.
- **Certificate parameters** - For the mentioned certificate_type in the EST server parameters, you can provide certificate-specific details in this section. These details include CSR parameters, SAN details and the configuration related to reenrollment.

For more details regarding the parameters, please refer to the tables below.

Figure 5. Sample secure_config.json file



Field descriptions for the general section parameters

Parameters - General	Type	Description
log_limit_number_of_lines	Integer	This parameter indicates the line count determining when the current log file is saved with a timestamp included in the file name and a fresh log file is generated for subsequent utilization.
silent_uninstallation	Boolean	This field is accessed by secure_config.json during the installation process. If the value is **true** then the user will not be prompted to uninstall the previously installed versions. If the value is **false** then the user will be prompted to uninstall the previous client.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters - General	Type	Description

install_for_all_users	Boolean	Accessible by secure_config.json.
		• This field is used to avoid multiple installations of AppViewX client in multiple places.
		• If this field is true then the installation must have admin access, and this will be installed in HKEY_CURRENT_USER registry
		• If this field is false, then
		  • no admin access is required and client will be installed in HKEY_LOCAL_MACHINE registry
		  • the EST task schedulers will not be created, since this task creation requires admin privileges. This option is mainly used for non C:\ folder installation and manual est auto commands
		• If the client is installed again, then based on this flag the installed path is obtained from windows registry and that client is uninstalled and the reinstallation happens again.

override_user	Boolean	The boolean value (true/false) determines which certificate parameters that are to be considered during the installation. If enabled then the end user can override the config.json's certificate parameters value over the secure_config.json's value. This is applicable only for the certificate section field values. Precedence table based on this field is as given below.

Precedence table for the certificate section based on the *override_user* Flag

	override_user flag	Values in secure_config.json	Values in config.json	Result - Values taken from
Certificate section	FALSE	Present	Absent	secure_config.json
		Absent	Present	config.json
		Absent	Absent	Do nothing
		Present	Present	secure_config.json

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

	override_user flag	Values in secure_config.json	Values in config.json	Result - Values taken from
Certificate section	TRUE	Present	Absent	secure_config.json
		Absent	Present	config.json
		Absent	Absent	Do nothing
		Present	Present	config.json

Field descriptions for the EST server section parameters

Parameters - EST Server Section	Type	Description
certificate_type	String	This parameter is **mandatory** and **case insensitive**. It can only have the following values • auth • user • machine • others Duplicate values are not allowed.
host_name	String	A valid IP/FQDN provided in EST end point configuration. For SAAS use Cloud Connector IP/FQDN as provided in the end point configuration
port_number	Integer	The port number whose value should be from 1 to 65535. Ensure it is the same as the port number found in the EST endpoint configuration in AppViewX GUI (Default port is 30021).
path_seg	String	It is the EST endpoint setting name from the AppViewx GUI. It should not have space in between, if the path segment is not available in both secure and config json files then the default EST path segment will be considered.

After configuring the server and the general parameters, The certificate section needs to be configured. The below image provides the example of the certificate section. The certificate section must be configured for the certificate_types mentioned in the EST server section.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
    "certificates": [
        {
        "certificate_id":1,
            "certificate_type": "machine",
            "certificate_country": "IN",
            "certificate_province": "TN",
            "certificate_locality": "Coimbatore",
            "certificate_organization": "AppViewX Inc.",
            "certificate_organization_unit": "PE",
            "reenrollment_trigger_before_no_of_days_of_expiry": 42,
           "fetch_san_details":"dynamic",
           "san_dns_names":["localmachine.appviewx.com","localmachine2.appviewx.com"],
       "fetch_san_details":"dynamic",
            "custom_values":[
                {
              "field_name": "san_rfc822name",
              "base_value": "$MACHINE",
              "additional_value": "@appviewx.com",
              "operation": "append"
            }
            ]
        },
        {
        "certificate_id":2,
            "certificate_type": "others",
            "certificate_country": "IN",
            "certificate_province": "TN",
            "certificate_locality": "Coimbatore",
            "certificate_organization": "AppViewX Inc.",
            "certificate_organization_unit": "PE",
            "common_name":"secure.appviewx.com",
            "reenrollment_trigger_before_no_of_days_of_expiry": 42
        },
```

```
        {
        "certificate_id":3,
            "certificate_type": "user",
            "certificate_country": "IN",
            "certificate_province": "TN",
            "certificate_locality": "Coimbatore",
            "certificate_organization": "AppViewX Inc.",
            "certificate_organization_unit": "PE",
            "reenrollment_trigger_before_no_of_days_of_expiry": 42,
            "fetch_san_details":"dynamic",
            "san_dns_names":["localuser.appviewx.com","localuser2.appviewx.com"],
            "custom_values": [
         {
              "field_name": "common_name",
              "base_value": "$USER",
              "additional_value": "@appviewx.com",
              "operation": "prepend"
            }
    ]
        },
        {
            "certificate_id":4,
            "certificate_type": "auth",
            "reenrollment_trigger_before_no_of_days_of_expiry":380
        }
    ]
}
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Field descriptions for the certificate section parameters

Parameters - Certificate Section	Type	Description
certificate_type	String	This parameter is **mandatory** and **case insensitive**. It can only have the following values • **auth**: Generates the common name based on the auth file **est_auth.crt** present in the **input** subfolder within the folder mentioned below • *Linux* : **appviewx_est_client_installer_generator** • *Windows* : **Generator** • **user**: Generates Logged in Username as CN for the CSR. • **machine**: Generates Machine as CN for the CSR. • **others**: Generates configured common_name as CN for the CSR and installs the certificate in the key_store.
certificate_id	Integer	This parameter is **mandatory** and contains the certificate id. Duplicate values are not allowed.
certificate_country	String	The country code and should be in ISO standards (i.e. 2 letter code).
certificate_province	String	The province name; it should be up to 128 characters.
certificate_locality	String	The locality name; it should be up to 128 characters.
certificate_organization	String	The organization name; it should be up to 64 characters.
certificate_organizationUnit	String	The organization unit; it should be up to 64 characters.
reennrollment_trigger_before_no_of_days_of_expiry	Integer	The number of days before which a re-enrollment can be triggered. The value can be up to 36500.
common_name	String	Can't have more than 64 characters - Mandatory for "**others**" certificate type
san_dns_names	List [string]	Can't have more than 255 characters - should be a proper FQDN
san_ip_addresses	List [string]	Should be valid ip addresses

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters - Certificate Section	Type	Description
store_name *[Applicable for Windows ONLY]*	String	If certificate type is “others” then store name should be either “user” or “machine”
certificate_email_address	String	Can't have more than 255 characters - Should be a valid email address
fetch_san_details	String	Can have the values as “dynamic” or “static” • If the flag is not present it is considered as static • This flag is only applicable in the secure_config.json • If set to dynamic - The SAN values are fetched dynamically from the DB which is internally mapped to a collection and can be updated through a workflow, And if there are any changes/updates in the SAN values. The certificate is re-enrolled with the updated SAN values even though the certificate is not due for renewal • If set to static - The SAN values are NOT fetched dynamically and instead fetched from the configuration file
custom_values	Custom values provided are framed during EST client run time to frame the field values that trigger the enrollment. They can be accessed by both config.json and secure_config.json. THe custom values are defined below.	
field_name	-	common_name or san_rfc822name to which the values need to be added.
base_value	-	The $MACHINE or $USER or any other value. If it’s $MACHINE then the machine name is considered, if it’s $USER then it will be the machine logged in user name.
additional_value	-	Any specific value

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters - Certificate Section	Type	Description
operation	-	Values can be **append** or **prepend**. • If the value is **append** then the final value will be, fieldvalue = base_value + additional_value. • If the value is **prepend** then the final value will be, fieldvalue = additional_value +base_value. If the field name is san_rfc822name then the final value will be added in CSR's SAN value.

Note: The above parameters are accessed by **config.json** and **secure_config.json** unless specified.

Note:

- It is not mandatory to have all types in the config file. You can keep only the required type and delete the others. For example, if the requirement is to enroll only User CERT, then delete "machine" and "others" from the list.
- If there are some missing fields/parameters in the **secure_config.json** then those will be ignored, and not made as mandatory fields. This is because the user can configure the missing fields in the **config.json** present in the installer folder.

Generator And Installer For EST Client in Linux Machine

Note: If the files are not in executable format then execute the command below to change it to an executable file:

```
chmod +x <file_name>
```

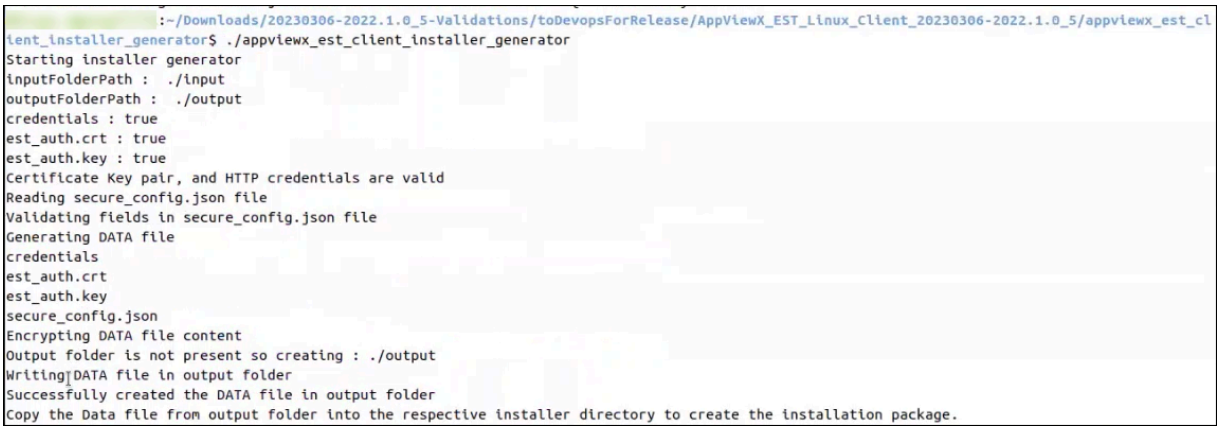

- AppViewX EST Installer Generator Steps for Linux
- EST Agent Installation Steps for Linux
- Verification
- Triggering Enrollment Request

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

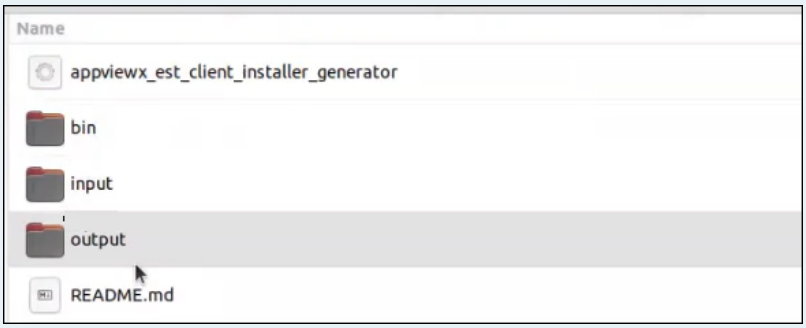
AppViewX EST Installer Generator Steps for Linux

1. Go to the **appviewx_est_client_installer_generator** folder.
2. Right click and select **Open in terminal**
3. Execute the following command

```
./appviewx_est_client_installer_generator
```



Troubleshooting: If the execution outcome displays errors, correct the values or parameters in the **secure_config.json** file and re-execute until it successfully creates the DATA file. The Data file is created in the **output** subfolder within the **appviewx_est_client_installer_generator** folder.



4. To create the installation package, navigate to **appviewx_est_client_installer_generator > output** and copy the DATA file present there and paste it into the **appviewx_est_client_installer > input** folder.
5. In the same **input** folder, (**appviewx_est_client_installer > input**), verify the **config.json** file.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Enter similar details as in the **secure_config.json** file mentioned in the section Configuring the AppViewX EST Client for Redistribution to End-Users. If the user needs to make changes over the admin configured values in secure_config.json. Then those can be made in config.json, provided that the **overrider_user_flag** is set to **true**. (Please refer the **Precedence Table for Certificate Section based on the override_user Flag**)

Now, the EST client folder (**appviewx_est_client_installer**) can be sent to the client machines, where the AppViewX EST Client needs to be installed. The admin performs the generation steps just once, and then the installer for the AppViewX EST client installer is shared with other users. The DATA file inside the appviewx_est_client_installer folder has all the configuration details provided during the generation of the AppViewX EST client installer.

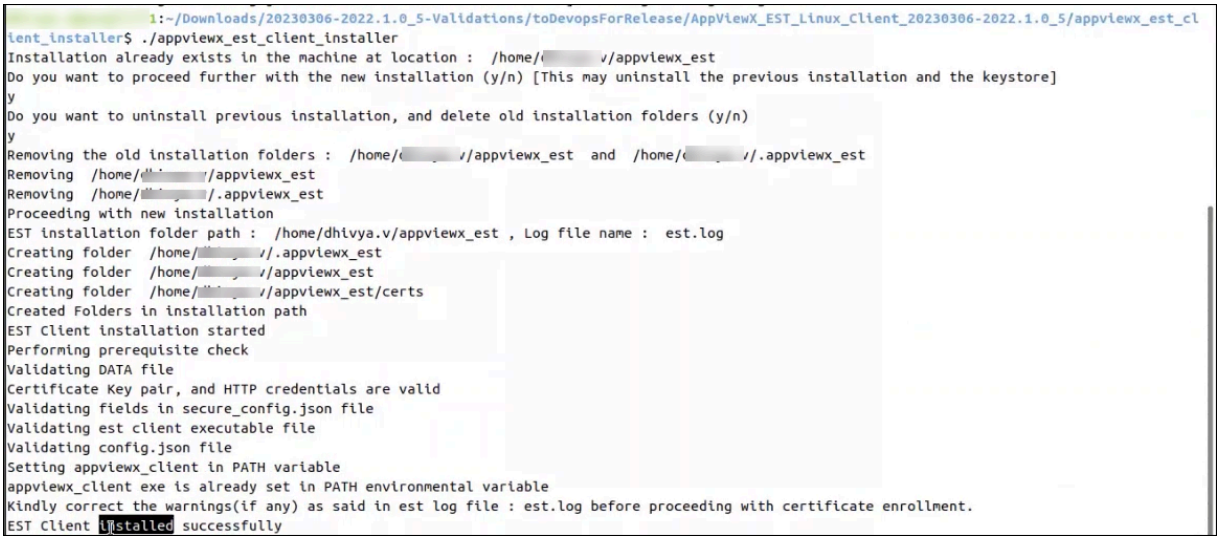
EST Agent Installation Steps for Linux

This step needs to be done on every machine where the EST client needs to be installed. Whereas the installer generation steps are done once by the admin.

If configuration changes are required in the certificate section and the **override_user** flag is set to **true**, during the generation of the EST agent, the user can make changes in the certificate section in the **config.json** file inside the **appviewx_est_client_installer** → **input** folder.

1. Go the **appviewx_est_client_installer** folder, right click and select **Open in terminal**.
2. Execute the following command:

```
./appviewx_est_client_installer
```



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- If there are errors in the config.json file, then correct the errors and execute the installer again. (The log files for the installation is saved in the file **appviewx_est_client_installer → appviewx_est_client_installer.log**)
- During installation every field in secure_config.json and config.json are checked and compared based on the **override_user** flag as mentioned in the table below. If any mandatory fields are missing/invalid then all the errors are gathered and displayed to the user and asking them to correct it before going in for the enrollment and the installation proceeds.
- If there is a previous client installation already available in the home folder and if the "silent_uninstallation" flag is set to true then the user will not be prompted to uninstall, if it's set to false then the user will be prompted to uninstall.
- If you enter Y and proceed then you would be prompted to delete the old installation folders. If you enter Y the old installation is deleted and proceed with the new installation, or else it will quit the program.
- Client is automatically installed in the User **Home** folder. The following folders are created in the Home folder after installation is complete.
  a. appviewx_est
  b. .appviewx_est
- Certificates are stored in the keystore folder under this filepath **/Home/<username>/.appviewx_est/key_store/key_store**. This can only be found after fetching the required certificates from the server.
- If you unknowingly delete the **appviewx_est** and **.appviewx_est** home folders, then this installation will be considered as a new installation.
- Users can execute the **appviewx_client** commands anywhere from the machine as this executable is included in the environment PATH variable. To do so, ensure to reload the .bashrc file. This is only done once at the time of installation. You can either run the command `source ~/.bashrc` or simply close and reopen the terminal.
- The latest log file for the AppViewX EST client can be found in the name of **est.log** and the old files are saved with time stamps as their file names. These logs are found in the **appviewx_est** folder present in the **home** folder.

3. To install with cron expression, execute the following command:

```
./appviewx_est_client_installer -cron “* * * * *”
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

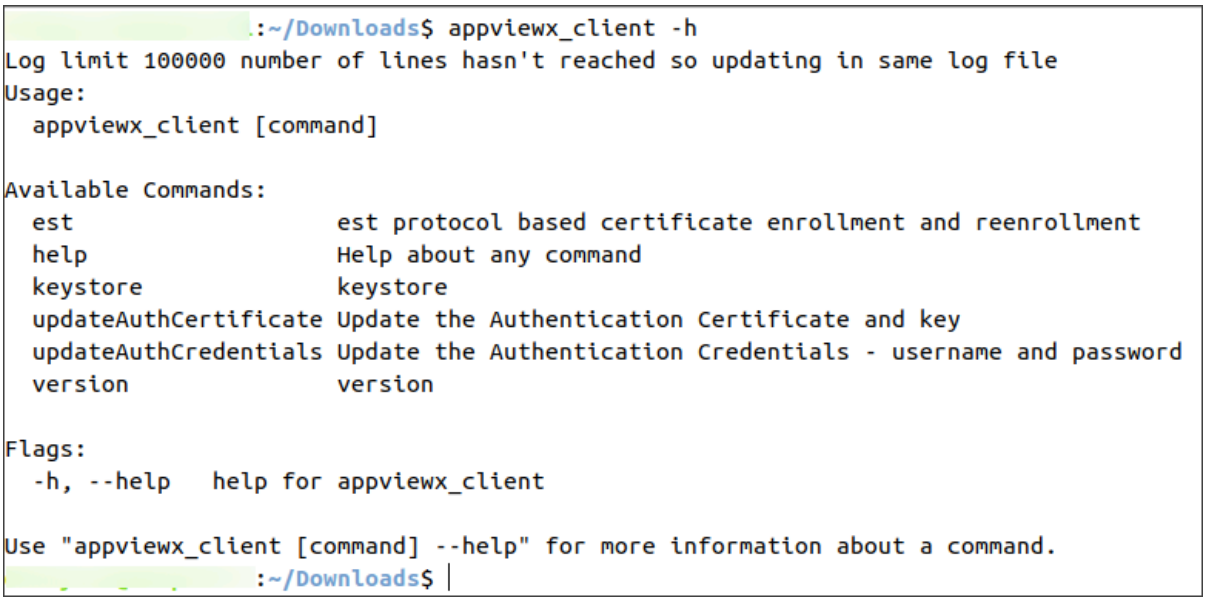
- This command installs the EST client and creates a crontab in the linux machine with the provided cron expression. Then the linux crontab daemon will then trigger the **appviewx_client est auto** command automatically in that particular time interval.
- The above cron expression is a sample command to trigger the est auto after every minute.
- To verify the cron jobs use the command `crontab -l`

The generated installation logs are captured in a log file called **appviewx_est_client_installer.log** in the same folder where the installer file is located.

Verification

1. To list the commands to be executed for verification, execute the following command:

```
appviewx_client -h
```



2. For more information about a command, execute the following command:

```
appviewx_client --help
```

If the command does not work due to any reasons then go to the **~/appviewx_est** folder and execute one from the following commands:

- To list the commands, execute the following command:

```
./appviewx_client -h
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
                  :~/appviewx_est$ ./appviewx_client -h
Log limit 100000 number of lines hasn't reached so updating in same log file
Usage:
  appviewx_client [command]

Available Commands:
  est                   est protocol based certificate enrollment and reenrollment
  help                  Help about any command
  keystore              keystore
  updateAuthCertificate Update the Authentication Certificate and key
  updateAuthCredentials Update the Authentication Credentials - username and password
  version               version

Flags:
  -h, --help   help for appviewx_client

Use "appviewx_client [command] --help" for more information about a command.
```

- For more information about a command, execute the following command:

```
./appviewx_client --help
```

Triggering Enrollment Request

1. Go to the **Home/appviewx_est** folder, right click, and select **Open in Terminal**.
2. Execute the following command:

```
appviewx_client est auto
```

```
                  :~/Downloads/20230306-2022.1.0_5-Validations/toDevopsForRelease/AppViewX_EST_Linux_Client_20230306-2022.1.0_5/appviewx_est_cl
ient_installer$ appviewx_client est auto
Validating the config.json file
Making Enrollment
Initiating Call  avxpll771.appviewx.com machine
Added a Certificate to Keystore ID : 0, SerialNumber : 4E0F5A037572E2449160D9B9AD6E8F91
Making Enrollment
Initiating Call  secure.appviewx.com others
Added a Certificate to Keystore ID : 1, SerialNumber : 1EF5F92BC76CFEDAC96EC24E7A8DF6C
Agent Execution Completed
```

3. To view the list of certificates created, execute the following command:

```
appviewx_client keystore list
```

```
dhivya.v@avxpll771:~/Downloads/20230306-2022.1.0_5-Validations/toDevopsForRelease/AppViewX_EST_Linux_Client_20230306-2022.1.0_5/appviewx_est_cl
ient_installer$ appviewx_client keystore list
+-------------------------------------------------------------------------------------------------------------------------------------------------
-----------------+
|ID   |Common Name             |SerialNumber                                |Download Type  |Created Date                |Expiry Date
                 |
+-------------------------------------------------------------------------------------------------------------------------------------------------
-----------------+
|0    |avxpll771.appviewx.com    |4E0F5A037572E2449160D9B9AD6E8F91                |p12            |Mon Mar 20 15:17:46 2023      |Tue Mar 19 2
3:59:59 2024      |
|1    |secure.appviewx.com       |1EF5F92BC76CFEDAC96EC24E7A8DF6C                 |p12            |Mon Mar 20 15:17:59 2023      |Tue Mar 19 2
3:59:59 2024      |
+-------------------------------------------------------------------------------------------------------------------------------------------------
```

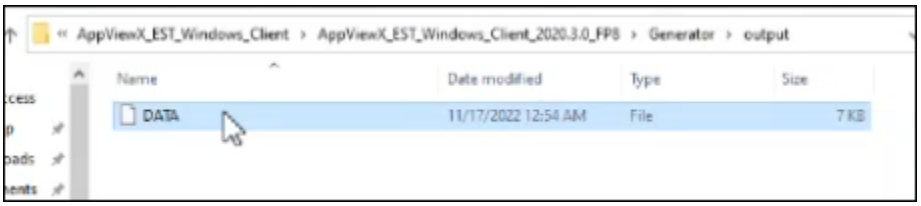
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Generator and Installer for EST Client in Windows Machine

- AppViewX EST Installer Generator Steps for Windows
- EST Agent Installation Steps for Windows

AppViewX EST Installer Generator Steps for Windows

1. Go to the extracted folder **AppViewX_EST_Windows_Client → Generator → input**
2. Run the installer file **appviewx_est_client_installer_generator.exe** (right-click the file and select **Run as administrator**).
   A folder named **output** will be generated in the same directory. If the **output** folder is not created, please review the secure_config.JSON file for potential errors and attempt the same step again.
3. Go to the **AppViewX_EST_Windows_Client → Generator → output** folder.
   A file named DATA is created as a result of the execution of the above installer file.



4. Copy this DATA file and place it in the **AppViewX_EST_Installer → input** folder.
5. In the same **input** folder, verify the **config.json** file.

> **Note:** Enter similar details as in the **secure_config.json** file mentioned in the section Configuring the AppViewX EST Client for Redistribution to End-Users. If the user needs to make changes over the admin configured values in secure_config.json. Then those can be made in config.json, provided that the **overrider_user_flag** is set to **true**. (Please refer the **Precedence Table for Certificate Section based on the override_user Flag**)

6. Navigate to the **Scheduler** folder (**AppViewX_EST_Installer → Scheduler)** and verify the files as shown below.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

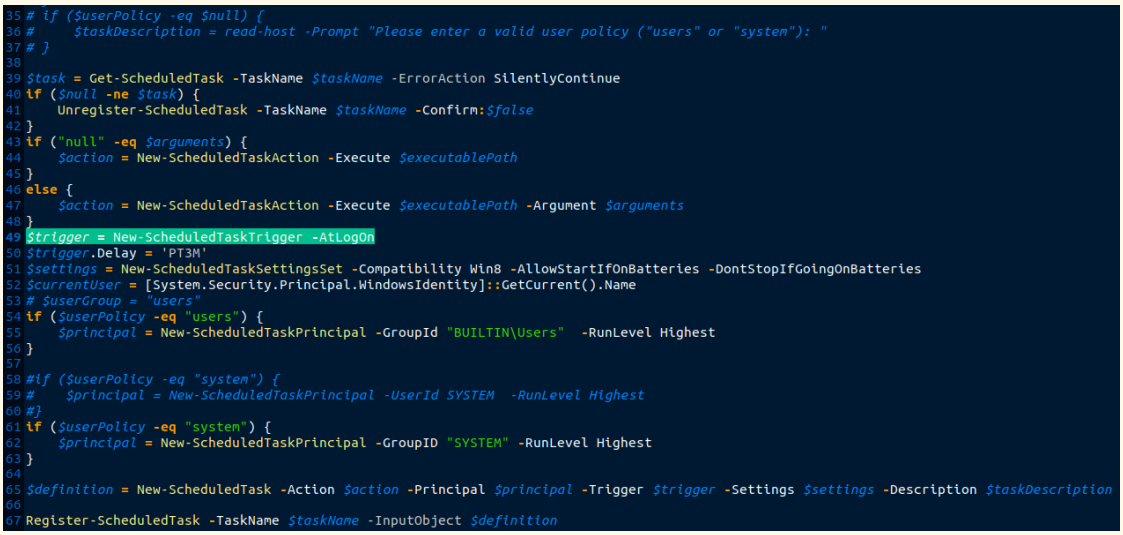
It contains the following details:

- **triggerJobSystem.ps1**: PowerShell Script for creating machine enrollment schedule task. The default trigger is at User LogOn.
- **triggerJobUsers.ps1**: PowerShell Script for creating user enrollment schedule task. The default trigger is at User LogOn.

Attention: By default the triggers will be at LogOn. You can customize it by following the steps below. To change this to trigger at a particular time daily.

a. Open the triggerjobSystem.ps1 which is responsible for scheduling the task for “auth” and “machine” certificate. Replace the following line which is responsible to trigger a task by log-on (shown in the below image) to *$trigger = New-ScheduledTaskTrigger -Daily -At "HH:MM."* This triggers the task everyday at the specified time HH:MM.

b. Similarly make the same changes in “triggerJobUsers.ps1” file. Esure that both the tasks are scheduled with sufficient time difference between them.



```
# if ($userPolicy -eq $null) {
#     $taskDescription = read-host -Prompt "Please enter a valid user policy ("users" or "system"): "
# }

$task = Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue
if ($null -ne $task) {
    Unregister-ScheduledTask -TaskName $taskName -Confirm:$false
}
if ("null" -eq $arguments) {
    $action = New-ScheduledTaskAction -Execute $executablePath
}
else {
    $action = New-ScheduledTaskAction -Execute $executablePath -Argument $arguments
}
$trigger = New-ScheduledTaskTrigger -AtLogOn
$trigger.Delay = 'PT3M'
$settings = New-ScheduledTaskSettingsSet -Compatibility Win8 -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries
$currentUser = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
# $userGroup = "users"
if ($userPolicy -eq "users") {
    $principal = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Users"  -RunLevel Highest
}

#if ($userPolicy -eq "system") {
#    $principal = New-ScheduledTaskPrincipal -UserId SYSTEM  -RunLevel Highest
#}
if ($userPolicy -eq "system") {
    $principal = New-ScheduledTaskPrincipal -GroupID "SYSTEM" -RunLevel Highest
}

$definition = New-ScheduledTask -Action $action -Principal $principal -Trigger $trigger -Settings $settings -Description $taskDescription

Register-ScheduledTask -TaskName $taskName -InputObject $definition
```

Now, the EST client folder (**AppViewX_EST_Installer**) can be sent to the client machines, where the AppViewX EST Client needs to be installed. The admin performs the generation steps just once, and then the installer for the AppViewX EST client installer is shared with other users. The DATA file inside the AppViewX_EST_Installer folder has all the configuration details provided during the generation of the AppViewX EST client installer.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EST Agent Installation Steps for Windows

This step needs to be done on every machine, where the EST client needs to be installed. Whereas the installer generation steps are done once by the admin.

If configuration changes are required in the certificate section and the **override_user** flag is set to be true, during the generation of the EST agent, the user can make changes in the certificate section present in the **config.json** file inside the **appviewx_est_client_installer →input** folder.

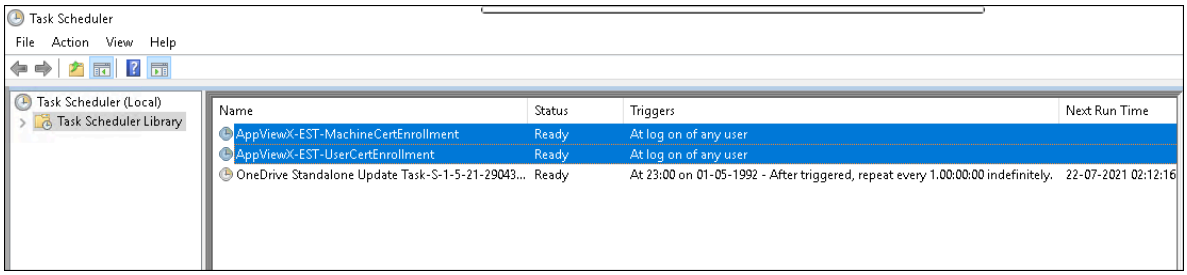
1. To install the agent software:

   a. Open the **AppViewX_EST_Installer** folder and then select the **installer.bat** file.

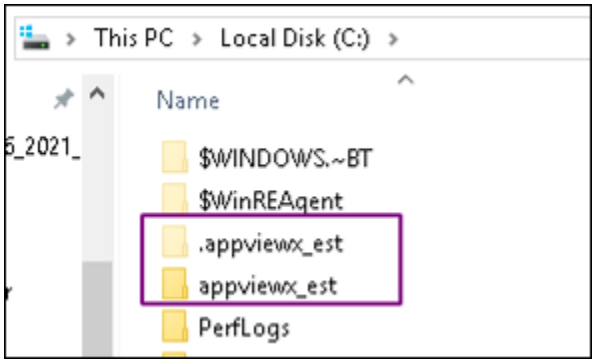
   b. Right click then select **Run as administrator**.
      - It creates **Machine** and **User Enrollment** tasks in the Windows Task Scheduler.
      - It encrypts the software with machine-unique parameters and copies to **C:/Drive**.

2. After the installation:

   a. Create **Machine** and **User enrollment** tasks in the task scheduler.



   b. Copy the files to the **C** drive

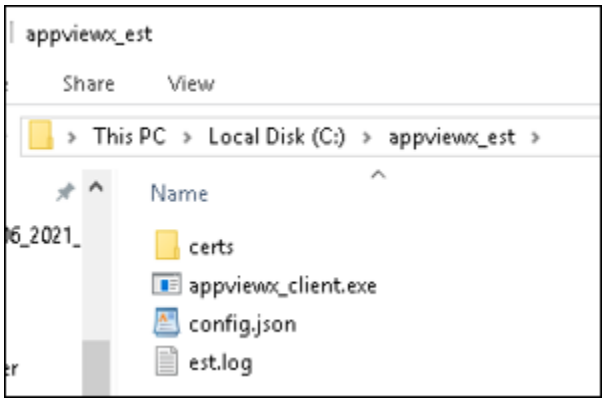


.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

> **Note:** Check whether appviewx_est and the .appviewx_est have all the permissions to write, read, and modify. If not then provide the necessary permissions.

c. Validate whether the config.json file is present in **C:/appviewx_est/config.json**.

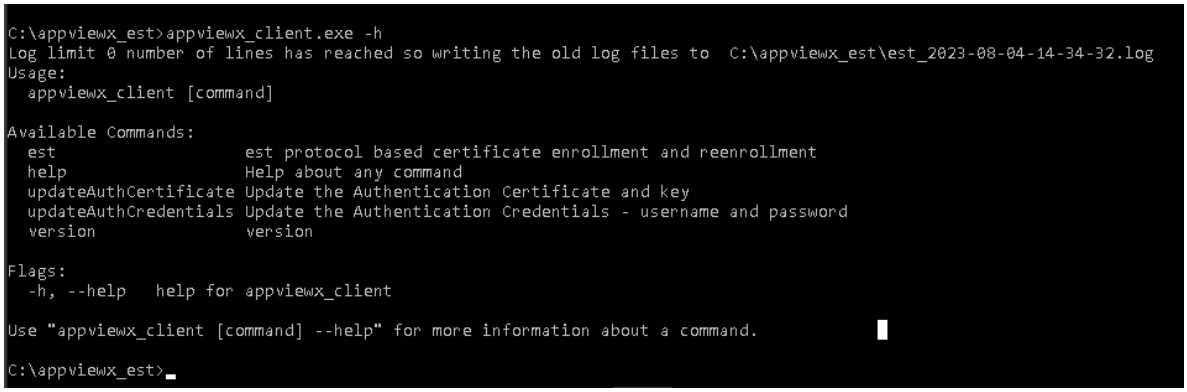


d. Open the command prompt with administrator privileges and navigate to **C:/appviewx_est**.

e. Execute the following command:

```
appviewx_client.exe -h
```

A list of commands is displayed to help users with different processes as shown below.



3. To trigger the enrollment task:

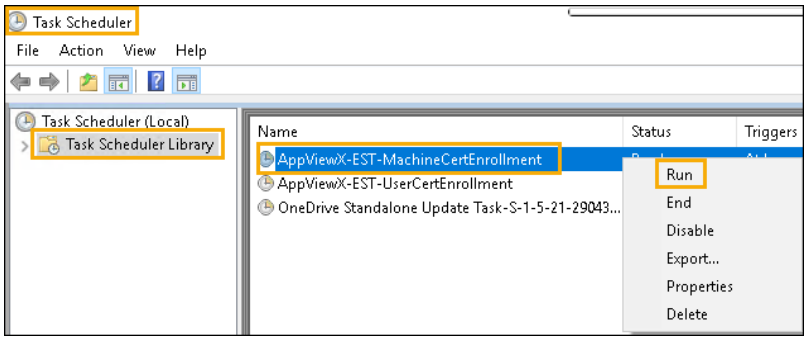
> **Note:** This agent can either trigger automatically when a user logs in or manually from the Task Scheduler.

a. Open the task scheduler library, and select the **AppViewX-EST-MachineCertEnrollment** file. Once the user logs out the system and logs back in , then the enrollment/reenrollment will be triggered automatically.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

b. Right-click and then select **Run** to run the tasks.

> **Note:** Within 30 seconds, the certificates will be installed in the store.



Enrollment request can be triggered from running the task from the task scheduler or can also be triggered by the following steps.

1. Open the command prompt with administrator privileges and navigate to **C:/appviewx_est**
2. Execute the command

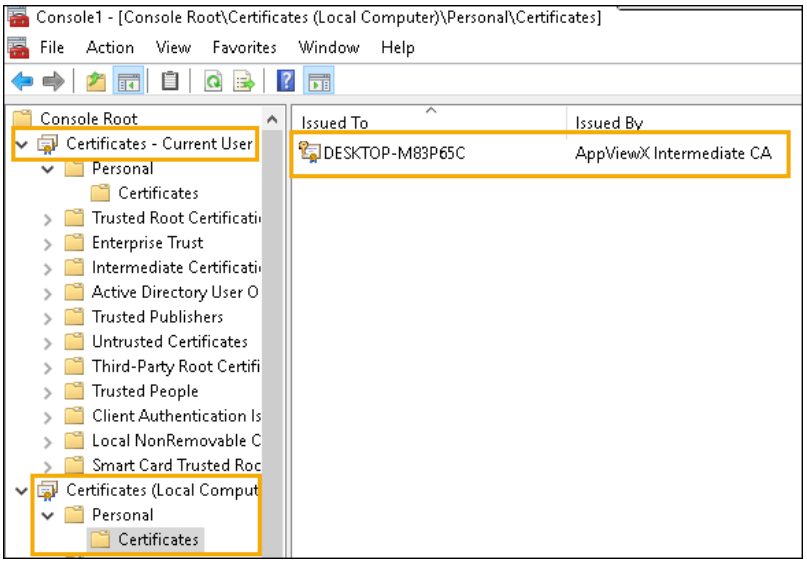
```
appviewx_client.exe est auto
```

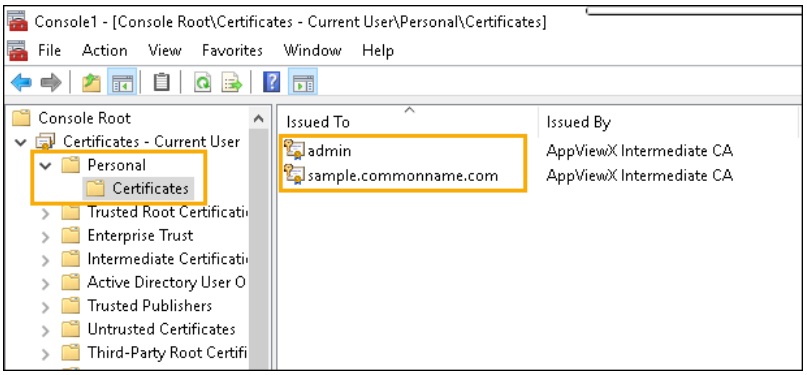
Within 30 seconds, the certificates will be installed in the store.

The latest log file for the AppViewX EST client can be found in the name of **est.log** and the old files are saved with time stamps as their file names. These logs are found in the **appviewx_est** folder present in the **C:/** drive.

The certificates are created based on the configurations provided. The **machine** type certificate can be found in the Machine certificate store whereas the **user** and the **others** type certificates are present in the User certificate store. The certificates are present in the sections as mentioned in the images below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Available Commands and Features in EST Client

- List of Available Commands and their Description
- Auto-Enrollment and Re-enrollment
- Manual Enrollment and Re-enrollment [Linux only]

List of Available Commands and their Description

Table of Available Commands and their Description

Available commands	Description
est	EST protocol based certificate enrollment and reenrollment.
help	Help about any command.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Table of Available Commands and their Description (continued)

Available commands	Description
keystore	Listing the certificates in the keystore.
updateAuthCertificate	Update the Authentication certificate and key. Example `appviewx_client updateAuthCertificate --authCert “<certificate path>” --authKey “<keypath>”`
updateAuthCredentials	Update the Authentication Credentials - username and password. You will be prompted to enter the username and the password after running this command.
version	Version details.

Note: For more details, use “`-h`” besides the command to list all the features/details under the specified command.

Auto-Enrollment and Re-enrollment

- Auto-enrollment or re-enrollment is accessed through the following command:

```
appviewx_client est auto -
```

  This enrolls certificates based on the **secure_config** and the **config** files.
- If certificates are already enrolled, then the validity of the certificates are checked with the value **reenrollment_trigger_before_no_of_days_of_expiry** present in the configuration files. If the pending validity of the certificate **reenrollment_trigger_before_no_of_days_of_expiry**, then re-enrollment is triggered, otherwise, no operation is performed.

Manual Enrollment and Re-enrollment [Linux only]

- Manual enrollment and re-enrollment do not come under any certificate type mentioned in the configuration files.
- Manual enrollment is accessed through the following command:

  Example 1:

```
appviewx_client est manual-enrollment csr-mode --csr-file <csr-file-complete-path> --est-server-url <est-server-url>
```

  Example 2:

```
appviewx_client est manual-enrollment csr-mode --csr-file <csr-file-complete-path> --est-server-hostname <est-server-hostname> --est-server-pathseg
 <est-server-pathsegment/agent name>
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The description for every parameter is given in the table below:

Flags	Input Type	Description
--csr-file	string	Input CSR filename Example: /home/user/test.csr
--est-server-hostname	string	EST server hostname
--est-server-pathseg	string	EST server name present in the server setting (default value: defaultEST)
--est-server-port	int	EST server port number configured in the EST server settings (default value: 30021)
--est-server-url	string	EST server URL present in the est server setting page. (Not required if the hostname, port, and pathseg are given.)

- Manual re-enrollment is triggered using two modes:
  - **csr-mode**

    Ensure that the certificate corresponding to the csr sent is present in the inventory before triggering the re-enrollment.

    Example 1:

    ```
    appviewx_client est manual-reenrollment csr-mode --csr-file <csr-file-complete-path> --est-server-url <est-server-url>
    ```

    Example 2:

    ```
    appviewx_client est manual-reenrollment csr-mode --csr-file <csr-file-complete-path> --est-server-hostname <est-server-hostname> --est-server-pathseg <est-server-pathsegment/agent name>
    ```

    Note: Please refer to the table found in the manual-enrollment, for the description of these parameters.

  - **cert-mode**

    Similar to the manual re-enrollment using csr-mode. The certificates should be enrolled and should be present in the inventory before triggering re-enrollment.

    Example:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
appviewx_client est manual-reenrollment cert-mode --cert-file <cert-file-complete-path> --cert-file-type <cert-file/extension-type> --est-server-hostname <est-server-hostname> --est-server-pathseg <est-server-pathsegment/agent name> --output-privatekey-file <path-to-store-private-key> --key-size <Key-length>
```

Descriptions for the flags/parameters for the manual cert-mode are given in the table below:

Flags	Input Type	Description
--cert-file	string	Input Certificate filename. Example: /home/user/test.crt
--cert-file-type	string	Input Certificate file types (cer, crt, pem, p7b)
--key-size	int	Key size of the generated Private Key. If not given, the key size is taken from the old certificate
--output-privatekey-file	string	Output Private key filename. Example: /home/user/output/ hostname.key
--est-server-hostname	string	EST server hostname
--est-server-pathseg	string	EST server name present in the server setting (default value: defaultEST)
--est-server-port	int	EST server port number configured in the EST server settings(default value: 30021)
--est-server-url	string	EST server URL present in the est server setting page. (Not required if hostname, port and pathseg are given)

Keystore

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Linux
- Windows

Linux

- To view the list of certificates created, execute the following command :

```
appviewx_client keystore list
```



```
dhivya.v@avxpll771:~/Downloads/20230306-2022.1.0_5-Validations/toDevopsForRelease/AppViewX_EST_Linux_Client_20230306-2022.1.0_5/appviewx_est_client_installer$ appviewx_client keystore list
+----------+-----------------------+----------------------------------+-------------+--------------------------+--------------------------+
|ID        |Common Name            |SerialNumber                      |Download Type|Created Date              |Expiry Date               |
+----------+-----------------------+----------------------------------+-------------+--------------------------+--------------------------+
|0         |avxpll771.appviewx.com |4E0F5A037572E2449160D9B9AD6E8F91   |p12          |Mon Mar 20 15:17:46 2023  |Tue Mar 19 23:59:59 2024  |
|1         |secure.appviewx.com    |1EF5F92BC76CFEDAC96EC24E7A8DF6C   |p12          |Mon Mar 20 15:17:59 2023  |Tue Mar 19 23:59:59 2024  |
+----------+-----------------------+----------------------------------+-------------+--------------------------+--------------------------+
```

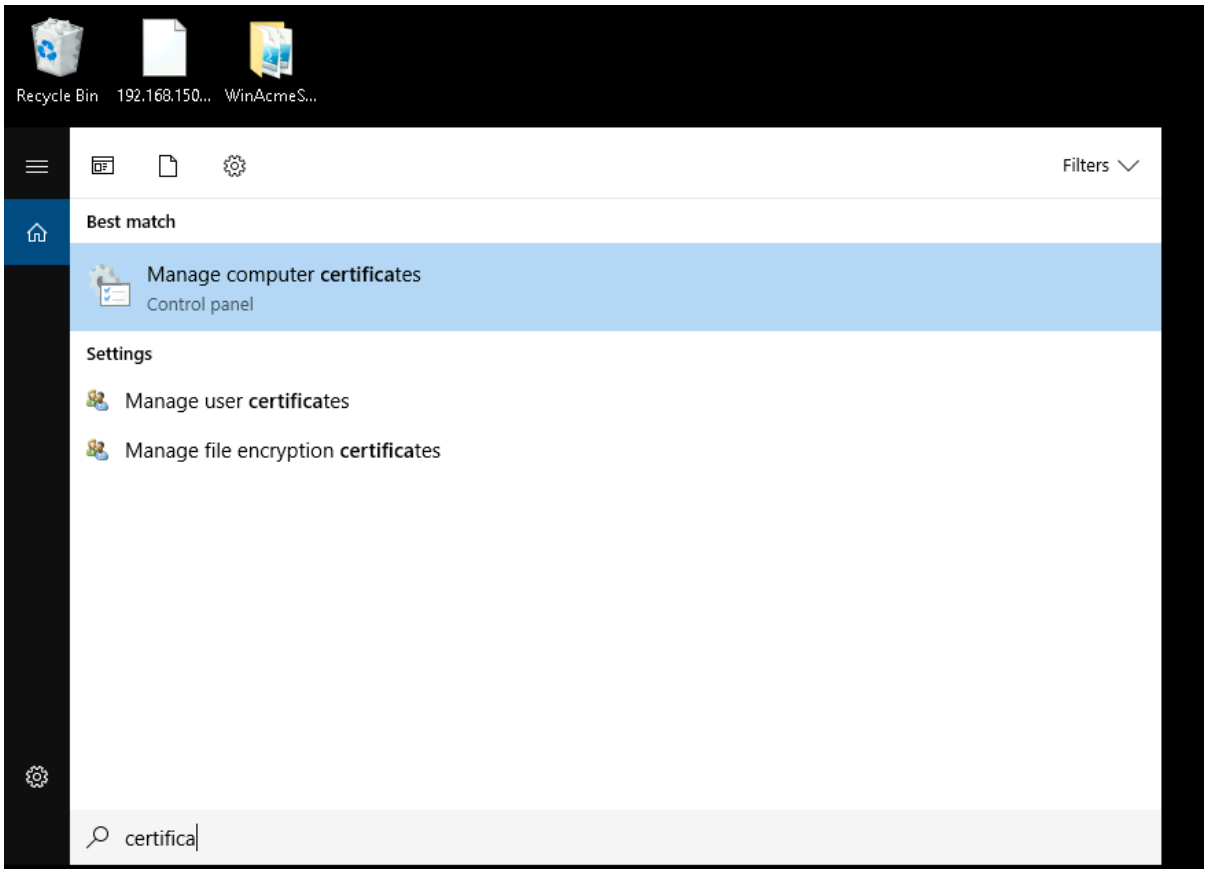
- To download the certificates based on **id** specified when using the `list` command above, execute the following command:

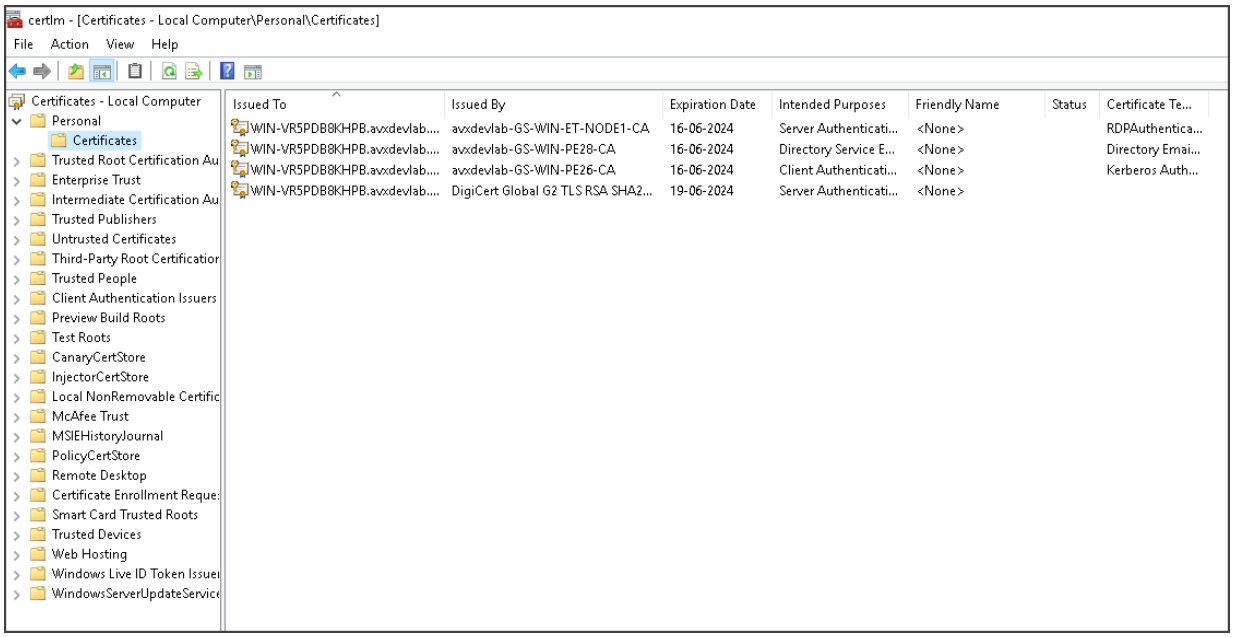
```
appviewx_client keystore download --id <id> --filepath <path to store the cert with file name and extension>
```

Windows

- To access Machine Certificate Type, go to **Start > Manage Computer Certificates**.
- To access User and Others Certificate Type, go to **Start > Manage User Certificates**.
- To view the certificates, go to **Personal > Certificates**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.





Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Troubleshooting Steps and Common Errors [Linux and Windows]

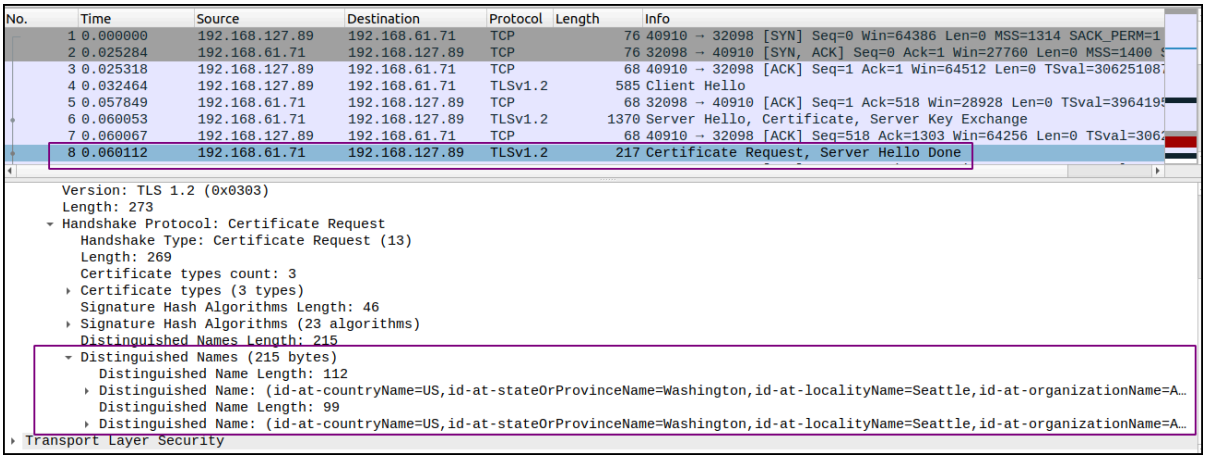
- Connection Errors
- Error Code: 401 Unauthorized
- 500-Internal Server Error
- Error Codes

Connection Errors

1. Check whether the IP address and the port number is correctly configured in the **secure_config.json** file, located in the **AppViewX_EST_Windows_Client → Generator → Input** folder.
2. Verify if the firewall policies permit the connection between the EST client and the server.

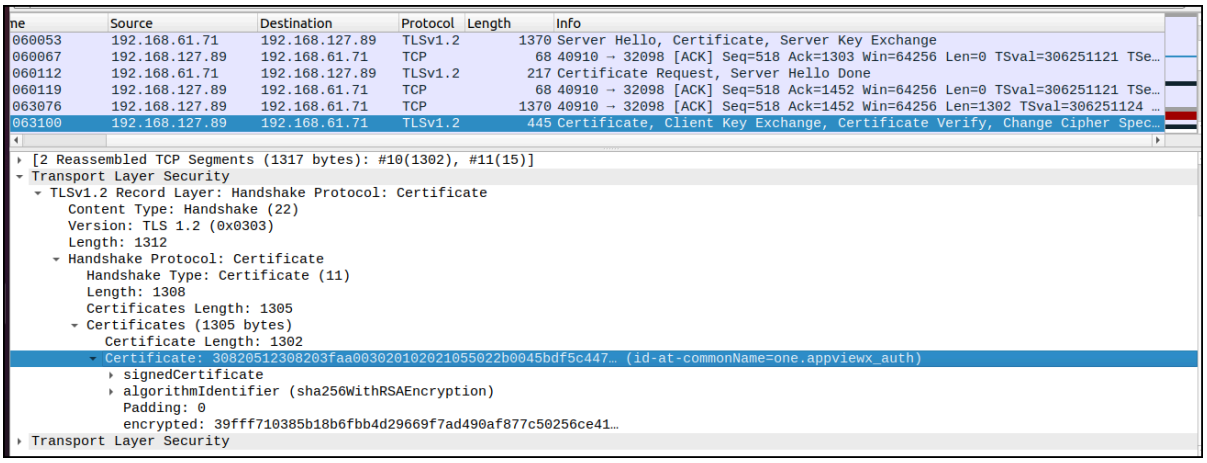
Error Code: 401 Unauthorized

1. Ensure the client sends the Authentication Certificate (try enrollment request from `curl` using the same client certificates).
2. Check the trusted CA added in the EST agent settings to validate whether the Client Authentication Certificate is signed by the Same CA.
3. If the authentication certificate is signed by a CA other than AppViewX CA, make sure it is added in the trusted CA list from the CLI.
4. Do a TCP dump and analyze the TLS transactions between server and client and make sure the client receives the Distinguished Name of the Trusted CA.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

5. In the TCP dump, make sure the client sends the Authentication Certificate in the Certificate Response field.



500-Internal Server Error

1. Make sure EST Service is running in the AppViewX Server
2. Check the EST Server Status. (Refer section: Verify EST Server Status (Enabled/Disabled).)
3. Check the EST Enrollment using `curl`. (Refer section: Testing EST Enrollment by using **CURL**).

Error Codes

Error Codes and their Descriptions

S. No.	Status Code	Error Codes	Error Messages	Description
1	500 - Internal Server Error	CERT-ENROLLMENT-001	Agent settings are not found (or) invalid for this agent	When there is no agent found for est with the specified name.
2	500 - Internal Server Error	CERT-ENROLLMENT-002	Agent settings are not valid	When EST agent settings are invalid.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
3	401 - Unauthorized	CERT-ENROLLMENT-003	Authentication failed for the auto-enrollment protocol	TLS / Basic / Digest authentication failed for the provided authentication parameters.
4	401 - Unauthorized	CERT-ENROLLMENT-006	Provided NONCE is invalid	• When TLS and HTTP auth are selected but the input doesn't contain any Basic auth value. • When TLS and HTTP auth is selected but the input doesn't contain any Digest auth value. Here Nonce is sent in the WWW-Authenticate header as per RFC.
5	500 - Internal Server Error	CERT-ENROLLMENT-007	Failure while creating nonce	When creating Nonce to send to the client in case of Digest HTTP authentication
6	500 - Internal Server Error	CERT-ENROLLMENT-008	Certificate conversion failed	While converting the certificate contents to PKCS7 format which is to be sent as a response to the client.
7	500 - Internal Server Error	CERT-ENROLLMENT-009	Error while converting to JSON	Error during map to JSON conversion.
8	401 - Unauthorized	CERT-ENROLLMENT-010	No client certificate was obtained to perform authentication.	When a client certificate is not found in the request to perform the TLS authentication.
9	500 - Internal Server Error	CERT-EST-001	Unable to get certificates requested by the client device	Could not obtain the certificates which were requested from the agent.
10	500 - Internal Server Error	CERT-EST-003	Certificate cannot be obtained after polling from the agent.	A certificate cannot be obtained even after retrying for the provided amount of time interval.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
11	500 - Internal Server Error		CSR parameters already available for selected CA.	When there is already a request present in the certificate inventory and a similar CSR is obtained for enrollment/re-enrollment.
12	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1020	Certificate enrollment failed for the provided CSR.	• Check for the request-id of the submitted CSR for further details. • Certificate or certificate creation requests may not be found to retrieve the certificate. • Exception while fetching work order mapping for the transaction id.
13	404 - Not Found	CERT-ENROLLMENT-PROTOCOL-1019	Certificate enrollment request does not exist. Please check the request sent from the AppViewX agent	The request from the EST agent is not found when received in subsystem certificate NB.
14	401 - Unauthorized	CERT-ENROLLMENT-PROTOCOL-1014	Authentication failed for the autoenrollment protocol.	When TLS authentication fails.
15	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1005	Error while fetching policy settings for an agent	When obtaining group or policy details.
16	400 - Bad Request	CERT-SCEP-1011	Unable to extract CSR in the SCEP request	Occurs when the CSR extraction fails.
17	404 - Not Found	CERT-SCEP-1012	Policy is not associated with the given certificate group	When the certificate policy for the provided agent is not present.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
18	404 - Not Found	CERT-SCEP-1013	Group policy does not have the given certificate authority	All the errors from 18 to 29 would be to validate the CSR parameters against policy
19	404 - Not Found	CERT-SCEP-1014	Group policy does not have the given hash function	
20	404 - Not Found	CERT-SCEP-1015	Group policy does not have the given key type	
21	404 - Not Found	CERT-SCEP-1016	Group policy does not have the given key length	
22	400 - Bad Request	CERT-SCEP-1017	Given common name must end with as per the common name defined in group policy	
23	400 - Bad Request	CERT-SCEP-1018	Given common name can not be same as the common name defined in group policy	
24	400 - Bad Request	CERT-SCEP-1019	Given organization must match with organization defined in group policy	
25	400 - Bad Request	CERT-SCEP-1020	Given organization unit must match with organization unit defined in group policy	
26	400 - Bad Request	CERT-SCEP-1021	Given locality must match with locality defined in group policy	

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
27	400 - Bad Request	CERT-SCEP-1022	Given state must match with the state defined in group policy	
28	400 - Bad Request	CERT-SCEP-1023	Given country must match with country defined in group policy	
29	404 - Not Found	CERT-SCEP-1024	Group policy does not have the given certificate type	
30	400 - Bad Request	CERT-CSR-0002	Failed to parse CSR, please validate the content.	CSR content is not proper while uploading it for submission
31	404 - Not Found	CERT-CA-0001	CA settings are not available.	CA setting selected in EST settings is not found
32	404 - Not Found	CERT-KEY-0003	Certificate/private key retrieval failed.	DAO exception while fetching certificate.
33	417 - Expectation Failed	CERT-CSR-0005	Csr submission failed. ${ERROR_MSG}	Custom error message from CA.
34	500 - Internal Server Error		More than one data returned from collection while fetching san list from the DB for the given server name.	More than one entry of SAN is present for the same server name.
35	500 - Internal Server Error		Error while processing.	Hookname is not mapped with the EST agent setting. Please run the DB query to add the hookname.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Best Practices for Client

- To define the mandatory CSR parameters, update the **<secure_config.json>** file in the **Installer Generator** folder.
- Use FQDN in EST Enroll and Re-Enroll URL configuration instead of mentioning server IP in the configuration.
- After the software installation, delete the **Installer** folder from the machine. The installer installs agent software in the **home** folder and it is recommended to delete the **Installer** from the machine.

EST Server Configuration Guide

This guide contains the predefined procedure for Enrollment over Secure Transport (EST) server configuration.

- Getting Started
- EST Configuration
- Gateway - EST Logs
- Verification of the EST Server
- Testing EST Enrollment by using CURL

Getting Started

- Overview
- AppViewX EST Client Security
- Prerequisites
- Enable EST Services
- Create Client Authentication Certificate Using AppViewX CA

Overview

Enrollment over Secure Transport (EST) is a simple and functional certificate management protocol. EST works in the client-server model. AppViewX offers both EST server and client functionalities with TLS based authentication between the server and client as per the protocol. This document helps with the configuration of the EST in the AppViewX GUI.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

AppViewX EST Client Security

AppViewX EST Clients provides two levels of security:

- Encrypts the authentication data using Installer Generator.
- Creates DATA-CHALLENGE during the installation using unique machine parameters and agent gets executed only when DATA-CHALLENGE decryption is successful.

AppViewX EST Installer Generator

Traditional EST Enrollment methods like curl or wget will have an Authentication Certificate kept open in the user machine.

AppViewX provides a solution to this using AppViewX Installer Generator Software, which encrypts the complete authentication data to a Single DATA file and during the installation we need to copy only the DATA file to the user machine. This restricts the user from reading or modifying authentication DATA.

AppViewX EST Installer

During the Installation of the AppViewX EST Client, it creates an encrypted DATA-CHALLENGE secret, which contains unique machine parameters and, in each execution, it triggers a request only when DATA-CHALLENGE decryption is successful. This protects agents from copying and executing from another machine.

Prerequisites

Before configuring the EST server, the user has to make the following changes in the AppViewX server:

- Make sure that the `<avx-platform-gateway-est>` and `<avx-vendor-cert-est-agent>` services are running in the cluster.

```
[appviewx@smenode2 ~]$ kubectl get services -A | grep est
external-system        avx-platform-gateway-est                NodePort    10.101.89.37     <none>        5301:30739/TCP
smedc1                 avx-vendor-cert-est-agent               ClusterIP   10.105.120.24    <none>        5306/TCP
[appviewx@smenode2 ~]$
```

> **Note:** If services are running, note the port number that is shown after 5301:<est_external_port>. This port must be configured in EST Settings UI.

- Make sure that the namespace for below services are configured with respective data center (DC) names:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- avx_platform_gateway_external=<dc name>
- avx_vendor_cert_est_agent=<dc name>

Enable EST Services

If EST services are not running, follow the steps to run the EST services:

1. Open the terminal window.
2. Add the avx_vendor_cert_est_agent and avx_platform_gateway_external in ENABLED_PLUGINS in appviewx.conf that is available inside the scripts folder </home/appviewx/appviewx_kubernetes/scripts>.
3. Specify the data center (DC) where the gateway must be deployed.

```
ENABLED_PLUGINS=appviewx_dependencies,avx_commons,avx_crontab,avx_config_server,avx_platform_core,avx_platform_amc,avx_platform_queue,avx_platfo
rm_gateway,avx_platform_gateway_external,avx_platform_web,avx_subsystems,avx_vendors,avx_subsystems_sync,avx_visual_page_builder,avx_vendor_cert
_network_discovery,avx_vendor_cert_scep_agent,avx_vendor_cert_intune_agent,avx_vendor_cert_est_agent,avx_vendor_cert_acme_agent
SSH_OTHER_USER=appviewx

avx_commons=absecon
avx_config_server=absecon
avx_platform_core=absecon
avx_platform_queue=absecon
avx_subsystems=absecon
avx_subsystems_sync=absecon
avx_vendors=absecon
avx_platform_gateway=absecon
avx_platform_web=absecon
avx_platform_amc=absecon
avx_platform_gateway_external=absecon
avx_visual_page_builder=absecon
avx_vendor_cert_network_discovery=absecon
avx_vendor_cert_scep_agent=absecon
avx_vendor_cert_intune_agent=absecon
avx_vendor_cert_est_agent=absecon
avx_vendor_cert_acme_agent=absecon
```

4. Execute the command: <plugins_install.sh>
5. Verify the EST is enabled by executing the command: <kubectl get services –A | grep est>

```
[appviewx@smenode2 ~]$ kubectl get services -A | grep est
external-system        avx-platform-gateway-est                NodePort    10.101.89.37     <none>        5301:30739/TCP
smedc1                 avx-vendor-cert-est-agent               ClusterIP   10.105.120.24    <none>        5306/TCP
[appviewx@smenode2 ~]$
```

6. Verify the plugin status and port number, do the steps as follows:

   a. Execute the <kubectl get services -A | grep est> command and make sure that the “avx-vendor-cert-est-agent” and “avx-vendor-cert-est-agent” is running.

   b. Make sure that the port number is 5301:30021 in avx-platform-gateway-est.

> **Note:** The number 5301:30021 must be used in the UI configuration.

```
-bash-4.2$ kubectl get services -A | grep est
absecon                avx-vendor-cert-est-agent               ClusterIP   10.101.59.249    <none>        5306/TCP
external-system        avx-platform-gateway-est                NodePort    10.100.79.210    <none>        5301:30021/TCP
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

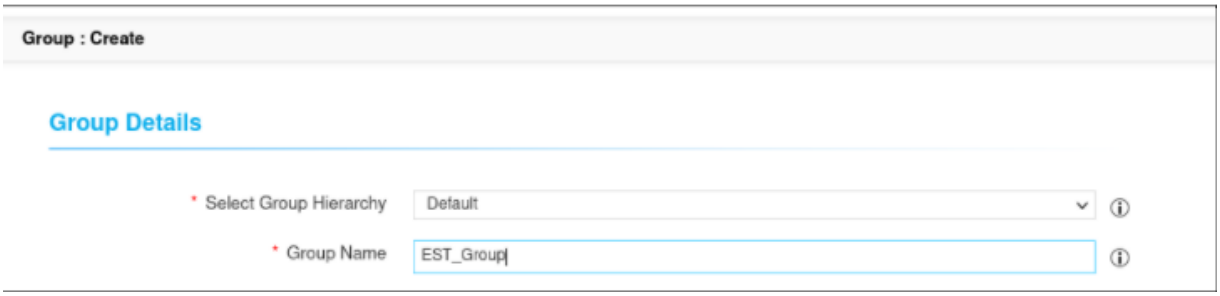
c. Execute the <kubectl get pods -n external-system -o wide> command to identify the nodes running in the EST service. EST will be available on all the nodes where external system runs.

```
-bash-4.2$ kubectl get pods -n external-system -o wide
NAME                                  READY   STATUS          RESTARTS   AGE   IP              NODE
avx-platform-gateway-676f67587b-54jj8   1/1     Running         5          64d   10.244.198.136   trialnode2.appviewx.net
avx-platform-gateway-676f67587b-h6xrf   1/1     Running         4          62d   10.244.251.30    trialnode3.appviewx.net
avx-platform-gateway-676f67587b-tbqcs   0/1     NodeAffinity    0          64d   <none>           trialnode3.appviewx.net
-bash-4.2$
```

d. Ping to the node names to get IP addresses.

```
-bash-4.2$ ping trialnode2.appviewx.net
PING trialnode2.appviewx.net (192.168.61.82) 56(84) bytes of data.
64 bytes from trialnode2.appviewx.net (192.168.61.82): icmp_seq=1 ttl=64 time=0.225 ms
64 bytes from trialnode2.appviewx.net (192.168.61.82): icmp_seq=2 ttl=64 time=0.098 ms
^C
--- trialnode2.appviewx.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.098/0.161/0.225/0.064 ms
-bash-4.2$ ping trialnode3.appviewx.net
PING trialnode3.appviewx.net (192.168.61.83) 56(84) bytes of data.
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=1 ttl=64 time=0.149 ms
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=3 ttl=64 time=0.114 ms
^C
```

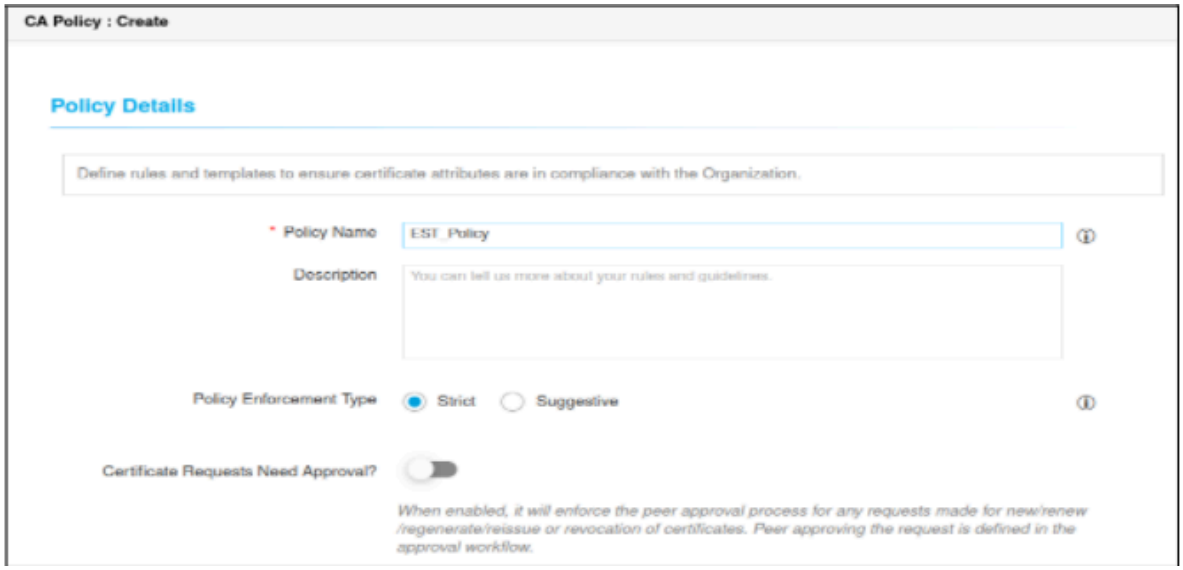
7. [Optional] Create a separate group for EST if required or use Else use the Default Group, where the “Certificate Request Needs Approval” should be disabled for the associated CA Policy.



8. Create a CA policy and associate with group. For more details, refer to CERT+ Admin Guide.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

a. Disable “Certificate Requests Need Approval?” in the Policy Details page.



b. To configure a policy with AppViewX details, click **AppViewX** in the **Certificate Authority** pane on the left side of the screen.

c. In the CA detail section, select **CA Accounts** from the dropdown list.

d. Add validity, and then click **Add**.

e. Select Bit length as 2048 and above (AppViewX Client supports 2048 RSA)

f. Select ECDSA curves based on requirement.

g. Select the hash function as SHA-256 and above.

h. Click **Save CA Details**.

i. Select the Group that is created earlier and update policy.

9. Upload a client authentication issuer certificate in AppViewX application.

a. By default, AppViewX EST Client software’s (Windows/Linux/Mac) will have an Authentication Certificate Encoded within the Software (which will be encrypted and kept within Client Software), user will never have direct access to it and this will be used for agent to communicate with AppViewX EST Server.

b. For initial validation, you can use default encoded authentication certificates in client software and issuer certificate. The file will be available in a common share folder with the following file name.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

i. The file name **<AppViewXIntermediateCA_D2 E3 B6 15 EE E6 2D 4C 1D 99 AC 11 6D 47 B5 CD.crt>**

ii. Upload above file in the respective appviewx environment and trust it in EST Settings.

iii. To upload a certificate, log in to AppViewX application with valid credentials.

iv. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

v. Click **CERT+** > **Certificate Inventory**.

vi. Click **Upload** > **CA Certificate**.

vii. Select CA, and then upload the file.

- Note the Serial Number “B5:CD” of the CA Certificate (This needs to be added as “Issuer Certificate in EST Client Authentication Configuration” later).
- If you want to use non AppViewX Certificate as the Issuer CA for EST Authentication. Refer the “EST Server Update FP5 Authenticate with External CA” guide and section Adding External CA Trust Certificate for EST Client Authentication
- Description: TLS Authentication handshake is happening in the GW and by default GW is holding only AppViewX Intermediate and AppViewX Root in the EST_TRUSTED_CA_CERTS, AppViewX GW will be sending these Certificates as the DN(Distinguished Name) response to the Clients.
- During TLS Handshake Client Validates whether the DN response from Server contains the CA Certificate which Signed Client’s Authentication Certificate. If not, client will not send the authentication Certificate to the Server, assuming this is not the right Server.

Note: OCSP and CRL Validation of Client Authentication Certificate for EST request is disabled by default in AppViewX. To enable reach out to AppViewX Support (support@appviewx.com).

If it is getting enabled, make sure OCSP or CRL responder is reachable from AppViewX to validate the client certificate status else all the client enrollment requests will fail with status “OCSP or CRL responder is not reachable”.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Create Client Authentication Certificate Using AppViewX CA

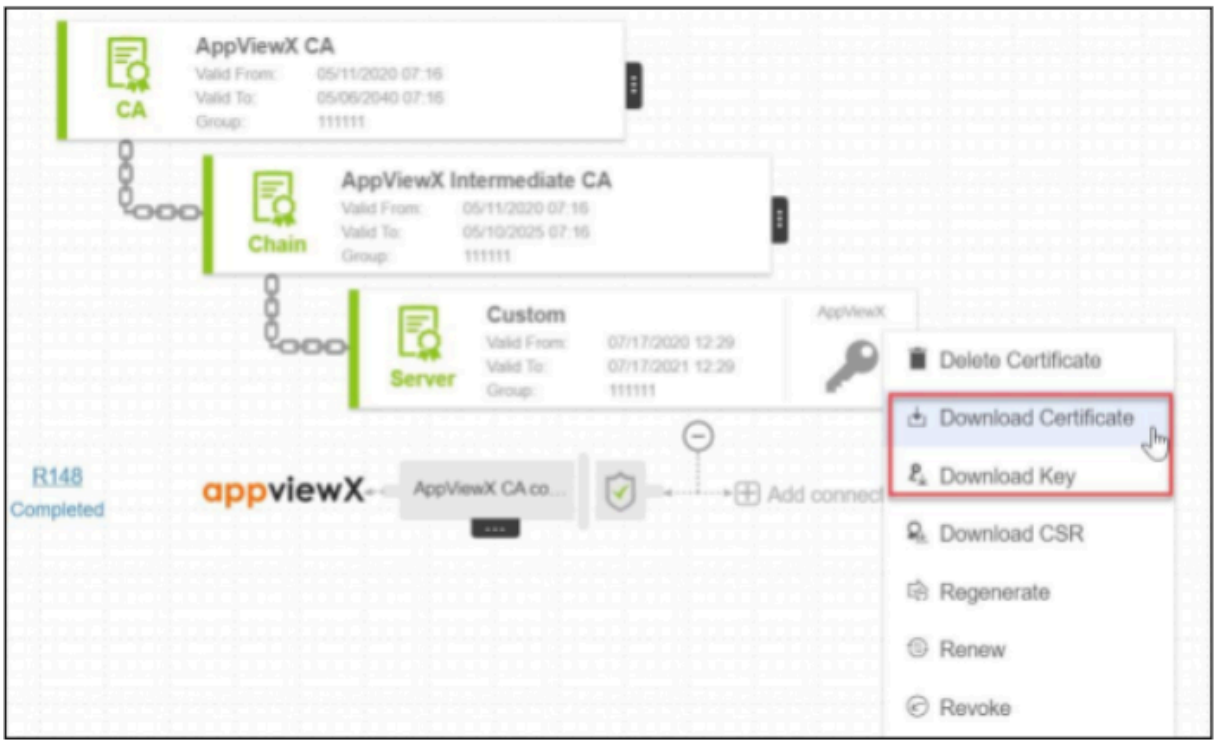
If the user does not have a client authentication AppViewX CA certificate, user can use AppViewX CA. To use a client authentication AppViewX CA certificate:

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
   The left navigation pane appears.
3. Click **CERT+.**
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE Inventory.**
5. Select **Enroll Certificate,** and then **Server.**
   The **Enroll Server Certificate** page appears.
6. In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list.

   Note: By default, the **Default** option is selected.

7. In the **CA Details** section, select/enter the details as required.
8. Select a **CSR Generation** mode: AppViewX, Upload CSR, HSM, or Endpoint.
9. Under the **CSR Parameters** section, enter a Common Name for the certificate.
10. While creating certificates, you can attach supporting documents by uploading it in the **Attachment** section.
11. Click **Add** to generate the certificate. The certificate holistic view with the newly created CSR appears.
12. Click **Submit**.
13. On the submit dialog box, enter relevant comments and click **Yes**.
14. Click **Refresh** on the top-right to refresh the holistic view. Now, a chain of certificates is displayed.
15. Hover over the vertical eclipse icon on the certificate and download the Certificate and Key.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Note: The user has to trust the AppViewX Intermediate CA certificate and select this certificate as **Issuer Certificate** during the EST configuration.

EST Configuration

To configure the EST server:

1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button.
   The left navigation pane appears.
3. Click **CERT+** .
   The **CERT+** left navigation pane appears.
4. Select **Administration** > **Auto-Enrollment** > **EST**.
   On the EST list view page, **defaultEST** is displayed by default.
5. Click **+ Add** icon on the top-right.
6. On the EST details page, under the **Agent Details** section, enter the Name, IP Address (node's IP address where EST plugin is running), and the Gateway Port.
7. Under the **Client Authentication** section, select an **Authentication Mode** from the drop- down list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Only Certificate TLS (If you are using AppViewX EST client) - During client authentication, only certificate TLS based authentication will be performed.
- Certificate TLS with HTTP as Fallback - During client authentication, when the certificate TLS fails, HTTP based authentication will be performed as a Fallback.
- Both Certificate TLS and HTTP - During client authentication, both certificate TLS and HTTP based authentication will be performed respectively after the successful completion of the other.

8. If the user selects **Certificate TLS with HTTP as Fallback** or **Both Certificate TLS** and **HTTP** mode, the user will be prompted to enter the username and password along with the option to select the **HTTP Authentication Mode**.
9. Select an HTTP Authentication Mode: **Basic** or **Digest**

- **Basic** - During client authentication, only the username and password values will be considered for the HTTP based authentication.
- **Digest** - During client authentication, along with the username and password, nonce and realm values will be supported.

> **Note:** This is the same certificate that was uploaded in the **Upload the Client Authentication CA Certificate** section.

10. Select the **Issuer Certificate** by entering the first three letters of the certificate name or serial number.
11. Under the **CA Settings** section, select the **Certificate Group** from the drop-down list.
12. Select the Certificate Type as **Client** or **Server** based on the requirement.
13. Select the **CA** and **CA Account** from the respective drop-down lists. At present, AppViewX supports only AppViewX CA, EJBCA, and Microsoft CA.
14. In the **CA Certificate** field, enter the certificate name and in the **CA Connector Name** field, enter a name for the CA Connector.
15. In the **Certificate Validity** field, enter the number of days.
16. Under the **Advanced Settings** section, select the **Yes** or **No** radio button to include or exclude truststore certificates. You can choose an option whether to share the trust store certificate with the client during the get CA operation.
17. Enter the **Retry Count** and **Retry Frequency** in the respective fields.
18. Click **Save.**

- Supported Operations
- Best Practices
- [Optional - OnPremise] Adding External CA Trust Certificate for EST Client Authentication

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- [Optional - OnPremise] Change SSL Certificate for EST-HTTPS Communication
- [Optional - SaaS] EST Client Authentication in Cloud Connector

Supported Operations

The AppViewX EST agent supports three operations as shown in the below table.

Supported Operation	Operation Path
Distribution of CA certificates	/cacerts
Enrollment of clients	/simpleenroll
Re-enrollment of clients	/simplereenroll

Best Practices

The following are the best practices:

- For auto-enrolment, create a separate certificate group and CA policy in AppViewX.
- Enable auto-renewal in the AppViewX policy.
- During policy creation, select only required bit-length (minimum 2048 bit).
- For machine enrollment, define an expected domain name in the CA policy for machine CSR (for example, *.appviewx.com) to avoid issuing certificates for different domain machines.
- Recommended to use TLS authentication with AppViewX EST clients.
- Recommended to use only private/internal CA as trusted for client authentication (Not recommended to use public CA as trusted to validate clients).
- Select appropriate certificate type: **Server** or **Client** (Select Server only if it is a server certificate and Client for machine and user certificates).
- The recommended validity for the issued certificate is one year.
- Use the trusted CA-signed certificate in a gateway for EST URL.
- Example URLs

Example URLs

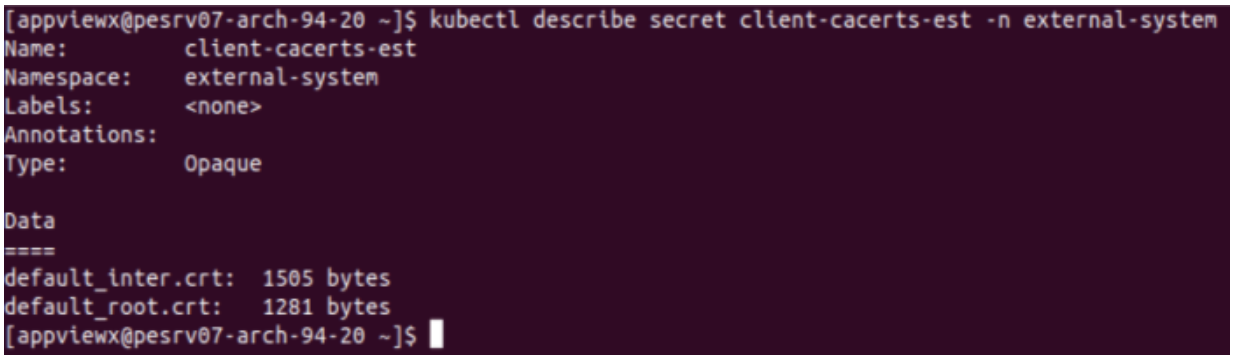
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- For default: `<https://est.appviewx.com:<port_number>/.well-known/est>`
- For AppViewX Enrollment: `<https://est.appviewx.com:<port_number/.well-known/est/appviewx/simpleenroll>`
- For AppViewX Re-enrollment:

```
<https://est.appviewx.com:<port_number/.well-
known/est/appviewx/simplereenroll>
```

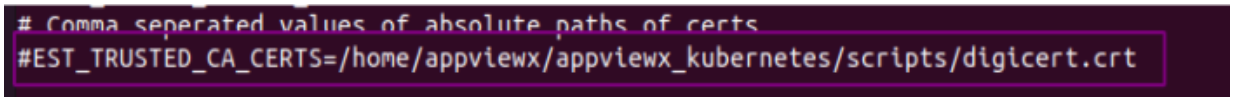
[Optional - OnPremise] Adding External CA Trust Certificate for EST Client Authentication

- By Default AppViewX Intermediate and AppViewX Root will be available in the location with filenames "`default_inter.crt`", "`default_root.crt`"
- Execute the command



- Add below plugins in the ENABLED_PLUGINS list

`ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway`



- And `run ./plugins_install.sh`

[Optional - OnPremise] Change SSL Certificate for EST-HTTPS Communication

- By default there will be self Signed Certificate available in the location.
- Add below plugins in the ENABLED_PLUGINS list

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway

```
# Please specify the absolute paths of files for the labels below
# EST_SERVER_ACCESS_CERT=
# EST_SERVER_ACCESS_KEY=
# Comma seperated values of absolute paths of certs
#EST_TRUSTED_CA_CERTS=/home/appviewx/appviewx_kubernetes/scripts/digicert.crt
```

- And run ./plugins_install.sh

```
[appviewx@pesrv07-arch-94-20 ~]$ kubectl describe secret server-tls-est -n external-system
Name:         server-tls-est
Namespace:    external-system
Labels:       <none>
Annotations:
Type:         kubernetes.io/tls

Data
====
tls.crt:  1046 bytes
tls.key:  1704 bytes
```

[Optional - SaaS] EST Client Authentication in Cloud Connector

For steps to replace the Default TLS Certificate with Signed Certificate and add ca issuer certificates for EST client authentication in CC, click here

Gateway - EST Logs

To access the EST logs:

1. Access the terminal window.
2. Go to **<Installed_Path>/logs** directory and find with the name format **<avxgw-MTLS-<yyyy-mm-dd>.log>**. For example, **<avxgw-MTLS-2021-03-17.log>**.
   - If the file size exceeds 100 MB, it will be rolled over and the latest logs will be available in the latest file that is named with an incrementing counter starting from 1 such as **avxgw-MTLS-<yyyy-mm-dd>.<incrementing_counter>.log.** For example, **<avxgw-MTLS- 2021-03-17.1.log>**.
   - EST Plugin Logs:

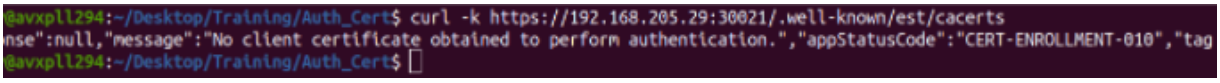
     </home/appviewx/appviewx/logs/avx-vendor-cert-est-agent-<pod_name>.log>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

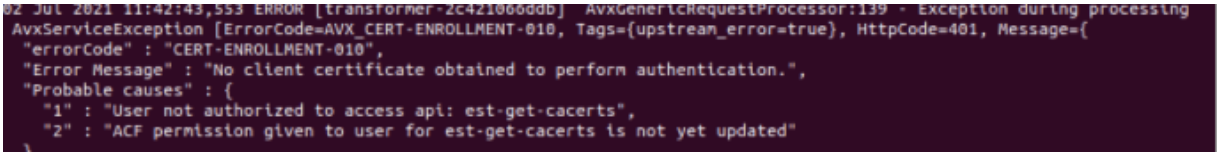
Verification of the EST Server

To verify the EST server:

1. Access the terminal window.
2. Go to **<appviewx/logs>** directory and execute the <kubectl get pods -A | grep est> command.
3. Go to **-f <pod_name>.log** directory.
4. Access CACerts URL from browser or Try curl from another machine.



5. Check the log file.

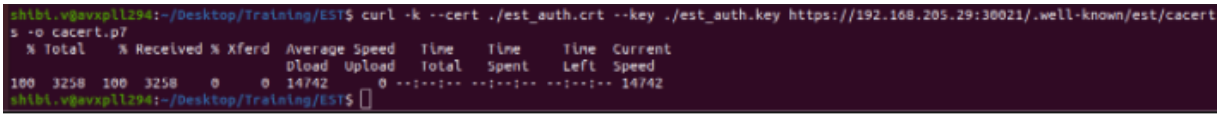


6. The response indicates that the EST is listening on Port and trying to do Certificate Authentication with Client.

Testing EST Enrollment by using CURL

To test the EST enrollment:

1. After the successful verification, create a test folder in the Linux client machine.
2. Copy the <**est_auth.crt**> and <**est_auth.key**> from the common share directory https://drive.google.com/drive/folders/1K4G5L8yB5TOvvLCAPjNC3lQWBWtlWua0
3. Generate the CSR in the same folder with <openssl> command.
   openssl req -new -newkey rsa:2048 -nodes -keyout rsakey.key -out req.p10
4. Trigger GetCA certs request using CURL command (update server IP and Pathseg depends on Server Config).
5. Make sure that the authentication CERT and Key is present in same location <*curl -k --cert ./est_auth.crt --key ./est_auth.key https://<server_ip>:30021/.well-known/est/cacerts -o cacert.p7*>. You will receive <cacert.p7> file with Configured CA Certificate in Step 9.

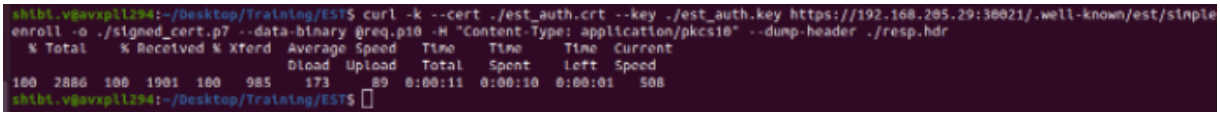


6. Convert the received CA Certificate to pem <*openssl base64 -d -in cacert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out cacert.pem*>.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Trigger enrollment request by using CURL and make sure that the authentication Cert, Key, and CSR are present in same location.

   <curl -k --cert ./est_auth.crt --key ./est_auth.key https://192.168.205.29:30021/.well-known/est/simpleenroll -o ./signed_cert.p7 --data-binary @req.p10 -H "Content-Type: application/pkcs10" --dump-header ./resp.hdr>



8. Verify the content of <signed_cert.p7>.



9. Convert the enrolled p7 Certificate in to pem

   <openssl base64 -d -in signed_cert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out signed_cert.pem>.

10. Make sure that you have received <cacert.p7> file with Configured CA Certificate.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

SCEP Configuration Guide

This guide contains the pre-defined procedure for the Simple Certificate Enrolment Protocol (SCEP) configuration

- Getting Started
- SCEP Service Flow
- EST Enrollment
- AppViewX Server URL Details

Getting Started

- Overview
- Prerequisites
- Enable SCEP Services
- Generate SCEP Registration Authority (RA)
- Configure SCEP via AppViewX GUI

Overview

The SCEP protocol services can be configured in AppViewX to enable the communications between the client (device endpoints) and AppViewX northbound services that processes the client requests such as certificate enrolment and renewal. Once the protocol service gets enabled, AppViewX will act as a RA in receiving and serving the client requests. The protocol must be enabled as HTTP service.

Prerequisites

Before configuring the SCEP server, the user has to make the following changes in the AppViewX server:

- Make sure that the and services are running in the cluster.

```
[appviewx@smenode1 ~]$ kubectl get services -A | grep scep
absecon                avx-vendor-cert-scep-agent                ClusterIP   10.105.243.26   <none>        5312/TCP
                                                 12d
external-system        avx-platform-gateway-scep                 NodePort    10.99.34.105    <none>        5302:30555/TCP
                                                 6d15h
[appviewx@smenode1 ~]$
```

Note: If services are running, note the port number that is shown after 5302:< scep_external_port>. This port number needs to be configured in SCEP Settings GUI.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Make sure that the namespace for below services are configured with respective data center (DC) names:
  - avx_platform_gateway_external= <dc name>
  - avx_vendor_cert_scep_agent= <dc name>

Enable SCEP Services

If SCEP services are not running, follow the steps to run the SCEP services:

1. Open the terminal window.
2. Add the avx_vendor_cert_scep_agent and avx_platform_gateway_external in ENABLED_PLUGINS in appviewx.conf that is available inside the scripts folder </home/appviewx/appviewx_kubernetes/scripts>
3. Specify the data center (DC) where the gateway must be deployed.

```
ENABLED_PLUGINS=appviewx_dependencies,avx_commons,avx_crontab,avx_config_server,avx_platform_core,avx_platform_amc,avx_platform_q
ueue,avx_platform_gateway,avx_platform_gateway_external,avx_platform_web,avx_subsystems,avx_vendors,avx_subsystems_sync,avx_visua
l_page_builder,avx_vendor_cert_network_discovery,avx_vendor_cert_scep_agent,avx_vendor_cert_intune_agent,avx_vendor_cert_est_agen
t,avx_vendor_cert_acme_agent
SSH_OTHER_USER=appviewx

avx_commons=absecon
avx_config_server=absecon
avx_platform_core=absecon
avx_platform_queue=absecon
avx_subsystems=absecon
avx_subsystems_sync=absecon
avx_vendors=absecon
avx_platform_gateway=absecon
avx_platform_web=absecon
avx_platform_amc=absecon
avx_platform_gateway_external=absecon
avx_visual_page_builder=absecon
avx_vendor_cert_network_discovery=absecon
avx_vendor_cert_scep_agent=absecon
avx_vendor_cert_intune_agent=absecon
avx_vendor_cert_est_agent=absecon
avx_vendor_cert_acme_agent=absecon
```

4. Execute the command <plugins_install.sh>
5. Verify the SCEP is enabled using command.

```
[appviewx@smenode1 ~]$ kubectl get services -A | grep scep
absecon               avx-vendor-cert-scep-agent               ClusterIP   10.105.243.26    <none>        5312/TCP
                                12d
external-system       avx-platform-gateway-scep                NodePort    10.99.34.105     <none>        5302:30555/TCP
                                6d15h
[appviewx@smenode1 ~]$
```

Generate SCEP Registration Authority (RA)

To generate SCEP registration authority,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The left navigation pane appears.

3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE Inventory**.
5. Select **Enroll Certificate**, and then Server.
   The **Enroll Server Certificate** page appears.
6. In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list.

   Note: By default, the **Default** option is selected.

7. In the **CA Details** section, select/enter the details asrequired.
8. Select a **CSR Generation** mode: AppViewX, Upload CSR, HSM, or Endpoint.
9. Under the **CSR Parameters** section, enter a Common Name for the certificate
10. While creating a certificate, you can attach supporting documents by uploading it in the **Attachment** section.
11. Click **Add** to generate the certificate. The certificate holistic view with the newly created CSR appears.
12. Click **Submit**.

Configure SCEP via AppViewX GUI

To configure the SCEP via GUI,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Navigate to **Inventory** > **Certificate** > **Auto enrolment** > **SCEP**.
5. Click the **Add** button.
6. On the SCEP details page, under the **Agent Details** section, enter the Name, IP Address (node's IP address where SCEP plugin is running), and the Gateway Port.

   Note: Use the port number that is appearing when you enable SCEP services

7. Set the SCEP password in the Challenge Password field.
8. Under the **CA Accounts** section, select the **Certificate Group** from the drop-down list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

9. Select the Certificate Type as **Client** or **Server** based on the requirement.
10. Select the **CA** and **CA Account** from the respective drop-down lists. At present, AppViewX supports only AppViewX CA, EJBCA, and Microsoft CA.
11. In the **Server Certificate** field, upload the RA certificate that is created in the AppViewX using respective CA.
12. In the **CA Connector Name** field, enter the desired connector name.
13. In the **Certificate Validity** field, enter the number of days.
14. Under the **Advanced Settings** section, select the **Yes** or **No** radio button to include or exclude truststore certificates. You can choose an option whether to share the trust store certificate with the client during the get CA operation.
15. Enter the **Retry Count** and **Retry Frequency** in the respective fields.
16. Select the required **Certificate Poll Type** (select the **Issuer and Subject** or **Transaction ID**).
17. Click **Save**.
18. Once saved, AppViewX will generate and populate the SCEP URL in the GUI, which can be used for establishing the SCEP service. Multiple SCEP services can be configured in AppViewX GUI with the same VMware and unique SCEP agent names.

SCEP Service Flow

Once the AppViewX SCEP service gets configured and enabled, the client can start requesting for the certificate enrolments using this service. The entire certificate enrolment process has been mentioned below:

- Certificate Enrollment

Certificate Enrollment

For enrolling a certificate using the AppViewX SCEP services, the following processes will be executed which are based on the client vendors:

- Get CA Certificate
- Request a Challenge Passphrase
- Enrollment Process
- Enrollment Using SCEP Client
- Enrollment using Cisco Router

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Get CA Certificate

During certificate enrolment request from the client, get CA certificate process will be executed first through the AppViewX enabled SCEP service. Some client vendors do not support get CA certificate process and this process will be skipped.

During this process execution, the client will request the user defined CA certificate from AppViewX. As the response to the client, AppViewX will share the user selected CA certificates, during the SCEP GUI configuration

Note: If the user has selected any intermediate certificate, in the response, AppViewX will share the complete chain of trust store certificates will be shared with the client. This CA certificate will be used for encrypting the data for further communication.

Request a Challenge Passphrase

This is an optional value only few client will use. During the certificate enrolment request, some clients will also send the challenge password along with the CSR (Certificate Signing Request). The SCEP service will validate this value against the challenge password value provided during respective SCEP service configuration in AppViewX GUI. If both the password value match, the enrolment process will be proceeded further.

Enrollment Process

During this process, the client will share the CSR (Certificate Signing Request) to AppViewX through SCEP service. AppViewX will forward the CSR to the user selected CA during its respective SCEP service configuration in AppViewX GUI. Once the CSR has been signed by the CA successfully, AppViewX will receive the signed certificate, create the chain of trust of certificates in the holistic view and push the certificate to the client as the response through the SCEP service. During push operation, the application connector for SCEP will be created and displayed in the holistic view.

Enrollment Using SCEP Client

Step 1

Get Enrollment URL from AppViewX Cert+ Auto enroll SCEP Page:

Step2

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Generate Private kay and CSR with passphrase

Openssl Eg: openssl genrsa -out enrollment.key 2048 && openssl req -new -key enrollment.key -out enrollment.csr

Step3

Initiate GetCA Request

sscep getca -c -u

Eg:sscep getca -c ca-cert -u http://192.168.66.50:5250/services/scep/cert-scep/app

Step4

Request for Certificate:

sscep enroll -u <scep_url> -k ./<key_file> -r ./<csr_file> -c <ca_cert_file> -l

./<output_certificate>

Example:sscep enroll -u http://192.168.66.50:5250/services/scep/cert-scep/app -k ./enrollment.key -r ./enrollment.csr -c ca-cert-1 -l ./cert1.crt

Enrollment using Cisco Router

To enroll using Cisco router,

1. Configure using the Cisco Router Trustpoint.

   Cisco Router Trustpoint Configuration:

   crypto pki trustpoint scep-test

   enrollment url http://192.168.66.50:5250/services/scep/cert-scep

   fqdn SCEP_DEMO_Cisco_Router.avxdevcert.com

   subject-name CN=SCEP_DEMO_Cisco_Router

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
CSR_67_50#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CSR_67_50(config)#
CSR_67_50(config)#crypto pki trustpoint scep-test
CSR_67_50(ca-trustpoint)#$//192.168.66.50:5250/services/scep/cert-scep
CSR_67_50(ca-trustpoint)# fqdn SCEP_DEMO_Cisco_Router.avxdevcert.com
CSR_67_50(ca-trustpoint)# subject-name CN=SCEP_DEMO_Cisco_Router
CSR_67_50(ca-trustpoint)#
```

2. Initiate GetCA Request from Router.

```
CSR_67_50(config)#crypto pki authenticate scep-test
Trustpoint 'scep-test' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
       Fingerprint MD5: 0FB963B4 A5540CA6 7A462211 F6194AE8
      Fingerprint SHA1: 8ECAB98C 317286E1 BFF83C3B A2010DCC C0967E6C

% Do you accept this certificate? [yes/no]:
```

3. Initiate Enrollment Request.

```
CSR_67_50(config)#crypto pki enroll scep-test
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=scep_router_test
% The subject name in the certificate will include: SCEP_DEMO_Cisco_Router.avxdevcert.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose scep-test' commandwill show the fingerprint.

CSR_67_50(config)#
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Verification after Enrollment

```
CSR_67_50(config)#do sh crypto pki certificates scep-test
Certificate
  Status: Available
  Certificate Serial Number (hex): 3272BE7B534C7EED
  Certificate Usage: General Purpose
  Issuer:
    cn=avx_intermediate_ca
  Subject:
    Name: SCEP_DEMO_Cisco_Router.avxdevcert.com
    hostname=SCEP_DEMO_Cisco_Router.avxdevcert.com
    cn=SCEP_DEMO_Cisco_Router
  CRL Distribution Points:
    http://192.168.66.50/controller/avxcrl?crlFileName=212469579805591063.crl
  Validity Date:
    start date: 13:28:51 IST Jul 9 2019
    end   date: 13:28:51 IST Jul 8 2020
  Associated Trustpoints: scep-test

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 02F2D7F505E38617
  Certificate Usage: Signature
  Issuer:
    c=US
    st=Washington
    l=Seattle
    o=AppViewX Inc
    cn=AppViewX Intermediate CA
  Subject:
    cn=avx_intermediate_ca
  CRL Distribution Points:
    http://192.168.66.50/controller/avxcrl?crlFileName=975242343495596841.crl
  Validity Date:
    start date: 12:59:15 IST Jul 9 2019
    end   date: 14:12:06 IST Jul 6 2024
  Associated Trustpoints: scep-test est_test
  Storage: nvram:US#8617CA.cer


CSR_67_50(config)#
```

EST Enrollment

EST Enrollment Using Curl

1. Add Authentication Certificate and Key in the location
2. Generate CSR in the location using Openssl

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Eg: openssl genrsa -out enrollment.key 2048 && openssl req -new -key enrollment.key

3. Initiate GeCACert Request using Curl
   - curl --cert <auth_cert>--key <auth_key>https://<ip>:<port>/.well-known/est/cacerts - o <output_ca_p7>

     Convert Recived p7 Certificate in to pem using openssl
   - openssl base64 -d -in <output_ca_p7>| openssl pkcs7 -inform DER -outform PEM - print_certs -out <output_ca_cert_pem>

   Example
   - curl --cert est_auth.crt --key est_auth.key --cacert 192-168-96-22.pem https://192.168.66.50:5301/.well-known/est/cacerts -o cacerts.p7 Convert Recived p7 Certificate in to pem using openssl
   - openssl base64 -d -in cacerts.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out cacerts.pem
4. Initiate Enrollment Request
   - curl -k --cert <aith_cert>--key <auth_key> <simpleenroll_url> --data-binary @ <csr_file>-H "Content-Type: application/pkcs10" -o <signed_cert.p7>

     Convert Signed p7 Certificate in to pem using openssl
   - openssl base64 -d -in <sign_cert.p7>| openssl pkcs7 -inform DER -outform PEM - print_certs -out <sign_cert.pem>

   Example
   - curl -k --cert est_auth.crt --key est_auth.key https://<ip>:<port>/.wellknown/est/simpleenroll --data-binary @ <csrfile.csr>-H "Content-Type: application/pkcs10" -o output.p7

     Convert Recived p7 Certificate in to pem using openssl
   - openssl base64 -d -in output.p7 -out output.decode | openssl pkcs7 -inform DER - outform PEM -in output.decode -print_certs -out est_signed.pem

AppViewX Server URL Details

For default EST instance in AppViewX, it will be listening on below URLs for the Operation paths: https://<IP>:<port>/.well-known/est/<operational_path>

Example: https://est.appviewx.com:<port>/.well-known/est/cacerts for getting ca certificate https://est.appviewx.com:<port>/.well-known/est/simpleenroll for Enrollment

For other EST instance in AppViewX, it will be listening on below URLs for the Operation paths with path segments: https://<IP>:<port>/.well-known/est/<agent_name>/<operational_path>

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Example:

https://est.appviewx.com:<port>/.well-known/est/agent1/cacerts for getting ca certificate https://est.appviewx.com:<port>/.well-known/est/agent1/simpleenroll for Enrollment

1. Save Gateway Certificate in the location where libest is running
2. Save Authentication Certificate and Key in the location (in this example name is est_auth.crt, est_auth.key)
3. Set the environment variable using below command:

   export EST_OPENSSL_CACERT=appviewx_gw.crt (**appviewx_gw.crt** is the public certificate of the AppViewX Gateway where EST is listening)

4. **Getca** certificate from EST server (defaultEST instance) with TLS authentication. (Authentication certificates are already placed in the client folder)

   ./estclient -g -s est.appviewx.com -p 5301 -o certs -c est_auth.crt -k est_auth.key

5. Enroll request

   ./estclient -e -s est.appviewx.com -p <port>-o certs -c est_auth.crt -k est_auth.key --pemoutput --common-name myclient3 -w 15

6. Enroll request for other EST instances

   ./estclient -e -s est.appviewx.com -p <port>-o certs -c est_auth.crt -k est_auth.key --pemoutput --common-name myclient3 --path-seg <agent_name> -w 15

ACME Configuration Guide

This guide gives an overview on how Certbot and Winacme clients works with AppViewX via ACME protocol to request for certificates from supported CAs.

- EST Client Authentication in Cloud Connector
- Certbot Configuration Guide
- Winacme Configuration Guide
- Posh-ACME Configuration Guide

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

EST Client Authentication in Cloud Connector

For steps to replace the Default TLS Certificate with Signed Certificate and add ca issuer certificates for EST client authentication in CC, click here

Certbot Configuration Guide

This guide gives an overview of how Certbot clients work with AppViewX via ACME protocol to request certificates from supported CAs.

- Introduction to ACME Protocol
- AppViewX Certbot
- Download Certbot Client
- Prerequisites for Running Clients
- Steps to Install Certbot Client
- Accessing Certbot
- Troubleshooting
- Glossary

Introduction to ACME Protocol

ACME, or Automated Certificate Management Environment, is a communications protocol that leverages an agent to automate the process of CSR generation and certificate/key rotation. It is primarily used by the popular public CA, Let's Encrypt, as a part of their business model of issuing 90-day Domain Validated certificates (as Organizational Validation and Extended Validation certificates require human supervision to issue, thus rendering the point of ACME moot), and automating their renewals.

The protocol was initially developed by the Internet Security Research Group (ISRG) for the Let's Encrypt CA, and, as an open-source tool, free to use. While originally only used by Let's Encrypt to issue x.509 (SSL/TLS) certificates, various other CAs, PKI vendors, and browsers are now beginning to support ACME to work with other kinds of certificates (S/MIME, Code-signing) as well. However, to leverage them, the CA should be able to access the DNS/HTTPS token that is published. This makes it better suited to be an internal PKI issuance method.

AppViewX Certbot

AppViewX customizes Certbot to provide extended functionality to customers over the existing Certbot client which helps to meet various business and operational needs. The enhanced features are:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Single Click Installation and Interactive digital certificate CLM operations. The **Supported Linux OS** flavors are
  - Ubuntu 20.4
  - CentOS 7
  - Redhat 8.6
  - Debian 10
  - Devuan 3
  - OpenSUSE Tumbleweed
- Support for working with Let’s Encrypt CA through AppViewX (where AppViewX acts like an ACME Proxy to Let’s Encrypt CA).
- Custom Attributes support in certbot command for enrollment and renewal.
- Addition of CA Certificate in native trust store for the ACME client to work with any CA issued SSL Server certificate.

Benefits of AppViewX Certbot

AppViewX Certbot checks the system environment for various paths such as

- **Python 3.8** (Ubuntu 20.4, CentOS 7, Redhat 8.6)
- **Python 3** (Debian 10, Devuan 3, OpenSUSE Tumbleweed)
- **OpenSSL**
- **Virtual environment (venv) and required dependencies** for certbot.
- **jq package** which is a prerequisite (must) to access Interactive digital certificate CLM operations.
- **REQUESTS_CA_BUNDLE environment variable** (custom CA bundle path in root user's ".bashrc" file) which is required to enable SSL verification. The root certificates trusted by Certbot can be overridden by setting the REQUESTS_CA_BUNDLE environment variable.

If any of the above packages are not installed or configured in your system, AppViewX will do it for you without any human intervention.

Download Certbot Client

The Certbot client is now available in the release portal - Click here.

Prerequisites for Running Clients

- The AppViewX server needs to have a valid certificate installed on its gateway.
- System Requirements

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. **Environment Details:** Linux
2. **Operating System:** As mentioned earlier in the AppViewX Certbot section - the **Supported Linux OS** flavors.

- Root user permissions
- A proper DNS entry for the linux server
- Certificate attributes should be configured to capture custom attributes in the AppViewX GUI (if required).
- A valid ACME endpoint should be configured on the AppViewX GUI.
- To enable client connections, it's essential to have ports 31443 open for on-premises deployment and 30020 in cloud connectors open for SaaS deployment in AppViewX.
- If your DNS validation is for **HTTP challenge**, it's essential to have port 80 accessible on your Linux machine to allow AppViewX to establish a connection.
- If your DNS validation is for **DNS challenge**, the DNS server should be up and running and the DNS credentials file should be correctly configured.

Steps to Install Certbot Client

- Accessing the Files
- Prerequisites
- Installing Certbot through Automated Installation Files
- Installing Certbot through Commands

Accessing the Files

1. Download the certbot client from the release portal.
2. Open your terminal and navigate into the directory where you downloaded the Certbot ZIP file.
3. Unzip the downloaded Certbot client **AppViewX_ACME_Certbot_Client.zip** using the command.

```
unzip AppViewX_ACME_Certbot_Client.zip
```

4. Navigate to the extracted directory named **certbot**.

```
cd certbot
```

5. To proceed with further installation steps, users will need to have root privileges. Login as sudo user using the command

```
sudo -i
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Prerequisites

- Adding Custom CA Certificates to Trust Store
- Setting the Custom CA Certificate Path Manually

Adding Custom CA Certificates to Trust Store

> **Attention:** The steps described in this section must be executed only if you want to perform the **SSL verification**.

1. To obtain the certificate chain.

   a. If the server certificate is created in AppViewX, download it from the AppViewX inventory, else download the certificate chain files (.pem or .crt) for the Certificate Authority (CA). This chain should include the root certificate as well as any intermediate certificates of the server.

   b. If there are individual certificates for root CA and intermediate CA's, combine these certificate files into a single file. This can be done either through a text editor or by using the `cat` command:

   ```
   cat intermediateca.crt rootca.crt > acmetrustchain.crt
   ```

   Here, **acmetrustchain.crt** is the concatenated trust chain certificate.

2. To address situations where Certbot does not trust the SSL certificate employed by the ACME server, the REQUESTS_CA_BUNDLE environment variable is used to supersede the root certificates trusted by Certbot.
   Determine the appropriate trust store on your Linux system. Common locations for trust store are /etc/ssl/certs/ca-certificates.crt and /etc/ssl/certs/ca-bundle.crt. If you do not find any trust store in your OS, you can manually create a file **ca-certificates.crt** in the respective location.

   a. Login as sudo user

   ```
   sudo -i
   ```

   b. Navigate to the directory where the **acmetrustchain.crt** file is located.

   c. Copy the entire contents of the certificate chain files and append them to the end of the trust store file using the **cat** command.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
cat acmetrustchain.crt >> /etc/ssl/certs/ca-certificates.crt
```

Note: The same trust store location path provided above (likely */etc/ssl/certs/ca-certificates.crt*) should be specified while executing *install.sh* and setting REQUESTS_CA_BUNDLE environment variable.

Setting the Custom CA Certificate Path Manually

This section describes the steps to manually set the custom CA certificate path within the root user's **.bashrc** file.

Attention: These steps must be performed only after you execute the steps in the above section - Adding Custom CA Certificates to Trust Store and if you've chosen the option “n” during the execution of the *install.sh* command in response to the question "Do you want to set a custom CA bundle path? (y/n)".

1. Login as sudo user

   ```
   sudo -i
   ```

2. Open the ".bashrc" file

   ```
   vi ~/.bashrc
   ```

3. Enter the **custom CA certificate path** in the REQUESTS_CA_BUNDLE variable `export REQUESTS_CA_BUNDLE="<custom ca certificate path>"`
4. Save and exit from the file.
5. Source the ".bashrc" file to update the latest changes using the command

   ```
   source ~/.bashrc
   ```

Note: You may need to logout and re-login as a **sudo user** to apply changes effectively.

Adding Custom CA Certificates to Trust Store

Attention: The steps described in this section must be executed only if you want to perform the **SSL verification**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. Obtain the certificate chain.

   a. Ensure that you have downloaded and saved the certificate chain files (.pem or .crt) for the CA. The chain should include the root certificate, any intermediate certificate.

   b. Concatenate the certificate files into a single file using a text editor or the **cat** command.

   ```
   cat intermediateca.crt rootca.crt > acmetrustchain.crt
   ```

   Here, **acmetrustchain.crt** is the concatenated trust chain certificate.

2. Determine the appropriate trust store on your Linux system.
   Common locations for trust store are **/etc/ssl/certs/ca-certificates.crt and /etc/ssl/certs/ca-bundle.crt**. If you do not find any trust store in your OS, you can manually create a file **ca-certificates.crt** in the respective location.

   a. Open the trust store file in a text editor with **root/superuser** privileges.

   b. Copy the entire contents of the certificate chain files and append them to the end of the trust store file using the **cat** command.

   ```
   sudo cat acmetrustchain.crt >> /etc/ssl/certs/ca-certificates.crt
   ```

   Note: The same trust store location path **/etc/ssl/certs/ca-certificates.crt** should be given while executing *install.sh* and setting REQUESTS_CA_BUNDLE environment variable.

Setting the Custom CA Certificate Path Manually

This section describes the steps to manually set the custom CA certificate path within the root user's ".bashrc" file.

Attention: These steps must be performed only after you execute the steps in the above section - Adding Custom CA Certificates to Trust Store and if you've chosen the option “n” during the execution of the *install.sh* command in response to the question "Do you want to set a custom CA bundle path? (y/n)".

1. Login as sudo user

   ```
   sudo -i
   ```

2. Open the ".bashrc" file

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
vi ~/.bashrc
```

3. Enter the **custom CA certificate path** in the REQUESTS_CA_BUNDLE variable

   `export REQUESTS_CA_BUNDLE = “<custom ca certificate path>”`

4. Save and exit from the file.
5. Source the ".bashrc" file to update the latest changes using the command

```
source ~/.bashrc
```

> **Note:** You may need to logout and re-login as a **sudo user** to apply changes effectively.

Installing Certbot through Automated Installation Files

1. Login as root user using the command below

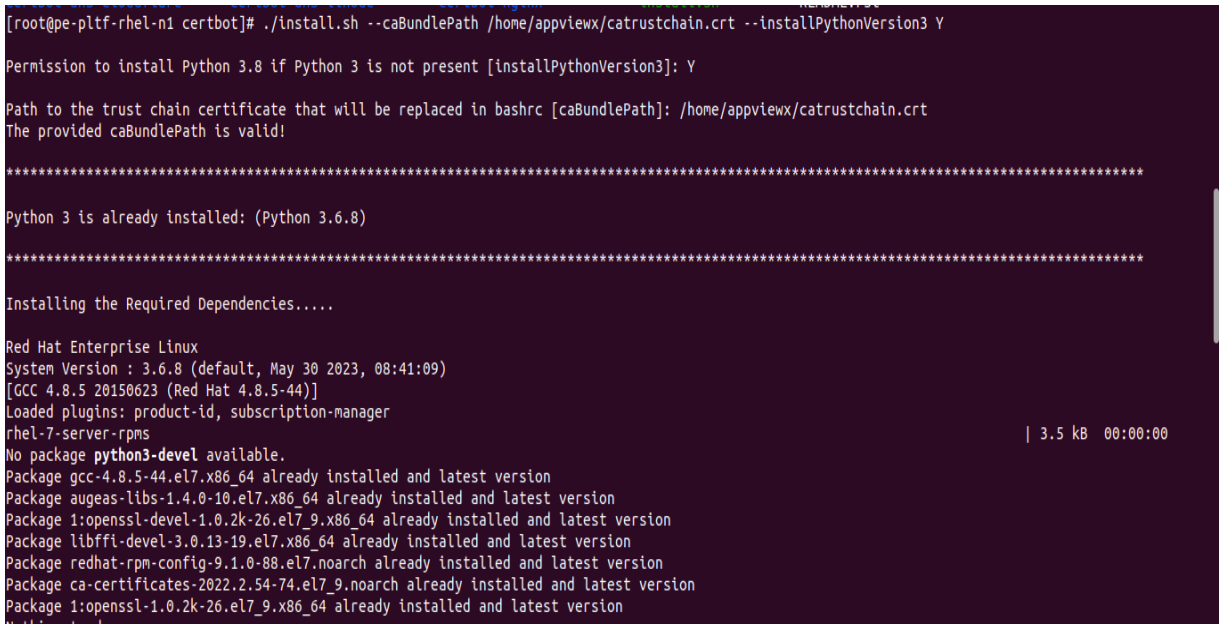
```
sudo -i
```

2. To install dependencies and set up the virtual environment, execute the command below.

```
./install.sh
```

   You may also pass additional parameters with the **install.sh** as in the command below.

```
./install.sh --caBundlePath /home/appviewx/caCertificate.crt --installPythonVersion3 Y
```



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameter Description

Parameters	Type/ Values	Mandatory	Description
--caBundlePath	Path of the caBundle certificate	No	To strictly enforce SSL verification during the enrollment or renewal of certificates through Certbot you should provide a custom CA BUNDLE path, indicating the path to your designated trust store file location with the parameter “caBundlePath”. The provided path will be used to set the REQUESTS_CA_BUNDLE environment variable in the user’s “.bashrc” file. Alternatively, if you opt to bypass SSL verification during certificate enrollment or renewal via Certbot. Do not provide the caBundlePath. In this scenario, the installation process will proceed without having to provide a CA BUNDLE path. However, you will still have the option to activate SSL verification by manually configuring a custom bundle path at a later time. Refer to the Prerequisite section to do the needful.
--installPythonVersion3	Y (or) N	No (default value : ‘N’)	The install.sh script examines the Python version present on the client system. If the detected version is below 3, the installation script will attempt to install Python 3.8 only if the installPythonVersion3 parameter is configured to "Y".

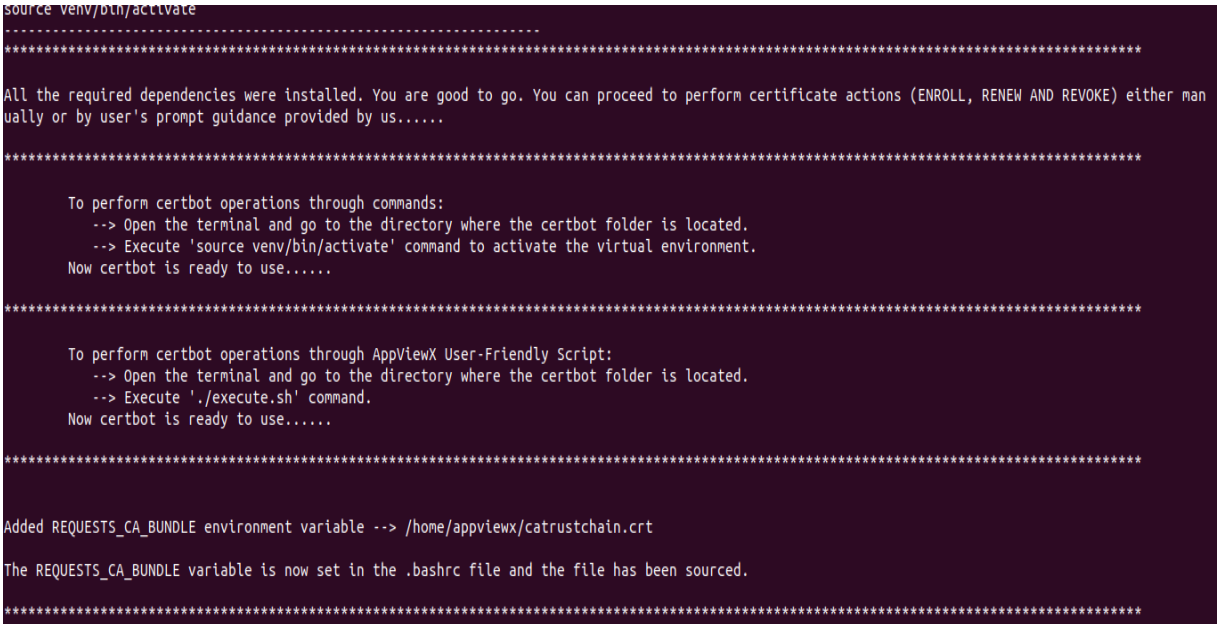
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters	Type/ Values	Mandatory	Description
			If the installPythonVersion3 parameter is set to "N", the installation process will be terminated if Python 3 or a higher version is not found on the client system.

During the installation process

- The install.sh script verifies the presence of the necessary Python version compatible with the operating system.
- In the event that the required version is absent and the installPythonVersion3 parameter is passed as “Y”, the script proceeds to install python 3.8.
- Furthermore, the script installs the mandatory certbot dependencies and establishes the essential virtual environment.

Once the installation is complete you will see the details as shown below.



Installing Certbot through Commands

1. Install all the required dependencies using the command below.

```
apt install python3-dev gcc libaugeas0 libssl-dev libffi-dev ca-certificates openssl
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Or

```
yum install python3-devel gcc augeas-libs openssl-devel libffi-devel redhat-rpm-config ca-certificates openssl
```

2. Open the certbot folder using the command

```
cd certbot_client/certbot
```

3. Setup the virtual environment using the command

```
python3 tools/venv.py
```

A virtual environment is activated within the Certbot folder. You can enroll a certificate, re-enroll or revoke using the commands mentioned in the Enroll Certificate section.

Accessing Certbot

• Overview
• Method 1: Using the Certbot Command Line
• Method 2: Using the AppViewX Certbot User-Friendly Script

Overview

Certbot can be accessed using two methods

1. Using the Certbot command line
2. Using the AppViewX Certbot user-friendly script

Method 1: Using the Certbot Command Line

• Activating the Developer Environment
• Enrolling Certificate
• Using Polling during Enrollment
• Custom and Certificate Attributes in Certbot Command
• Using EAB Details during Enrollment
• Schedule Task for Automated Certificate Renewal
• Revoking Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Activating the Developer Environment

To activate the developer environment, execute as shown below:

```
source venv/bin/activate
```

```
root@pe-pltf-devu-n2:/home/appviewx# cd certbot
root@pe-pltf-devu-n2:/home/appviewx/certbot# source venv/bin/activate
(venv) root@pe-pltf-devu-n2:/home/appviewx/certbot#
```

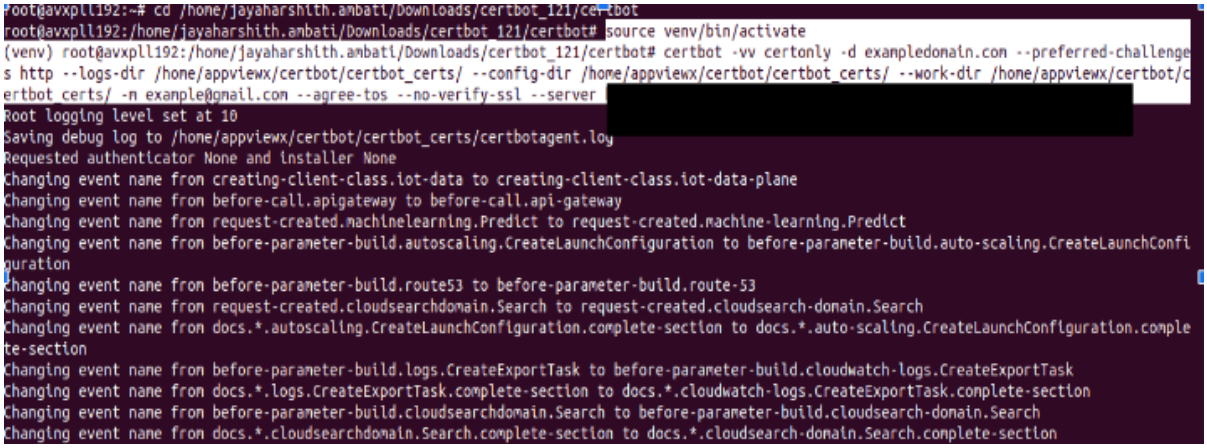
Enrolling Certificate

- A sample certbot certificate enrollment command is shown below.

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /home/appviewx/certbot/certbot_certs/

--config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME

server endpoint URL fetched from AppViewX GUI>
```



- Certbot can be run with **custom attributes**, allowing for additional command line arguments. These arguments can include multiple name-value pairs, which are then included in the "Finalize Order" call along with the CSR. The values for these fields will be provided as a JSON name/value pair, which we can retrieve and map to the custom attributes in our application. This mapping will enable us to include the custom attribute information in the certificate request for reporting purposes.
- A sample certbot certificate enrollment command with custom attributes is shown below.

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /home/appviewx/certbot/certbot_certs/

--config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME

server endpoint URL fetched from AppViewX GUI> --custom-attribute "Id:1,eai:test,inScope:yes,environment:envi1"
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- For more information on the usage of custom attributes in certbot refer to Custom Attributes in Certbot Command.
- For more information on the keywords used in certbot commands, refer to Certbot Keywords.

Using Polling during Enrollment

Polling can be activated when manual approval is configured for certificate generation. In this scenario, the client conducts polling for the certificate within a specified time frame, as determined by the configured parameters. If the certificate is approved before the polling duration expires, it will be retrieved. To enable polling in the certbot client, you may pass the parameters mentioned in the table below.

Parameters	Type	Mandatory	Description
--retry-after	Integer	No	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 10]
--retry-frequency	Integer	No	The number of times for which the certificate is polled from the client side. [Default value : 20]

A sample command with **retry-after** as **5** and **retry-frequency** as **10** is shown below. In this scenario, the certificate will be polled 10 times with a 5-second interval for each polling attempt. Therefore, the polling process will take a total of 10 * 5 = 50 seconds to complete.

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /home/appviewx/certbot/certbot_certs/
 --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME
 server endpoint URL fetched from AppViewX GUI> --custom-attribute "Id:1,eai:test,inScope:yes,environment:envi1" --retry-after 5 --retry-frequency 10
```

Note: To enable polling during the renewal process, it's important to include these parameters along with the renewal commands.

Custom and Certificate Attributes in Certbot Command

This section covers the **attributes** and **attribute-type** parameters.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. The **--attributes** field allows users to provide multiple attributes as a string with comma and colon separated values in the Certbot command.
   Format: **name:AppViewX,city:Coimbatore**

   The attributes field should adhere to the following guidelines.

   • The string must not be empty and must contain at least one name-value pair.
   • Multiple name-value pairs can be provided within the string separated by a comma.
   • Space is only allowed in the value field of the name-value pairs.
   • The attributes, after processing, will be sent as part of the payload in the finalize order call along with the CSR.
2. The "--attributes" field must be accompanied with the **--attribute-type** field which takes in one of the following inputs:
   ◦ cert
   ◦ custom
   ◦ both

   a. When **attribute-type** is passed as **cert** the attributes from the (--attributes) field are taken as certificate attributes. An example of certificate attribute is as follows:

   ```
   --attributes "id:1098,environment:development,Director:director_id" --attribute-type cert
   ```

   The below image depicts how certificate attributes are defined in certbot command.

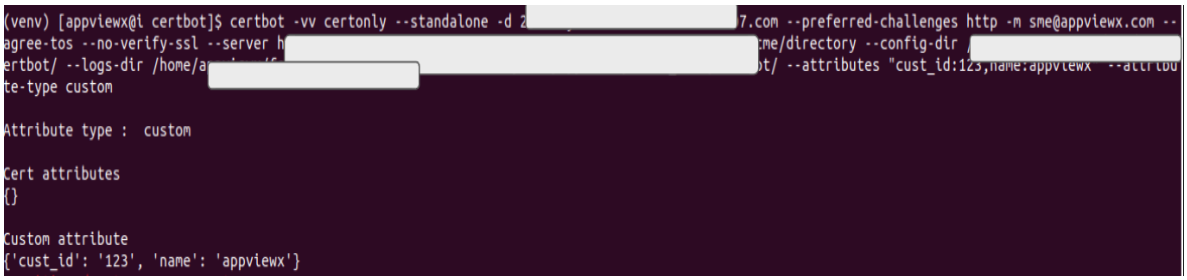
   

   b. When **attribute-type** is passed as **custom** the attributes from the (--attributes) field are taken as custom attributes. An example of certificate attribute is as follows:

   ```
   --attributes "cust_id:123,name:appviewx" --attribute-type custom
   ```

   The below image depicts how certificate attributes are defined in certbot command.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



c. When **attribute-type** is passed as **both**, A JSON mapping is expected by the AppViewX certbot. A new json file named **attributesMapping.json** needs to be created inside the certbot folder. A sample json file is given below.

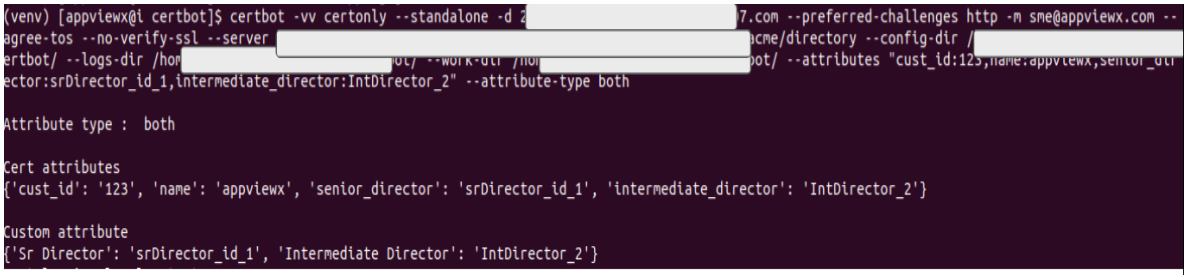
```
{
"senior_director" : "Sr Director",
"intermediate_director" : "Intermediate Director"
}
```

- The "key" [in the “key:value” pair from attributesMapping.json] refers to the certificate attribute key provided in the command, while the "value" corresponds to the custom attribute key where the value of the certificate attribute should be passed
- The attributes passed as input will be sent as certificate attributes and for the attributes present in the attributesMapping.json, the mapped value is being used as attribute name and sent as custom attribute.

An example of custom attribute is as follows:

```
--attributes "cust_id:123,name:appviewx,senior_director:srDirector_id_1,intermediate_director:IntDirector_2" --attribute-type both
```

The below image depicts how certificate attributes are defined in certbot command.



Note:

- The attributes are applicable only to *Method 1: Using the Certbot Command Line*.
- If the attributes and attribute-type field is not specified in the certbot command, normal flow of certbot will work fine without any exceptions.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Using EAB Details during Enrollment

A sample certbot certificate enrollment command with external account binding enabled in the ACME server.

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /home/appviewx/certbot/certbot_certs/
 --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME
 server endpoint URL fetched from AppViewX GUI> --eab-kid <Key identifier> --eab-hmac-key <MAC value>
```

Schedule Task for Automated Certificate Renewal

A single scheduled task is responsible to renew all certificates created by the certbot, but will only do so when it's actually necessary. The task runs every day at a specified time and checks the validity of all the certificates to determine if any of them should be renewed. Only the certificates that have a remaining validity period shorter than **30 days** will undergo renewal.

To automate renewal for Certbot through cron job, run the below command in the terminal:

```
(crontab -l ; echo "MM HH * * * /usr/bin/env bash -c 'source <certbot_folder/venv/bin/activate> && certbot renew --no-verify-ssl --no-random-sleep-on-renew
 --config-dir <config_dir>'") | crontab -
```

Fields to be provided in the above command:

- Specify time for renewal in **HH** (hours), **MM** (minutes)
- Specify path to '/venv/bin/activate' which is found in the installed certbot folder: **<certbot_folder/venv/bin/activate>**
- The path to the configuration directory that has been specified in the enrollment command. This directory contains the certificates that will be considered for renewal: **<config_dir>**.

Sample Command:

```
[root@cs-ia-rhel-n1 certbot]# crontab -l



[root@cs-ia-rhel-n1 certbot]# (crontab -l ; echo "37 22 * * * cd /home/appviewx/demo/certbot && /usr/bin/env bash -c
 'source /home/appviewx/demo/certbot/venv/bin/activate && certbot renew --no-verify-ssl --no-random-sleep-on-renew -
-config-dir /home/appviewx/demo/new3/'") | crontab -
[root@cs-ia-rhel-n1 certbot]# crontab -l



37 22 * * * cd /home/appviewx/demo/certbot && /usr/bin/env bash -c 'source /home/appviewx/demo/certbot/venv/bin/acti
vate && certbot renew --no-verify-ssl --no-random-sleep-on-renew --config-dir /home/appviewx/demo/new3/'
[root@cs-ia-rhel-n1 certbot]#
```

As per the above command, the scheduled renewal task is triggered at 06:30 am on a daily basis.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note:

- The cron jobs operate according to the server's predefined timezone, typically set to UTC by default. You can verify this timezone by running the date command in the terminal. Scheduled tasks will commence in accordance with the cron system's understanding of time and time zones.
- If you need to modify the time for a cron job that you've previously set up, you can adjust it by editing the time in the crontab file using the following command:

```
crontab -e
```

- To check the scheduled cron jobs execute the command

```
crontab -l
```

- To enable polling during the renewal process, it's important to include the polling parameters along with the renewal commands.

Revoking Certificate

The revocation of the certificate can be done using two ways: one is using the cert path and other is using the cert name.

Cert Path

```
certbot revoke --cert-path /home/certbot_client/certbot/certbot_certs/live/<domain_name>/fullchain.pem --config-dir /home/certbot_client/certbot/certbot_certs/ --work-dir /home/certbot_client/certbot/certbot_certs/ -m <mail_id> --no-verify-ssl --agree-tos --server <ACME server endpoint URL fetched from AppViewX GUI>
```

Cert Name

```
certbot revoke --cert-name <domain_name> --config-dir /home/certbot_client/certbot/certbot_certs/ --work-dir /home/certbot_client/certbot/certbot_certs/ -m <mail_id> --no-verify-ssl --agree-tos --server <ACME server endpoint URL fetched from AppViewX GUI>
```

Method 2: Using the AppViewX Certbot User-Friendly Script

- Activating the Virtual Environment
- Enrolling or Renewing Certificate
- Revoking Certificate

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Creating or Editing the Configuration File
• Points to Remember

Activating the Virtual Environment

With the AppViewX Certbot user friendly script you can execute commands to perform enroll, renew, and revoke certificate actions by activating the virtual environment as described in the steps below.

1. Navigate to the certbot folder and open terminal from that path.

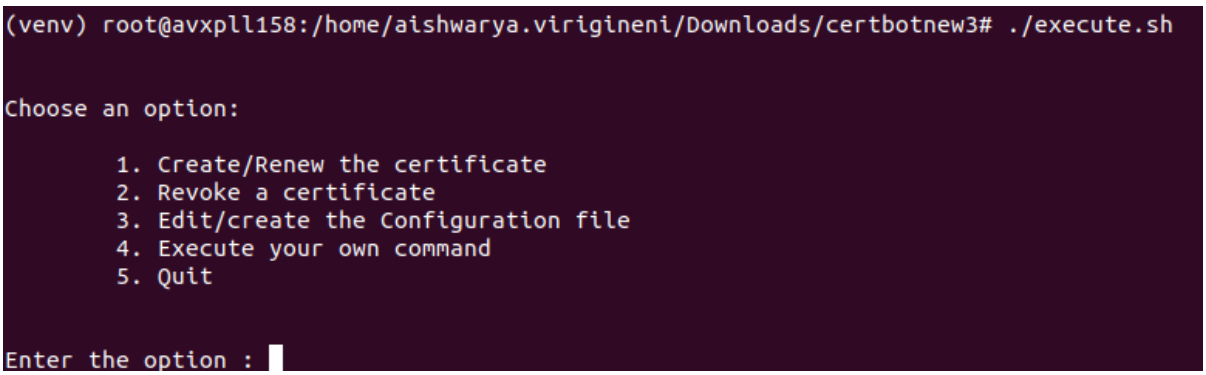
```
cd /path/to/file/AppViewX_ACME_Certbot_Client
```

2. Run the command

```
./execute.sh
```

> **Note:** You must login as a root user (`sudo -i`) before executing the `execute.sh` file.

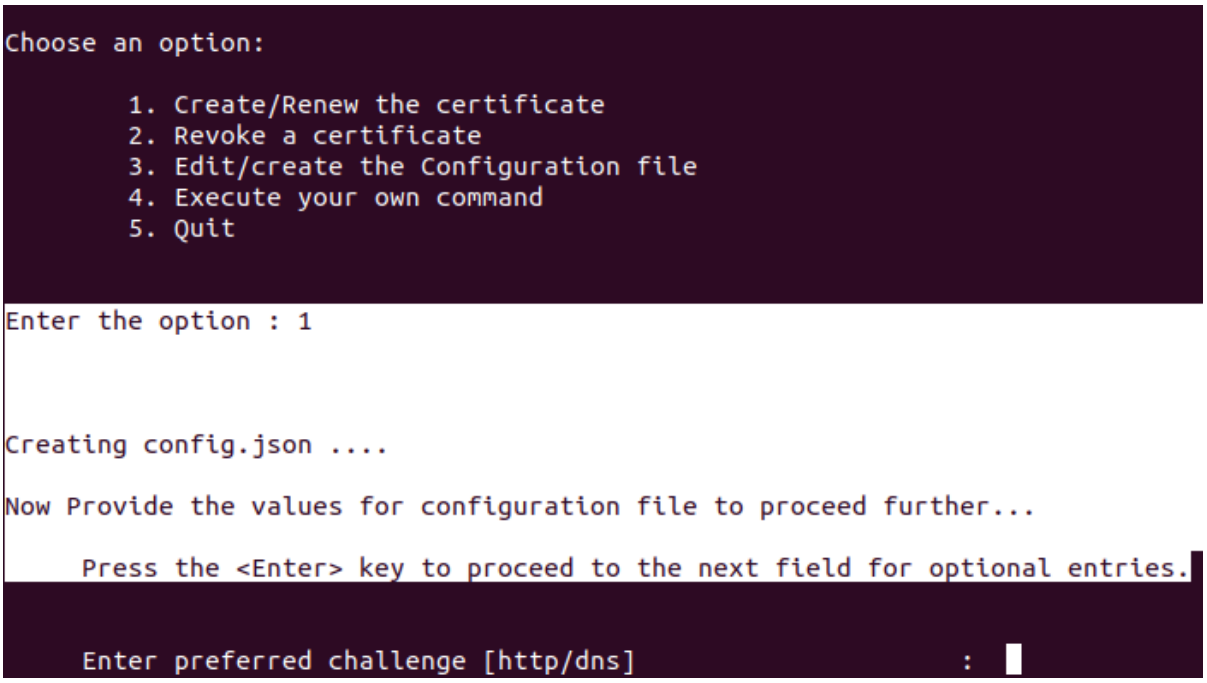
Once certbot is ready to use, it displays the following options.



- 1. Create/Renew a certificate
- 2. Revoke a certificate
- 3. Edit/create the Configuration file
- 4. Execute your own command
- 5. Quit

3. When using the user prompt for the first time you are automatically redirected to option 3 even if you select option 1 or 2. This is to fill all the parameters that are required for the command to be executed as shown in the next sections.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



All the parameters are stored in a json config file (/<filepath>/AppViewX_ACME_Certbot_Client/certbot/config.json) created by AppViewX. A sample of the configuration being updated is shown below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
Choose an option:

        1. Create/Renew the certificate
        2. Revoke a certificate
        3. Edit/create the Configuration file
        4. Execute your own command
        5. Quit


Enter the option : 1



Creating config.json ....

Now Provide the values for configuration file to proceed further...

     Press the <Enter> key to proceed to the next field for optional entries.


     Enter preferred challenge [http/dns]                    :  http
     Enter logs directory path (optional)                    :  /home/appviewx/certbot/certbot_certs/
     Enter config directory path (optional)                  :  /home/appviewx/certbot/certbot_certs/
     Enter work directory path (optional)                    :  /home/appviewx/certbot/certbot_certs/
     Enter email address                                     :  example@gmail.com
     Enter server URL                                        :  <ACME server endpoint URL fetched from AppViewX GUI>
     Enter whether to perform SSL verification? [y/n]        :  y
     Enter EAB kid (optional)                                :
     Enter EAB HMAC key (optional)                           :


Inputs saved to Configuration file
```

```
Inputs saved to Configuration file

Creating/Renewing a cert option selected....


*********************************************************************
The following are the recently configured values provided by you.
*********************************************************************

The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :
```

Enrolling or Renewing Certificate

1. Now basis the previous section, to create/renew a certificate enter **1**.

   A JSON configuration file will be displayed which has the fields with previously saved values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
Enter the option : 1


Creating/Renewing a cert option selected....


*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :
```

2. To proceed with the displayed values (already existing values in the JSON configuration file), press the **ENTER** key.
3. Enter the *domain name* for which the certificate needs to be enrolled.

```
*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :


        Enter the domain names for which the certificate needs to be created     : exampledomain.com



certbot -vv certonly -d exampledomain.com --null --preferred-challenges http --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /ho
me/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME server end
point URL fetched from AppViewX GUI>
```

The process continues and the certificate from the specified path is created.

Revoking Certificate

1. To revoke a certificate enter **2**.

   A JSON configuration file will be displayed which has the fields with previously saved values.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
Choose an option:

        1. Create/Renew the certificate
        2. Revoke a certificate
        3. Edit/create the Configuration file
        4. Execute your own command
        5. Quit


Enter the option : 2


Revoking a cert option selected.....


*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Server plugin configured is                : null
The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :
```

2. To proceed with the displayed values (already existing values in the JSON configuration file), press the **Enter** key.
3. Enter the *certificate path* for which the certificate needs to be revoked.

```
Revoking a cert option selected.....


*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Server plugin configured is                : null
The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :


        Enter the Certificate Path                                          : /home/path_to_the_cert_that_needs_to_be_revoked


certbot -vv revoke --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appvie
wx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME server endpoint URL fetched from AppViewX GUI> --cert-path /home/pat
h_to_the_cert_that_needs_to_be_revoked
```

The process continues and the certificate from the specified path is revoked.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Creating or Editing the Configuration File

1. To edit the displayed values (already existing values in the JSON configuration file), enter **1** to exit and then enter **3** to edit the configuration file.

```
Choose an option:

        1. Create/Renew the certificate
        2. Revoke a certificate
        3. Edit/create the Configuration file
        4. Execute your own command
        5. Quit


Enter the option : 3


Creating or Editing Configuration file Option is selected


*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Server plugin configured is               : null
The Preferred Challenges selected is          : http
The Logs Directory path provided is           : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is         : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is           : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                 : example@gmail.com
The Server URL provided is                    : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                     : y
The EAB Kid value provided is                 :
The EAB HMAC Key provided is                  :


  Press the <Enter> key to proceed using the previously configured value.


  Enter preferred challenge [http/dns]                        :
```

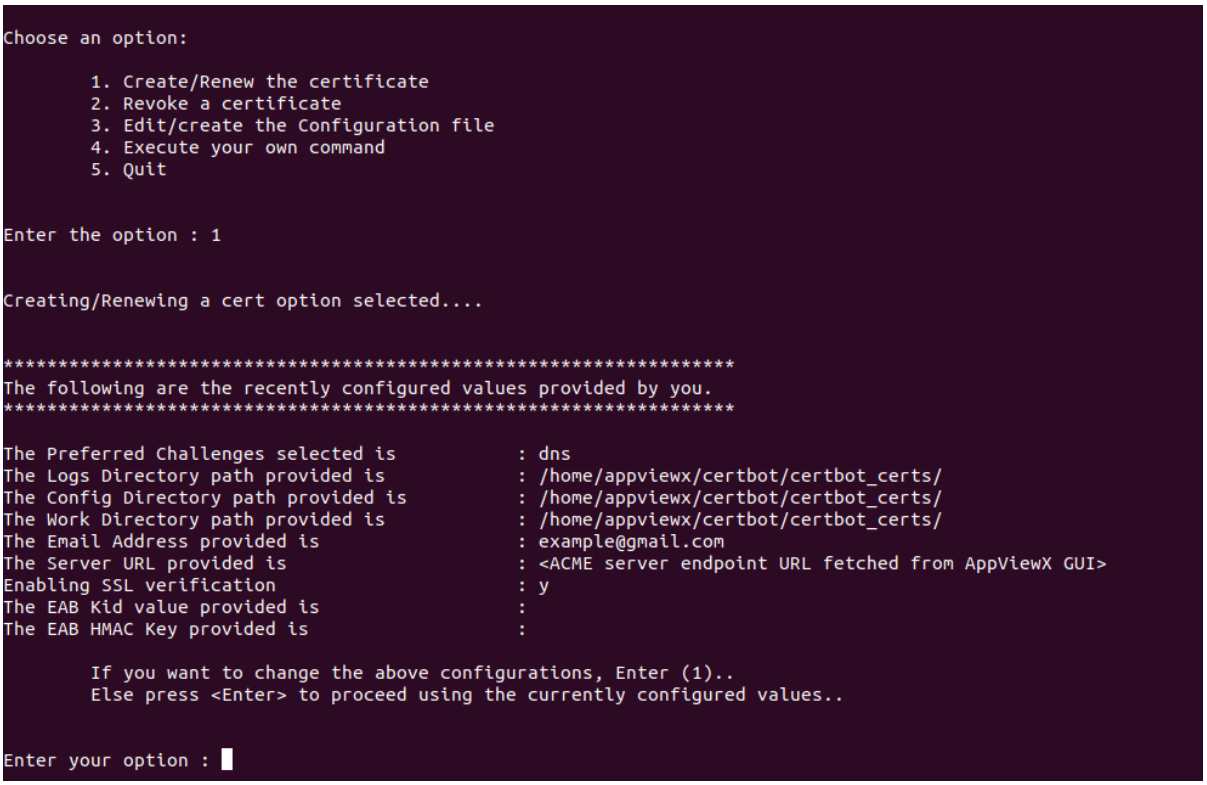
2. As an example, change the **preferred_challenges** value to *DNS*. Enter the value "DNS" accordingly.

```
  Press the <Enter> key to proceed using the previously configured value.


  Enter preferred challenge [http/dns]                        :  dns
  Enter logs directory path [ Enter 1 if you want to clear ]  :
  Enter config directory path [ Enter 1 if you want to clear ]:
  Enter work directory path [ Enter 1 if you want to clear ]  :
  Enter email address                                         :
  Enter server URL                                            :
  Enter whether to perform SSL verification? [y/n]            :
  Enter EAB kid [ Enter 1 if you want to clear ]              :
  Enter EAB HMAC key [ Enter 1 if you want to clear ]         :


Inputs saved to Configuration file
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Note: If you intend to proceed with the displayed values (already existing values in the JSON configuration file), press the **Enter** key.

3. Select and enter the *DNS server* among all the list DNS servers supported by certbot.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
****************************************************************

The Preferred Challenges selected is           : dns
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :




The below are the server plugins.. Choose the required plugin

                          1 . dns_cloudfare                 :
                          2 . dns_digitalocean
                          3 . dns_dnsimple
                          4 . dns_dnsmadeeasy
                          5 . dns_gehirn
                          6 . dns_google
                          7 . dns_linode
                          8 . dns_luadns
                          9 . dns_nsone
                         10 . dns_ovh
                         11 . dns_rfc2136
                         12 . dns_route53
                         13 . dns_sakuracloud

Enter your Choice :
```

4. Enter the credentials of the DNS server such that the command would be executed accordingly.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
The below are the server plugins.. Choose the required plugin

                          1 . dns_cloudfare                 :
                          2 . dns_digitalocean
                          3 . dns_dnsimple
                          4 . dns_dnsmadeeasy
                          5 . dns_gehirn
                          6 . dns_google
                          7 . dns_linode
                          8 . dns_luadns
                          9 . dns_nsone
                         10 . dns_ovh
                         11 . dns_rfc2136
                         12 . dns_route53
                         13 . dns_sakuracloud

Enter your Choice : 12


dns_route53 option selected....



***************************
ROUTE53 CREDENTIALS FILE
***************************
[default]
aws_access_key_id=<enter_valid_aws_access_key_id>
aws_secret_access_key=<enter_valid_aws_secret_access_key>


The above are the present values of the credentials file for dns_route53..
        If you want to  change them, Enter (1) to edit credentials..
        Else press <Enter> to continue with the old value..


Enter your option :
```

a. This process involves creating a secrets folder (in */path/to/file/AppViewX_ACME_Certbot_Client/certbot)* which stores all the credential files with token/credentials) of all the DNS servers supported. The token/credentials are provided by the users.

```
*************************
ROUTE53 CREDENTIALS FILE
*************************
[default]
aws_access_key_id=<enter_valid_aws_access_key_id>
aws_secret_access_key=<enter_valid_aws_secret_access_key>


The above are the present values of the credentials file for dns_route53..
        If you want to  change them, Enter (1) to edit credentials..
        Else press <Enter> to continue with the old value..


Enter your option :


        Enter the domain names for which the certificate needs to be created     : exampledomain.com


certbot -vv certonly -d exampledomain.com --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-d
ir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME serv
er endpoint URL fetched from AppViewX GUI>
```

b. Once the credentials file is created, you can continue with the existing credentials file values or modify them to proceed with the new values by using the prompted guidance on the screen.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

c. For DNS route 53 alone, certbot application stores the required credentials/tokens in the /root/.aws/credentials path. Initially it checks for the **.aws** folder in /root/.aws path and if not found it creates a **.aws** folder and a credentials file inside it.

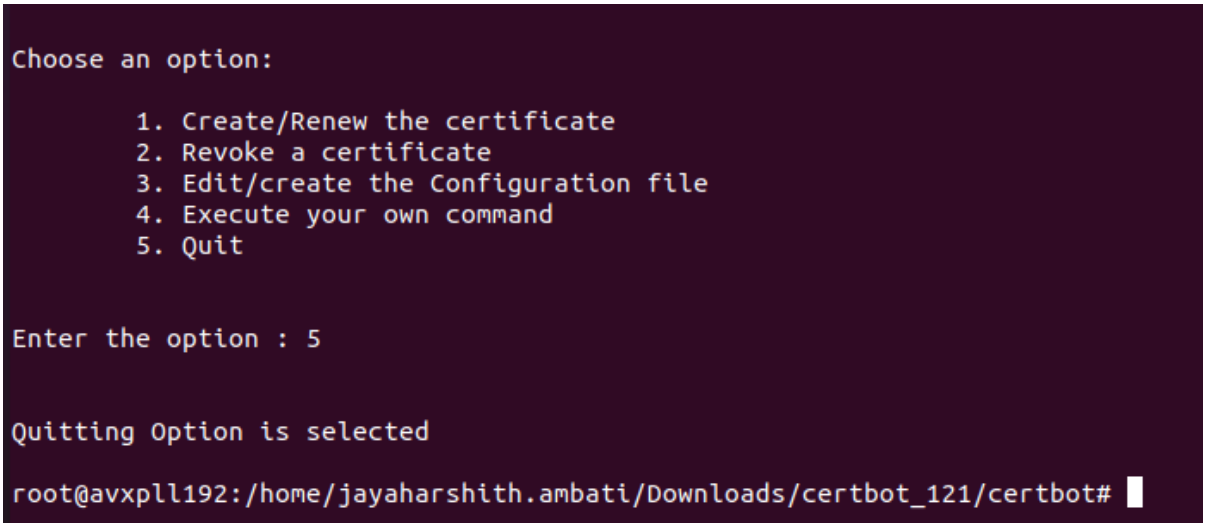
d. If the **.aws** folder and **credentials** file is found in the root directory, the values are updated as per the inputs provided. You can proceed with the existing values or with new values by editing the credentials file.

e. For all the remaining DNS servers, inputs (tokens/keys) for the credentials file are taken from the user. Once the credentials file is created, you can continue with existing credentials file values or modify and proceed with the new values by using the prompted guidance on the screen.

5. To execute your own commands manually select/enter option **4**.



6. After the selected option's functionality is done, all the five options would be displayed each time in the same virtual environment until the quit option **5** is selected.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Points to Remember

1. Preferred challenges should either be given as **http** or **dns** only.
2. **Agree to terms of services** and **verify ssl** fields should either be given as *y (yes) or n (no)*.
   If the ***verify ssl*** field is enabled (i.e. when the **verify ssl** field is given as **y**), refer to the section Adding Custom CA Certificates to Trust Store.
3. Provide valid **email address** and **domain names**.
4. The **eab_kid** and **eab_hmac_key** fields.
   a. These are optional fields, you can proceed to the next by pressing the **Enter** key without providing the values.
   b. The values can be cleared from the JSON configuration file by selecting **1** at the time of editing the configuration file.
5. You can enter new values when option 3 (Edit/Create the Configuration file) is selected. Select fields can be edited/updated and for all retaining old values press the **Enter** key.
6. The **domain name** field
   a. Provide a ***single domain name*** to acquire a certificate for a particular domain.
   b. Provide comma separated ***multiple domain names*** to acquire a certificate for all the given domains.
   c. ***Wildcard certificates*** can be acquired by providing input for a particular domain.
7. The **jq** package.
   a. Having the ***jq*** package installed on your system is a prerequisite (must) to proceed with the user prompt guidance provided by the script. Ignore this step if it's not compatible with your environment.
   b. After executing the *execute.sh* script, the system checks if the **jq** package is installed on your system.
   c. If it is not installed on your system and you want to access the user prompt guidance,click 1 to proceed with the installation.
   d. You may also click 2 to exit and execute your own command manually in the same virtual environment created by *execute.sh* script.

Troubleshooting

• Client-Side Errors

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Client-Side Errors

General Errors

Sr. No.	Error Message	Description	Troubleshooting
1	Challenge failed for domain testav.appviewx.com Notifying user: Certbot failed to authenticate some domains (authenticator: standalone). Some challenges have failed.	HTTP challenge validation failed.	Make a DNS entry.
2	Unable to locate credentials To use certbot-dns-route53, configure credentials as described at https://boto3.readthedocs.io/en/latest/guide/configuration.html#best-practices-for-configuring-credentials and add the necessary permissions for Route53 access.	DNS challenge validation failed. Invalid credentials were utilized for DNS challenge validation.	Ensure the credentials in the credentials file are valid.
3	An error occurred (InvalidClientTokenId) when calling the ListHostedZones operation: The security token included in the request is invalid. To use certbot-dns-route53, configure credentials as described at https://boto3.readthedocs.io/en/latest/guide/configuration.html#best-practices-for-configuring-credentials and add the necessary permissions for Route53 access.	DNS challenge validation failed. The required credentials file for DNS challenge validation is missing.	Ensure the credentials file with the required credentials is present and valid.
4	{"appStatusCode":"AVX_GW_009","message":"Resource not found, reason - Invalid apiid"} An unexpected error occurred: acme.messages.Error: about:blank	The provided endpoint url is improperly configured.	Ensure that the endpoint URL is valid.
5	An unexpected error occurred:	The user interface has	Verify that the user interface

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
	requests.exceptions.ConnectionError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: / avxapi/acmeTest/acme/directory (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f3ddc7d7970>: Failed to establish a new connection: [Errno -2] Name or service not known'))	an incorrect configuration for the endpoint.	is correctly set up with the appropriate endpoint configuration.
6	An unexpected error occurred: requests.exceptions.InvalidURL: Failed to parse: https:// <hostname/ipaddress>:314423/avxapi/acmeTest/ acme/ directory	The provided endpoint URL contains an invalid port number. **(or)** Network configuration regulations, firewall rules that prevent access to the required port.	Ensure that the port specified in the endpoint URL is valid.
7	An unexpected error occurred: ValueError: Requesting <hostname/ ipaddress>.appviewx.net/avxapi: Connection refused	The user interface has an incorrect configuration for the endpoint port.	Verify that the port is properly configured within the user interface.
8	Client with the currently selected authenticator does not support any combination of challenges that will satisfy the CA. You may need to use an authenticator plugin that can do challenges over DNS.	The challenge type set on the server side is HTTP, but the request sent	The request made from the client must be configured

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
		from the client was configured using the DNS challenge.	to use HTTP challenge.
9	Client with the currently selected authenticator does not support any combination of challenges that will satisfy the CA.	The challenge type set on the server side is DNS, but the request sent from the client was configured using the HTTP challenge.	The request made from the client must be configured to use DNS challenge.
10	Notifying user: Certbot failed to authenticate some domains (authenticator: standalone). Some challenges have failed.	Obtaining wildcard certificates through HTTP challenge validation.	Obtain wildcard certificates exclusively through the DNS challenge validation.
11	Certificate did not match expected hostname: <hostname/ ipaddress> Certificate: {'subject': ((('commonName', 'comman_name'),),), … An unexpected error occurred: requests.exceptions.SSLError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: / avxapi/acmeTest/acme/directory (Caused by SSLError(SSLCertVerificationError("hostname '<hostname/ipaddress>' doesn't match 'serverside_configured_<hostname/ipaddress>'")))	Setting up the ACME endpoint with an IP address to facilitate SSL verification.	Configure the ACME end point with FQDN (Fully Qualified Domain Name) instead of IP address for SSL verification.
12	Another instance of Certbot is already running	Attempting to launch Certbot	Terminate the Certbot process

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
		while another instance is already active, or when the Certbot process is forcefully terminated.	that ended abruptly, or terminate the currently active Certbot process. Use the command: **pkill -9 certbot**
13	The following error was encountered: [Errno 13] Permission denied: '/home/jayaharshith.ambati/certbotagent.log' Either run as root, or set --config-dir, --work-dir, and --logs-dir to writeable paths.	In cases where administrative privileges are not granted.	Ensure administrative privileges (sudo access) is provided to run Certbot.
14	Too many flags setting configurators/installers/authenticators 'standalone' -> 'dns-route53'	Utilizing both the standalone plugin and the DNS plugin (DNS Route 53).	At any given time, we have the option to select only one plugin, which means we can choose either --standalone or --dns-route-53, but not both simultaneously.
15	IndexError: list index out of range	When there is a lack of input for at least one custom attribute.	Using custom attributes requires at least one input to be provided.
16	key, value = attr.split(':')	When custom attributes are not	Custom attributes need

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
	ValueError: not enough values to unpack (expected 2, got 1)	provided in the format of key-value pairs.	to be provided in the form of key-value pairs.
17	An unexpected error occurred: The "externalAccountBinding.protected" field is invalid.:: kid is invalid	When the **--eab-kid** value is altered or provided incorrectly, an error occurs.	Please ensure that the provided **--eab-kid** value matches the configuration set in the AppViewX UI.
18	{"detail":"The \"externalAccountBinding.signature\" field is invalid.","type":"urn:ietf:params:acme:error:invalidExternalAccountBindingParameters(signature)"} An unexpected error occurred: The "externalAccountBinding.signature" field is invalid.	When the **--eab-hmac-key** value is altered or provided incorrectly, an error occurs.	Please ensure that the provided **--eab-hmac-key** value matches the configuration set in the AppViewX UI.
19	An e-mail address or --register-unsafely-without-email must be provided.	Email address is not provided in the command.	Please ensure that a valid email address is provided in the command.
20	An unexpected error occurred: requests.exceptions.SSLError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: /avxapi/acmeTest/acme/directory (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1131)')))	SSL Verification failed.	In order to activate SSL Verification, it's essential to confirm that the server trust chain certificates exist within the machine's trust store. To

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
			achieve this, you can refer to the instructions outlined in in “Setting the Custom CA Certificate Path Manually.”
21	Could not bind TCP port 80 because it is already in use by another process on this system (such as a web server). Please stop the program in question and then try again.	Port 80 is not accessible.	Stop any process running on port 80 as the Linux machine should be accessible from AppViewX CC (port 80) for HTTP-01 challenge.

Other General Errors

Some of the other general errors that can be encountered are as follows:

Sr.No.	Error and Cause	Solution
1	Firewall blockage connectivity error A "firewall blockage connectivity error" when using Certbot typically occurs when the Certbot client is unable to establish a connection to external servers due to network restrictions or firewall rules. This can prevent Certbot from successfully completing the domain ownership verification process required to obtain SSL/TLS certificates.	Ensure that network restrictions or firewall rules are configured as necessary.
2	The port to contact with Acme End point is not accessible error	**Firewall Rules:** If your server is behind a firewall or network

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Sr.No.	Error and Cause	Solution
		security appliance, ensure that the necessary ports (typically ports 80 and 443) are allowed for inbound and outbound connections. ACME challenges often use these ports to verify domain ownership. **Blocked Ports:** Some hosting providers or network environments might block certain ports, including ports 80 and 443, to prevent web services from being accessible. Verify that the necessary ports are open and accessible.

Errors due to extra arguments

Errors are also encountered if any extra arguments, other than supported arguments are given in the certbot command. They are as follows:

1. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -`

   Error: certbot: error: unrecognized arguments: -

2. **Sample command:** `certbot certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> cert`

   Error: certbot: error: unrecognized arguments: cert

3. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -cert`

   Error: certbot: error: Unable to open config file: ert. Error: No such file or directory

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -test`

   Error: certbot: error: argument -t/--text: ignored explicit argument 'est'

Glossary

• Certbot Keywords

Certbot Keywords

Keyword	Expected Input	Comments
-v, --verbose	NA	This flag can be used multiple times to incrementally increase the verbosity of the output, e.g. -vvv. (default: 0)
(default) run	NA	Obtain and install a certificate in your current web server.
certonly	NA	Obtain or renew a certificate, but do not install it.
--standalone	NA	Run a standalone web server for authentication.
-d (Domain)	<domain1.com> or <domain2.com>, <domain3.com>, <domain4.com>	Comma-separated list of domains to obtain a certificate for.
--preferred-challenges	http/dns	A sorted, comma delimited list of the preferred challenge to use during authorization with the most preferred challenge listed first. The default value of preferred challenges is an **empty list.**
--config-dir	<path_to_config_directory>	The config directory contains Certbot's configuration files,

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keyword	Expected Input	Comments
		including information about the certificates, domains, renewal settings, and more. It's where Certbot stores its persistent configuration data. Certbot keeps track of the certificates it manages, their associated options, and renewal schedules in this directory. Custom configuration directory path (**default**: /etc/letsencrypt).
--work-dir	<path_to_work_directory>	The work directory is used by Certbot to store temporary files and data while it performs operations like certificate issuance and renewal. This directory is where Certbot creates and stores temporary challenges required for domain ownership verification during the certificate issuance process. It's a workspace for Certbot's internal processes. Custom working directory path (**default**: /var/lib/letsencrypt).
--logs-dir	<path_to_logs_directory>	The logs directory contains log files that record the activities and events related to Certbot's operations. These logs can provide valuable information for troubleshooting issues and understanding the certificate issuance and renewal process. Logs include details about challenges, certificate renewals, errors, and more.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keyword	Expected Input	Comments
		Custom logs directory path (**default**: /var/log/letsencrypt).
-m	<example1@gmail.com> or <example2@gmail.com>, <example3@gmail.com>	Email used for registration and recovery contact. Use commas to register multiple emails. Email address for important account notifications.
--agree-tos	NA	Agree to the ACME server's Subscriber Agreement.
--no-verify-ssl	NA	Disable verification of the ACME server's certificate.
--server	<Acme Server Endpoint URL fetched from AppViewX GUI>	ACME Directory Resource URI. (default: https://acme-v02.api.letsencrypt.org/directory)
--eab-kid EAB_KID	<value_of_EAB_KID>	Key Identifier for External Account Binding (Optional).
--eab-hmac-key EAB_HMAC_KEY	<value_of_EAB_HMAC_KEY>	HMAC key for External Account Binding (Optional).
revoke	NA	Used for revoking a certificate.
--cert-path	<path_to_certificate> Example: /home/appviewx/certbot/certbot_certs/live/certbot.appviewx.info/fullchain.pem	Path to where certificate is saved (with certonly --csr), installed from, or revoked (default: None)
--dns-route53	NA	Obtain certificates using a DNS TXT record (if you are using Route53 for DNS). (default: False).

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keyword	Expected Input	Comments
--attributes	Sample input: **"name:AppViewX,city:Coimbatore"** The string should not be empty and must contain at least one name-value pair.	The --attributes field allows users to provide multiple attributes as a string with comma and colon separated values in the Certbot command. [It is optional, but **--attributes** field must be accompanied with the **--attribute-type** field.]
--attribute-type	Any one of the following : **cert/ custom/both**	Takes in one of the following inputs **cert/custom/both**. [It is optional, but must be included when **--attributes** is passed.]
--retry-after	Integer	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 10]
--retry-frequency	Integer	The number of times for which the certificate is polled from the client side. [Default value : 20]

Winacme Configuration Guide

This guide gives an overview on how Winacme clients works with AppViewX via ACME protocol to request for certificates from supported CAs.

- Introduction to ACME Protocol
- Winacme
- Installation and Configuration
- Winacme Usecases

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Introduction to ACME Protocol

ACME, or Automated Certificate Management Environment, is a communications protocol that leverages an agent to automate the process of CSR generation and certificate/key rotation. It is primarily used by the popular public CA, Let's Encrypt, as a part of their business model of issuing 90-day Domain Validated certificates (as Organizational Validation and Extended Validation certificates require human supervision to issue, thus rendering the point of ACME moot), and automating their renewals.

The protocol was initially developed by the Internet Security Research Group (ISRG) for the Let's Encrypt CA, and, as an open-source tool, free to use. While originally only used by Let's Encrypt to issue x.509 (SSL/TLS) certificates, various other CAs, PKI vendors, and browsers are now beginning to support ACME to work with other kinds of certificates (S/MIME, Code-signing) as well. However, to leverage them, the CA should be able to access the DNS/HTTPS token that is published. This makes it better suited to be an internal PKI issuance method.

Winacme

- Introduction to WinAcme
- System Requirements
- Startup Problems
- Prerequisite for Running Clients

Introduction to WinAcme

WinAcme, also known as "wacs," stands as an open-source software dedicated to simplifying SSL/TLS certificate management within Windows server environments. Its primary purpose is to automate the intricate process of obtaining and renewing SSL certificates through seamless interaction with Let's Encrypt, a prominent Certificate Authority offering complimentary SSL certificates. Operating primarily through a command-line interface, WinAcme aligns itself with various Windows versions, ensuring its adaptability across a diverse range of systems. Its versatility shines through support for multiple validation methods, effectively easing the management of SSL certificates.

The essence of WinAcme lies in its commitment to providing a user-friendly solution for individuals and entities seeking to secure their digital domains. The tool's capabilities extend beyond the basics, allowing the issuance of wildcard certificates, centralized configuration management, and extensibility via plugins and hooks. As a result, WinAcme empowers administrators and developers by simplifying SSL/TLS certificate management, reducing manual intervention, and enhancing overall security for websites and web applications. With its active community and dedication to enhancing online security, WinAcme

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

emerges as a valuable asset for those navigating the complexities of SSL certificate management in Windows environments.

System Requirements

- *Operating System*: Windows Server 2012 R2 SP1 and higher.
- *Framework*: .NET Core 5 or higher
- *RAM*: 4GB or higher

Startup Problems

- You may need to install Microsoft Visual C++ 2015 Redistributable Update 3
- If you run into the error about `api-ms-win-crt-runtime-l1-1-0.dll`, you may need KB2999226.
- If you run into the error about `hostfxr.dll`, you may need KB2533623.
- If you run into an error like a `Failure processing application bundle`, perhaps this thread might provide a solution.
- If the program doesn't seem to start but an error like `Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:App.AppXc99k5qnnsvxj5szemm7fp3g7y08we5vm.mca` is displayed in the Event Viewer, this thread might provide a solution.

Prerequisite for Running Clients

- The AppViewX server needs to have a valid certificate installed on its domain.
- A proper DNS entry for the Linux server.
- A valid ACME endpoint should be configured on the AppViewX GUI.
- To enable client connections, it's essential to have ports 31443 open for on-premises deployment and 30020 in cloud connectors open for SaaS deployment in AppViewX.
- If the domain validation is set as HTTP, it's essential to have port 80 accessible on your Windows machine to allow AppViewX to establish a connection.

Installation and Configuration

- Downloading the Files
- Configuring the URL

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

• Configurations For Task Scheduling
• Configurations To Enable Polling

Downloading the Files

1. Download the latest version from the AppViewX release portal.
2. Unzip files to a non-temporary folder, so that the scheduled task will be able to run. We recommend using `%program files%\win-acme`
3. The **settings.json** file inside the *win-acme* folder will be used for further configurations.

Configuring the URL

The following change must be done in the **settings.json** file:

- From the ACME GUI in AppViewX, take the URL from the **Directory URL** field (CERT+ →ADMINISTRATION→Auto Enrollment → ACME) and update the **DefaultBaseUri** field in the **settings.json** file.

Configurations For Task Scheduling

A single scheduled task is responsible to renew all certificates created by the program, but will only do so when it's actually necessary. The task runs every day and checks if the certificate is getting too old. This relies on the threshold specified within the **settings.json** file under the parameter **RenewalMinimumValidDays**. Certificates that have a remaining validity period shorter than the threshold will undergo renewal. The following are configuration settings in the **settings.json** file located within the *win-acme* directory:

Adjusting settings under the Cache field

- Adjust the value of **"ReuseDays"** to **"0"**:

  When you renew or re-create a certificate with the exact same set of domain names as a previously requested certificate, **"ReuseDays"** determines how many days the program will use a cached version of the certificate. Setting "ReuseDays" to 0 prevents these cached files from being used for renewals.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The default value for **"ReuseDays"** is set to **"1"**.

```
"Cache": {
  "ReuseDays": 0,
  "DeleteStaleFiles": false,
  "Path": null
},
```

Adjusting settings under the ScheduledTask field

1. Adjust the value of **"RenewalMinimumValidDays"** to the number of days a certificate should be still valid. If a certificate's remaining validity falls below this specified threshold, the system will initiate automatic renewal.

   The default value for **"RenewalMinimumValidDays"** is set to **"nul"**, which is interpreted as 7 days.

   For instance, if you set the parameter to 10, certificates with less than 10 days of validity remaining will undergo renewal through the task scheduler. Certificates with 10 days or more remaining validity will not be renewed.

2. Adjust the**"StartBoundary"** to specify the start time for the scheduled task.

   The default value for **"StartBoundary"** is set to **"09:00:00"**, which is interpreted as 9:00 am (local time).

3. *Optional Step (Perform if necessary)* - Set **"RandomDelay"** to **"00:00:00"** (0 hours), time to wait for starting the scheduled task to spread the load on the servers and thus prevent users from getting TooManyRequests errors.

   The default value for **"RandomDelay"** is set to **"04:00:00"**, which is interpreted as 4 hours.

```
"ScheduledTask": {
  "RenewalDays": 55,
  "RenewalMinimumValidDays": 10
  "RandomDelay": "00:00:00",
  "StartBoundary": "10:00:00",
  "ExecutionTimeLimit": "02:00:00"
},
```

Configurations To Enable Polling

The following configurations are within the **'Acme'** category in the **settings.json** file:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Configure the **"RetryCount"** parameter to determine the maximum number of times to refresh validation and order status, while waiting for the ACME server to complete its tasks. By default, this value is set at **15**.
- Configure the **"RetryInterval"** parameter to the amount of time in seconds to wait for each retry. By default, this value is set to **5 seconds**.
- *Example*: Let's consider a scenario where the **RetryCount** is set at **30**, and the **RetryInterval** is configured as **5** seconds. In this case, the **total timeout duration (polling time)** would be calculated as **30 multiplied by 5 seconds**, resulting in **150 seconds**.



Winacme Usecases

- Creating First Certificate
- Scheduling Tasks for Auto-Renewal
- Revoking Certificates
- Health Checks
- Monitoring
- Testing and Troubleshooting
- Support for Other .NET Version

Creating First Certificate

There are different ways to run winacme,

- Enroll using interactive terminal
- Run in background using the powershell command

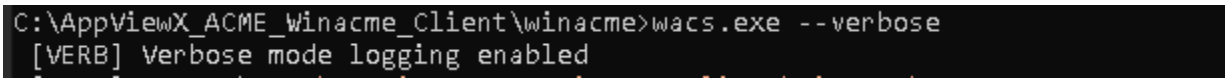
- Enroll Using Interactive Terminal
- Winacme Enrollment Process in the Background

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Enroll Using Interactive Terminal

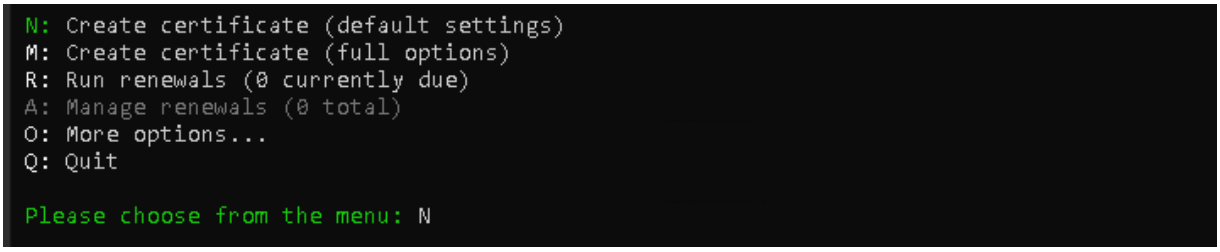
Before you begin: To proceed with enrollment run the following command with administrator privileges.

```
wacs.exe
```

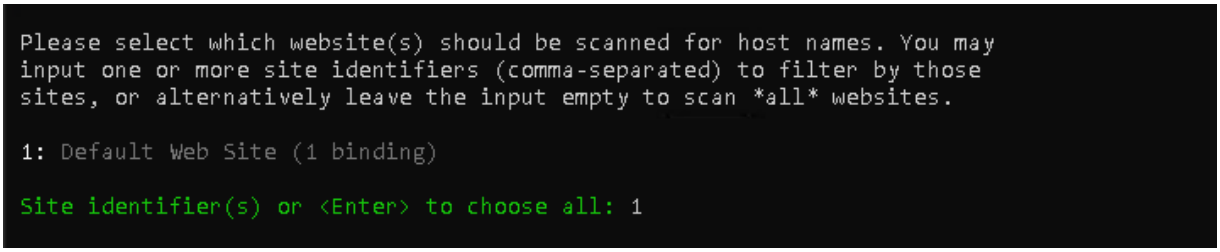


The default settings are for users looking to install a regular (non-wildcard) certificate on their local IIS instance.

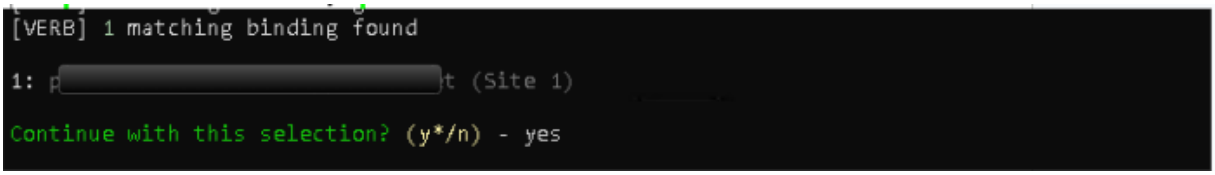
1. To create a new certificate with default settings, choose N in the main menu.



2. Choose how you want to determine the domain name(s) that are to be included in the certificate. This can be derived from the bindings of an IIS site or can be entered manually.







Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Note: Note : If EAB is enabled in the Appviewx ACME configuration settings, WINACME will prompt to enter the key identifier and key (base64 url encoded) [enter the value from MAC value in the place of key (base64 url encoded)]

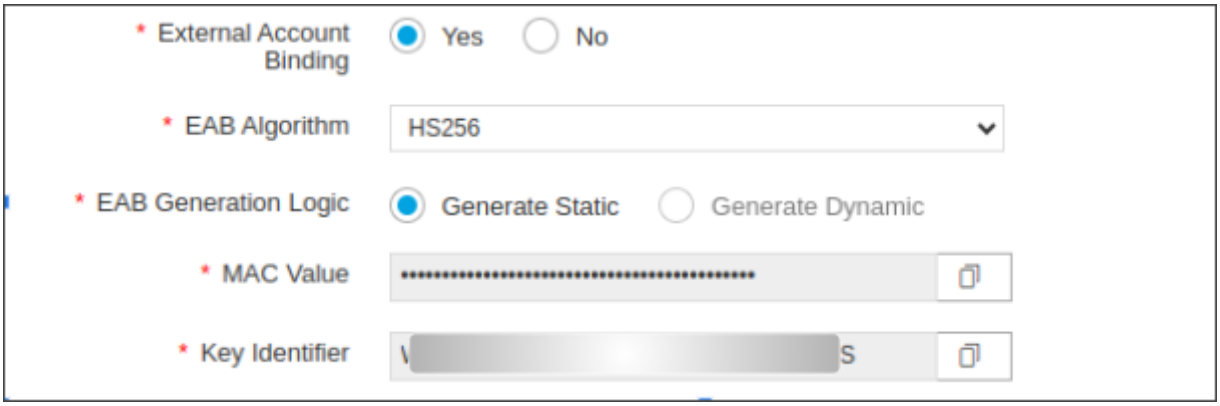
```
Create certificate failed, retry? (y/n*) - yes

This ACME endpoint requires an external account. You will need to provide a
key identifier and a key to proceed. Please refer to the providers
instructions on how to obtain these.

Key identifier: [redacted]

Key (base64url encoded): ****************************************
[testwinacme.appviewx.net] Authorizing...
```

Appviewx ACME configuration:



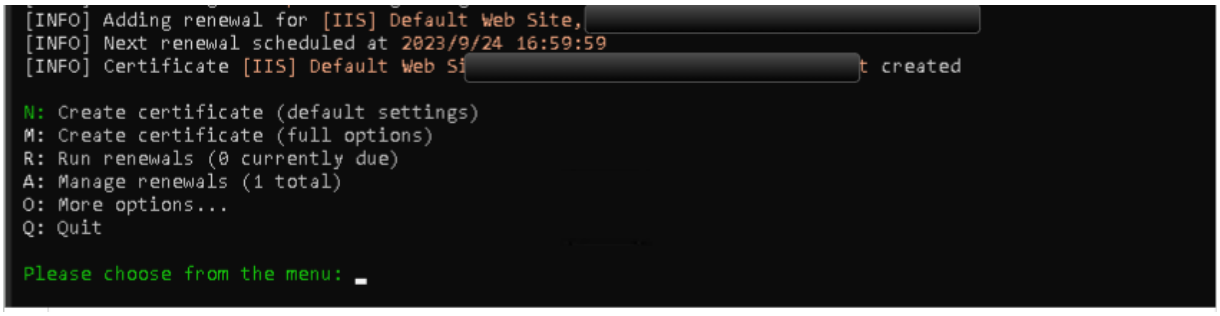
3. A registration is created with the ACME server if no existing one is found. Users will be prompted to agree to its terms of service and to provide an email address that the administrators can use as contact information.

```
[VERB] No account found, creating new one
[VERB] Terms of service downloaded

Enter email(s) for notifications about problems and abuse (comma-separated): <Enter>
```

4. The program negotiates with the ACME server to try and prove the ownership that you want to create the certificate for. By default, the http validation mode is picked, and handled by AppViewX's self-hosting plugin. Getting the validation right is often the trickiest part of getting an ACME certificate. If there are problems, refer to the common issues.
5. After the proof has been provided, the program gets a new certificate from the ACME server and updates or creates IIS bindings as required according to the logic documented here.

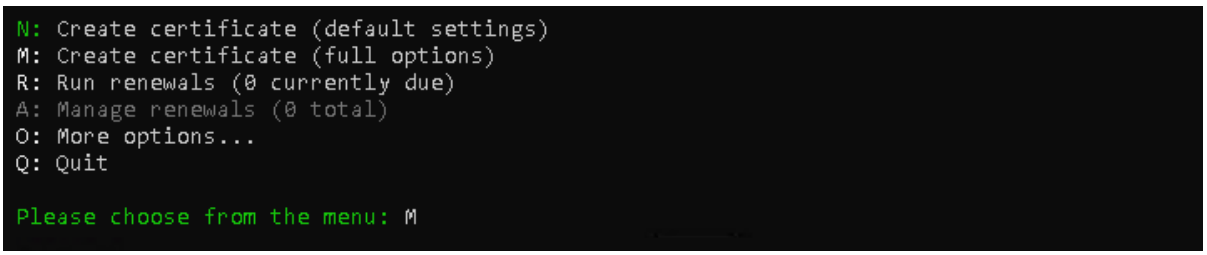
Copyright © 2024 AppViewX, Inc. All Rights Reserved.



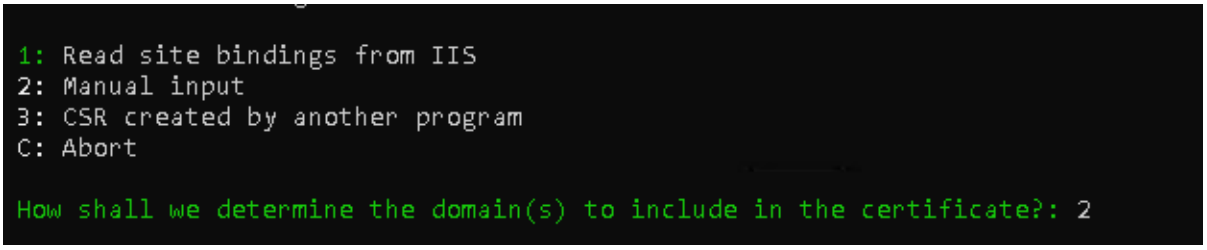
6. The program stores all choices made while creating the certificate and applies them for each subsequent renewal.

Steps for using “M: create certificates with full option”

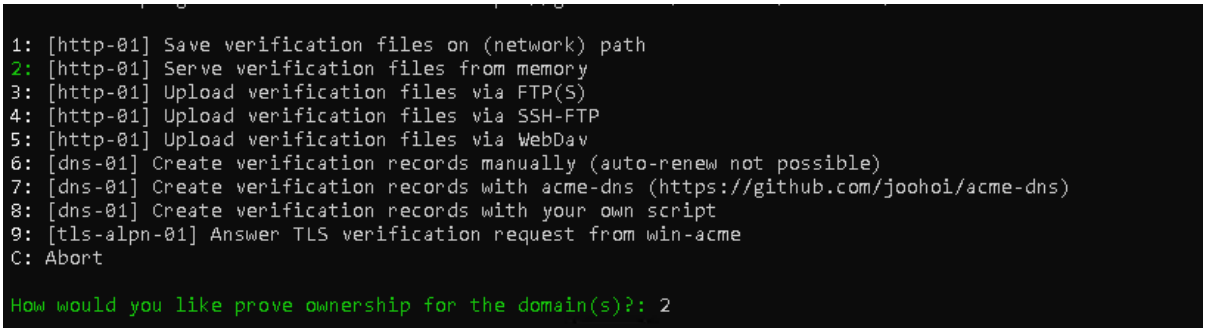
1. Choose ‘M’ to create certificates using full options.



2. Choose 1, to read site bindings from IIS server or else choose 2 to provide the domain name manually.



3. Continue with the default options for validations (The number highlighted in green color).



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

4. Provide the default option 2 to create the private key for the certificate.

```
1: Elliptic Curve key
2: RSA key
C: Abort

What kind of private key should be used for the certificate?: 2
```

5. To store the certificate in windows certificate store, enter 4.

```
1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

How would you like to store the certificate?: 4
```

6. Choose the WebHosting option/ default option to store the certificates in that particular store. (The certificates can be found in the windows machine certificate store → Web Hosting → Certificates)

```
1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 3
```



Note: To store the certificate in the personal store use the option **2 instead of 3.**

7. Enter the default option 5 and continue.

```
1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

Would you like to store it in another way too?: 5
```

8. To create and update the https bindings in IIS server , choose 1.

```
1: Create or update https bindings in IIS
2: Create or update ftps bindings in IIS
3: Start external script or program
4: No (additional) installation steps

Which installation step should run first?: 1
```

9. Enter 4, to add no other installation steps and continue.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
1: Create or update https bindings in IIS
2: Create or update ftps bindings in IIS
3: Start external script or program
4: No (additional) installation steps

Add another installation step?: 4
```

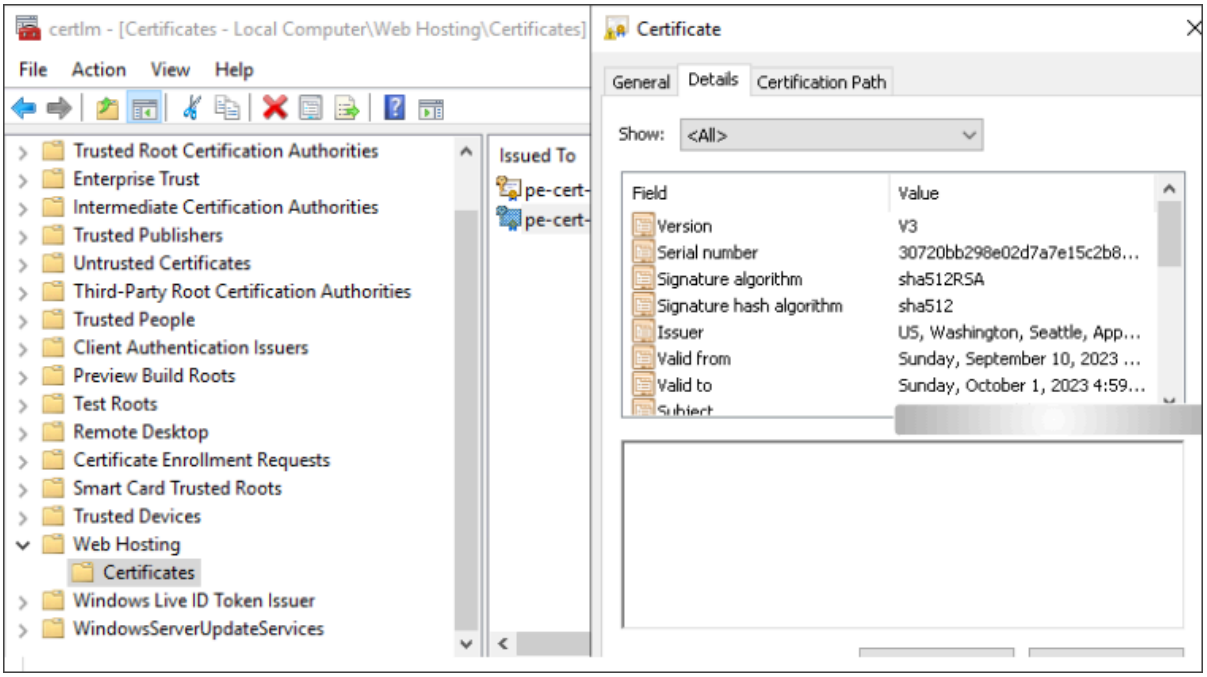
10. Provide an email address (or) press enter to skip.

```
[VERB] No account found, creating new one
[VERB] Terms of service downloaded

Enter email(s) for notifications about problems and abuse (comma-separated): <Enter>

[DBUG] Creating new ES256 signer
[DBUG] Send HEAD request to https://pe-cert-swat-224131.appviewx.net:31443/avxapi/acmeTest/acme/ne
```

11. The certificate will be binded to the chosen IIS server and the certificate will be stored in the windows certificate store.



Winacme Enrollment Process in the Background

Winacme is initiated as a hidden process using a PowerShell script. Thus, when the PowerShell script is executed, the terminal opens in the background and remains invisible to the user.

Steps to run the winacme enrollment process in background:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

1. There are three PowerShell scripts provided from AppViewX. Choose the script as per the requirement and follow the steps below.
   - **Run winacme using manual hostname as input** - The PowerShell script below fetches the certificate for the hostname specified and binds it with the IIS server for the site id specified.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source manual --host <host-name> --emailaddress <email id (or) NA> --installation iis --installationsiteid
 <site id> --verbose --eab-key-identifier <eab-key-identifier> --eab-key <eab-key> --eab-algorithm <eab-algorithm>"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

> **Note:** The command `--eab-key-identifier -O7R97x8T52ASpwAYZJzJ --eab-key _Pqh5h6yJKThrXiqy6GGsfVIZdgNNw --eab-algorithm HS256` is only applicable when EAB is enabled in the server side.

   - **Run using CSR as input for certificate generation** - The PowerShell script belowfetches the certificate using the given csr file and binds the certificate to the specified site id.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source csr --csrfile <Path to the csr file> --pkfile <Path to the key file> --emailaddress <email id (or) NA>
 --installation iis --installationsiteid <site id>  --verbose"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

   - **Run using site id as input for certificate generation** -
     - Multiple site ids can be given in comma separated format in this script.[e.g.: 1,2,3]
     - This PowerShell script fetches the hostnames of the servers mentioned in the <site id> and creates a single certificate.
     - The hostnames of all the specified IIS servers are present in the SAN DNS of that certificate.
     - All the servers mentioned in the <site id> are binded with the same certificate.
     - This is not applicable for IP based binding and only works for hostname based bindings.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source iis --siteid <site id>  --emailaddress <email id (or) NA> --installation iis --verbose"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

> **Note:** The command `--eab-key-identifier -O7zaR976x8T52AGASpwAAAYZJzJ --eab-key _PqhM5h6yJnXKThr7Xiq4y6GGlFsfGVICZdgNNw --eab-algorithm HS256` is only applicable when EAB is enabled in the server side.

Please refer these points to replace placeholder values in the commands:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- `<path to the wacs.exe file>` → wacs.exe file path (Present inside the winacme installation folder)
- `<host-name>` → hostname for which the certificate needs to be acquired.
- `<site id>` →This id can be found in the IIS server manager.
- `<email id (or) NA>` → An email address or NA. (Should not be empty) This is binded to the winacme account.
- `<Path to the csr file>` → Path of the CSR file.
- `<Path to the key file>` → Path of the Key file associated with the given csr.

2. Save the required script in .ps1 format (new ps1 file can be created using windows PowerShell ISE → File → New) and Open PowerShell with **admin** privileges and navigate to the PowerShell script.
3. Run the power shell script `.\<shell script file name>`
4. To ensure that the task is being run in the background. Open the windows task manager and look for the process “wacs”. (This may be found as separate process or under windows PowerShell process)
5. If the manual approval is enabled in the CA policy settings, this process waits for the certificate to be approved. (The client polls the acme server for the certificate according to the “RetryCount” and “RetryInterval” values provided in the settings.json file. [Path - C:\AppViewX_ACME_Winacme_Client\winacme\settings.json].
6. After receiving the certificate, this process is terminated. The certificate is found in the windows certificate store (under the tab Web Hosting/certificates).

Scheduling Tasks for Auto-Renewal

WIN-ACME schedule’s task using the configurations from **settings.json**. Please refer to this section for more details.

> **Attention:** Ensure that you have removed the **".store"** directory within the winacme folder. Neglecting this step might result in the creation of a scheduled task using parameters from the previous **settings.json** configuration, disregarding the recent adjustments.

It is possible to create a renewal task for win-acme in Windows using either a command or an interactive terminal session.

Creating Task Scheduler through Command

1. Open command prompt with admin privilege and run the command

```
wacs.exe --verbose --setuptaskscheduler
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
C:\AppViewX_ACME_Winacme_Client\winacme>wacs.exe --verbose --setuptaskscheduler
[VERB] Verbose mode logging enabled
[VERB] ExePath: C:\AppViewX_ACME_Winacme_Client\winacme\wacs.exe
[VERB] ResourcePath: C:\AppViewX_ACME_Winacme_Client\winacme\
[VERB] PluginPath: C:\AppViewX_ACME_Winacme_Client\winacme
[EROR] This version of the program does not support external plugins, please download the pluggable version.
[VERB] Looking for settings.json in C:\AppViewX_ACME_Winacme_Client\winacme\.store\win-acme
[VERB] Copying settings_default.json to settings.json
```

```
[INFO] Deleting existing task win-acme renew
[INFO] Adding Task Scheduler entry with the following settings
[INFO] - Name win-acme renew
[INFO] - Path C:\AppViewX_ACME_Winacme_Client\winacme
[INFO] - Command wacs.exe --renew --baseuri
[INFO] - Start at 09:00:00
[INFO] - Time limit 02:00:00
[DBUG] Creating task to run with previously chosen credentials
[VERB] Exiting with status code 0
```

2. Ensure that the **"Start at"** time in the end of the log matches with the **"StartBoundary"** time specified in the settings.json file.

Creating Task Scheduler through Interactive Terminal

1. Run the command below and choose option “O” to go into “More Options”

```
wacs.exe --verbose
```

```
N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (6 total)
O: More options...
Q: Quit

Please choose from the menu: O
```

2. Choose option “T”

```
S: Manage secrets
T: (Re)create scheduled task
E: Test email notification
A: ACME account details
I: Import scheduled renewals from WACS/LEWS 1.9.x
M: Encrypt/decrypt configuration
U: Check for updates
Q: Back

Please choose from the menu: T
```

```
[INFO] Deleting existing task win-acme renew (                                avxapiacmeTestacmedirectory) from Windows Task Scheduler
[INFO] Adding Task Scheduler entry with the following settings
[INFO] - Name win-acme renew (                                avxapiacmeTestacmedirectory)
[INFO] - Path C:\Winacme\AppViewX_ACME_Winacme_Client_2020.3.0_FP8\winacme
[INFO] - Command wacs.exe --renew --baseuri "https://                                avxapi/acmeTest/acme/directory"
[INFO] - Start at 19:15:00
[INFO] - Time limit 02:00:00
```

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Ensure that the **"Start at"** time aligns with the **"StartBoundary"** time specified in the settings.json file.

3. Type **'n'**.

```
Do you want to specify the user the task will run as? (y/n*) - no

[DBUG] Creating task to run with previously chosen credentials
```

This sets up a scheduled task in the Windows Task Scheduler for the renewal of winacme, using the parameters specified in the settings.json file.

You can cross verify by refreshing the "Task Scheduler Library" to find the **"win-acme renew"** task. And check if the **"Next Run Time"** of this task matches to the defined **"StartBoundary"** time.

Points to Remember

- Whenever the scheduled **"win-acme renew"** task is triggered, the newly generated certificates from the renewal process will take the place of the older certificates in the **"Certificates - LocalComputer\Web Hosting\Certificates"** section present within the **"Manage computer certificates"** console.
- Certificates that have a remaining validity period that is equal to or greater than the specified **"RenewalMinimumValidDays"** will not be subjected to renewal and will remain unaltered in the certificates console.
- After scheduling a winacme renewal task using the specified settings.json, the task will continue to operate with those configurations until a new winacme renewal task is generated with altered settings.
- Later on, if you want to (re) create a scheduled task for winacme renewal, simply go through the steps **"a"** and **"b"** as described earlier. This will overwrite any existing winacme renewal task in the task scheduler, if there is one.
- Other properties of the scheduled task like **"RenewalDays"**, **"ExecutionTimeLimit"** can also be changed in a similar manner. Some of these parameters can be changed from the Task Scheduler itself, as long as the name is not modified.

Revoking Certificates

Revoking a certificate should only be done when the private key is believed to have been compromised, not when simply replacing or canceling it. Revocation can be done from the main menu with **Manage renewals > Revoke certificate**.

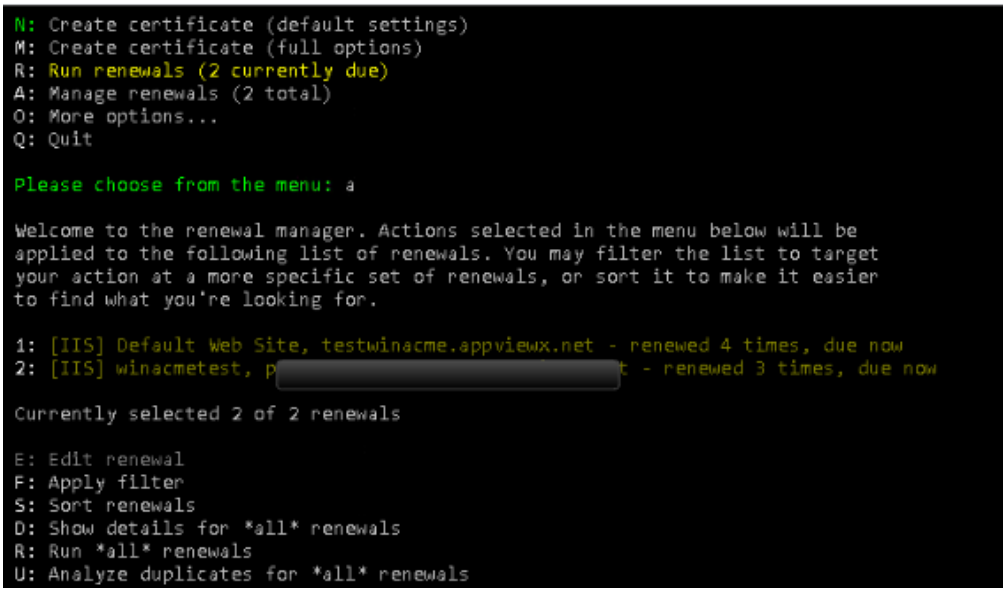
To revoke a certificate in winacme

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

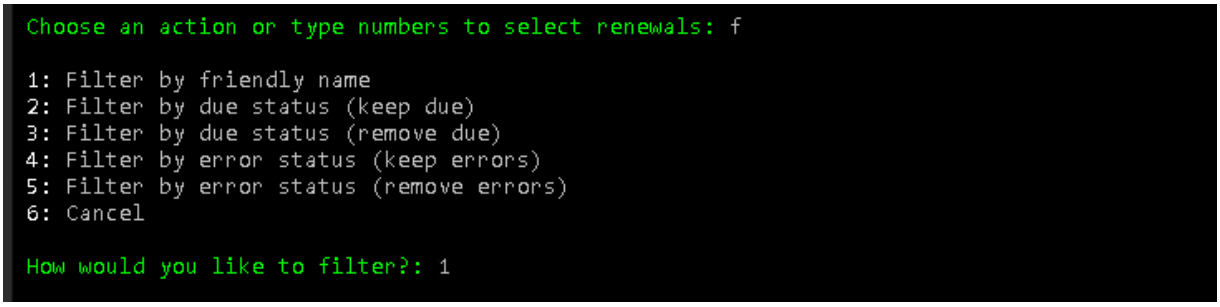
1. Run the command

```
wacs.exe
```

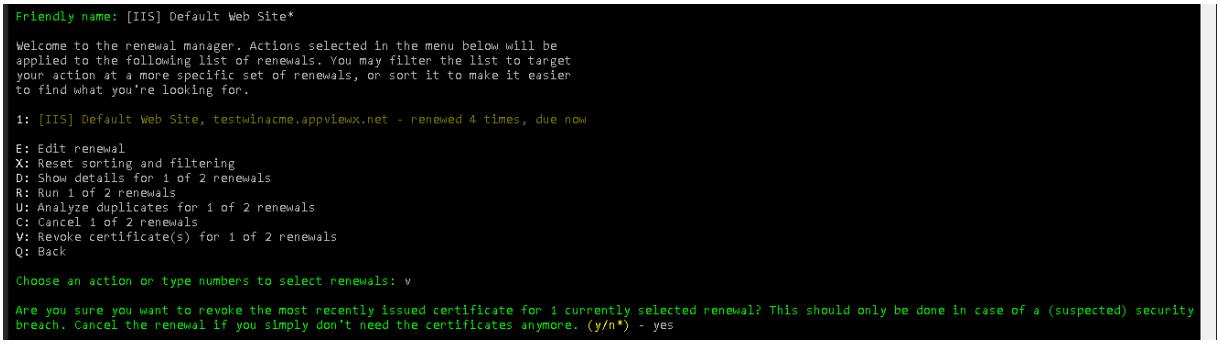
2. Press ‘A’ to list the certificates, these names can be used to revoke a particular certificate.



3. Enter ’V’ to revoke all certificates, If one particular certificate is to be revoked, Use ‘F’ option to apply filter.



4. If ‘F’ is chosen, this menu will be prompted. Enter ‘1’ to filter by friendly name.

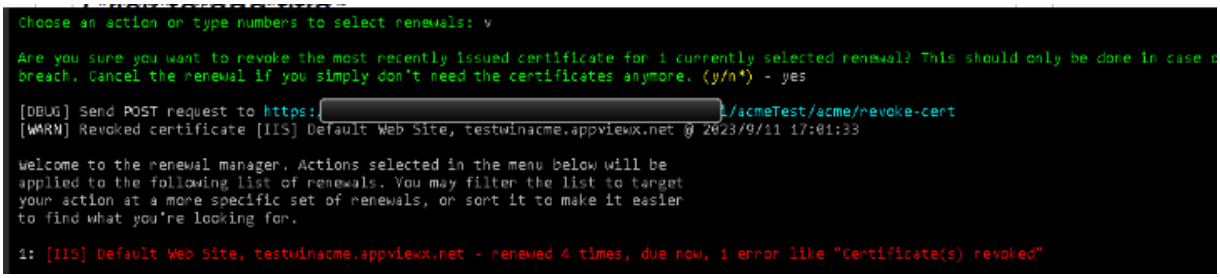


5. Enter the friendly name as shown below. (Friendly names are displayed in the step 1)

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Option	Description
Example 1	If the name displayed in the menu is `[IIS] winacme-test, pe-cert-swat-142107.appviewx.net` then enter the following in the friendly name filter → `[IIS] winacmetest*`
Example 2	If the name displayed in the menu is `[IIS] Default Web Site, testwinacme.appviewx.net` then enter the following in the friendly name filter - `[IIS] Default Web Site*`

6. Verify if the intended certificate is filtered.
7. Enter ‘V’ to revoke the selected certificate and type ‘yes’ for the revoke prompt as shown in the figure.



Health Checks

The health of the scheduled task is checked each time the program is run manually. It can also be (re)created from the menu (More options → (Re)create scheduled tasks).

Monitoring

The renewal process can be monitored from the Windows Event Viewer and log files written to `%programdata%\win-acme\$baseuri$\Log`.

Testing and Troubleshooting

To test or troubleshoot the renewal process, renewals can be triggered manually from the menu. When listing the details for renewal, the program displays any errors that have been recorded during the previous runs.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
1	It was not possible to find any compatible framework version The specified framework 'Microsoft.NETCore.App', version '5.0' was not found. - The following frameworks were found: 6.0.21 at [C:\Program Files\dotnet\shared\Microsoft.NETCore.App] 6.0.21 at [C:\Program Files\dotnet\shared\Microsoft.NETCore.App] You can resolve the problem by installing the specified framework and/or SDK. The .NET Core frameworks can be found at: - https://aka.ms/dotnet-download	The .net version of winacme is not compatible with the .net version found in the windows machine	Refer this section for possible solutions.
2	Unable to connect to ACME server System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.Http.WinHttpException (80072EE7, 12007): Error 12007 calling WINHTTP_CALLBACK_STATUS_REQUEST_ERROR, 'The server name or address could not be resolved'.	The default base uri name is not configured in the settings.json / the configured url or the port is wrong.	Configure the correct url in the default base uri section in settings.json file.
3	Failed to create order: Unable to fetch acme server url. - Agent Settings name given is invalid	The Agent name provided in the URL is incorrect / Agent setting is not configured in the ACME server side configuration.	Configure the correct url in the default base uri section in settings.json file.

Support for Other .NET Version

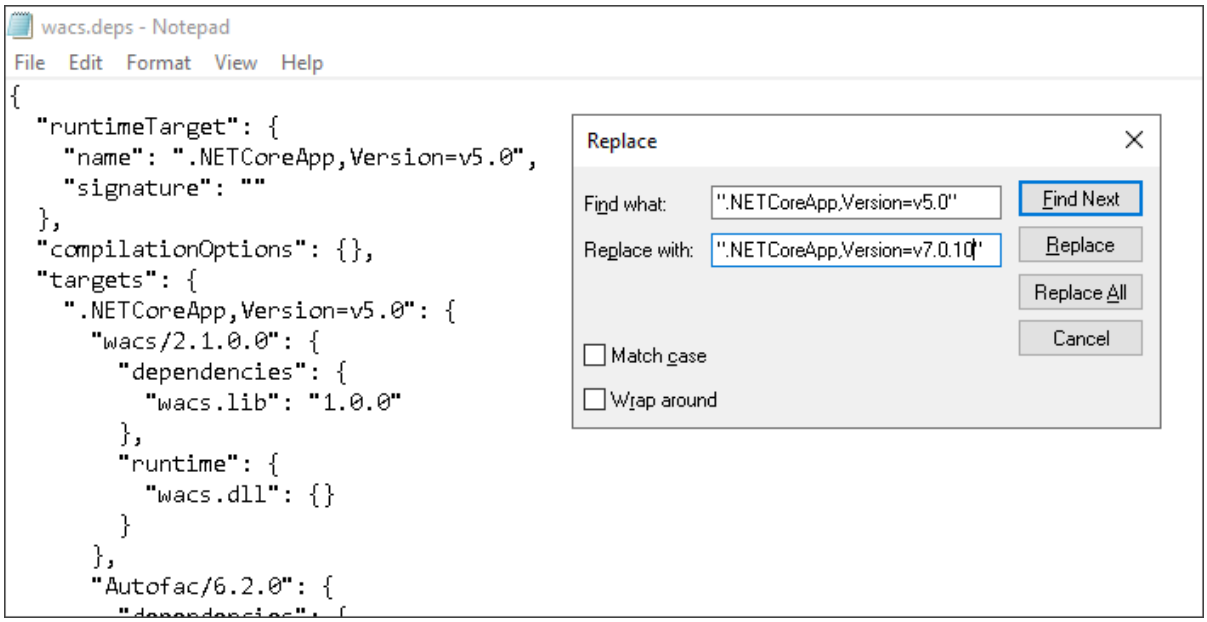
The default version of .NET that winacme supports is .NET v5. For newer .NET versions, the configurations in `wacs.dep` and `wacs.runtimeconfig` need to be changed. These files are found in the WIN-ACME folder. Follow the steps to do the same:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Changes in the "wacs.dep" file

- Use *CTRL+H* to open the *find and replace* menu to replace the strings `.NETCoreApp,Version=v5.0` with `".NETCoreApp,Version=v<version of .NET in the pc>"`
- The above string needs to be replaced at all occurrences in the file, to do so, use the **Replace All** option.
- Use the complete version number when replacing, such as 7.0.10

  Example: `".NETCoreApp,Version=v5.0"` is replaced with `".NETCoreApp,Version=v7.0.10"`



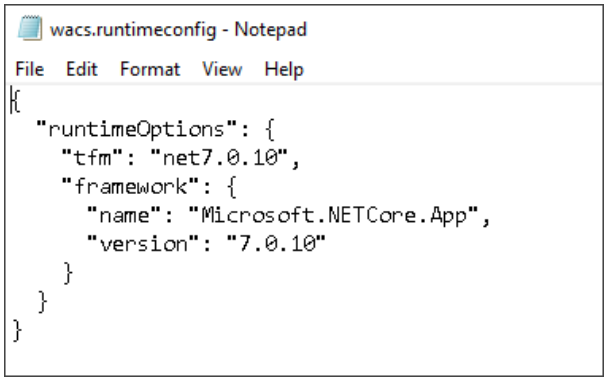
- Similarly replace (replace all) the string `"Microsoft.NETCore.Platforms": "5.0.0"` with `"Microsoft.NETCore.Platforms": "<version of .NET in the pc>"`.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Changes in the "wacs.runtimeconfig" file

- Replace (use replace all) the string `"tfm": "net5.0"` with `"tfm": "net<version of .NET in the pc>"`
- Also replace `"version": "5.0.0"` with `"version": "<version of .NET in the pc>"` as shown in the figure below.



Posh-ACME Configuration Guide

This guide gives an overview on how Posh-ACME clients works with AppViewX via ACME protocol to request for certificates from supported CAs.

- ACME Protocol
- Posh-ACME
- Installing Posh-ACME and its Dependencies
- Executing Posh-ACME
- Executing Posh-ACME with Enhanced Data
- Troubleshooting Client-Side Errors
- Glossary

ACME Protocol

ACME, or *Automated Certificate Management Environment*, is a communications protocol that leverages an agent to automate the process of CSR generation and certificate/key rotation. It is primarily used by the popular public CA, Let's Encrypt, as a part of their business model of issuing 90-day Domain Validated certificates (as Organizational Validation and Extended Validation certificates require human supervision to issue, thus rendering the point of ACME moot), and automating their renewals.

The protocol was initially developed by the Internet Security Research Group (ISRG) for the Let's Encrypt CA, and, as an open-source tool, free to use. While originally only used by Let's Encrypt to issue x.509

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

(SSL/TLS) certificates, various other CAs, PKI vendors, and browsers are now beginning to support ACME to work with other kinds of certificates (S/MIME, Code-signing) as well. However, to leverage them, the CA should be able to access the DNS/HTTPS token that is published. This makes it better suited to be an internal PKI issuance method.

Posh-ACME

Posh-ACME is a PowerShell module designed to facilitate the management of digital certificates, specifically in the context of the Automated Certificate Management Environment (ACME) protocol. ACME is commonly used for obtaining and renewing SSL/TLS certificates automatically. This module empowers administrators and developers to handle various aspects of certificates, including certificate creation, renewal, revocation, and installation, all within a familiar and script-able PowerShell environment.

With Posh-ACME, you can interact with various certificate authorities, manage DNS records for domain validation, and automate the entire certificate lifecycle. This tool is particularly valuable for web administrators, DevOps teams, and anyone who needs to secure their applications and services with SSL/TLS encryption. Posh-ACME streamlines the certificate management process, making it easier to ensure the security and privacy of web applications and websites. Whether you need to secure a single website or manage certificates for a large-scale infrastructure, Posh-ACME offers a user-friendly and flexible solution for handling your certificate needs with ease and efficiency.

Note: The inherent challenges of using native Posh-ACME includes the absence of support for custom attributes and the requirement for manual installation of PowerShell (for Linux), Posh-ACME, and its dependencies.

- AppViewX Posh-ACME
- Benefits of Posh-ACME
- Downloading Posh-ACME Client
- Prerequisite for Running Clients
- Providing Sudo Permissions in Linux

AppViewX Posh-ACME

AppViewX customizes Posh-ACME to provide extended functionality to customers over the existing Posh-ACME client which helps to meet various business and operational needs. The enhanced features include:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- Single click installation and interactive digital certificate CLM operations. The **Supported OS** flavors are
  - Windows Server 2019
  - Linux (Ubuntu 20, RHEL 8)
- Support for the inclusion of multiple attributes in Posh-ACME command for enrollment and renewal. These attributes can be included in the payload sent to the server when enrolling or renewing certificates.
- Simplifies the installation process by bundling PowerShell, Posh-ACME, and their associated dependencies into a single package. This eliminates the need for separate installations of these components, streamlining the setup.
- The ability to configure polling behavior when approval is necessary for enrolling or renewing a certificate which allows for more flexible and customized approval workflows.
- Facilitates the automation of certificate renewal on a daily basis. Certificates that are due for renewal are automatically processed, reducing manual intervention and ensuring certificates remain up-to-date.
- Addition of CA Certificate in native trust store for the ACME client to work with any CA issued SSL Server certificate.

Benefits of Posh-ACME

AppViewX provided Posh-ACME checks the system environment for various paths such as

- **Powershell installation** for Linux.
- **Required dependencies** for Posh-ACME.

If any of the above packages are not installed or configured in your system, AppViewX will do it for you without any human intervention.

Downloading Posh-ACME Client

The Posh-ACME client is now available in the release portal - https://release.appviewx.com/downLoadArtifact?id=1199

Prerequisite for Running Clients

- The AppViewX server needs to have a valid certificate installed on its gateway.
- System Requirements

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

  - Environment Details - Linux or Windows.
  - Operating System : As mentioned earlier in the AppViewX Posh-ACME section, the supported Linux OS flavors are Supported Linux OS.
  - For IIS Server Binding - Windows PowerShell 5.1 or later (Desktop edition) with .NET Framework 4.7.1 or later.
- Root user permissions for setup process in Linux.
- Admin privileges are required during setup and runtime in Windows.
- A proper DNS entry for the services in the DNS server.
- A valid ACME endpoint should be configured on the AppViewX GUI.
- To enable client connections, it is essential to have ports 31443 open for on-premise deployment and 30020 in cloud connectors open for SaaS deployment in AppViewX.
- If the DNS validation is for HTTP challenge, it's essential to have port 80 accessible on the client machine to allow AppViewX to establish a connection.
- If the DNS validation is for DNS challenge, the DNS server should be up and running and the DNS credentials file should be correctly configured.
- Certificate attributes and custom attributes should be configured to capture the attributes in the AppViewX GUI (if required).

Providing Sudo Permissions in Linux

1. To provide access to port 80 for a non-root user

   a. Ensure that you are currently located within the POSHACME_AVX directory.

   b. Execute the command below to grant the **pwsh** executable the capability to bind to port 80 without requiring root privileges.

   ```
   sudo setcap 'cap_net_bind_service=+ep' pwsh
   ```

   This step is essential to facilitate the http-01 challenge.

2. To add custom CA certificates to TrustStore

   a. Determine the appropriate trust store on your Linux system. Common locations for trust stores are /etc/ssl/certs/ca-certificates.crt and /etc/ssl/certs/ca-bundle.crt.

   b. Obtain the **acmetrustchain.crt** file from the **POSHACME_AVX** directory and place it in the trust-store of the machine.

   c. Log in as the root user. Use the command below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
sudo -i
```

d. Copy the entire contents of the certificate chain file **acmetrustchain.crt** and append them to the end of the trust store file using the `cat` command below.

```
cat acmetrustchain.crt >> /etc/ssl/certs/ca-bundle.crt
```

e. After execution, exit from the sudo user session.

Installing Posh-ACME and its Dependencies

Instructions for Administrators

1. Download the latest version of Posh-ACME client from the AppViewX release portal.
2. Open your terminal/command prompt and navigate into the directory where the downloaded Posh-ACME ZIP file is present.
3. Unzip the downloaded Posh-ACME client **AppViewX_ACME_PoshACME_Client.zip** to the current directory using the command below.

   For Linux:

   ```
   unzip AppViewX_ACME_PoshACME_Client.zip
   ```

   For Windows:

   ```
   tar -xf AppViewX_ACME_PoshACME_Client.zip
   ```

4. Navigate into the extracted folder named **POSHACME_AVX** using the command below.

   ```
   cd POSHACME_AVX
   ```

5. Obtain server trust chain certificates - If the server certificate is created in AppViewX, download it from the **AppViewX inventory**, else download the **certificate chain files** (.pem or .crt) for the Certificate Authority (CA). This chain of files should include the root certificate as well as any intermediate certificates of the server.

   Linux users - If there are individual certificates for root CA and intermediate CA's, combine these certificate files into a single file. This can be done either through a text editor or by using the 'cat' command:

   ```
   cat intermediateca.crt rootca.crt > acmetrustchain.crt
   ```

   In this case, **acmetrustchain.crt** represents the name of the server trust chain certificate file. Now place this server trust chain certificate within the POSHACME_AVX directory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Windows users - If there are individual certificates for root CA and intermediate CA, place the root CA certificates and intermediate CA certificates in the POSHACME_AVX directory under the folders **RootCA** and **IntermediateCA** respectively.

6. Navigate out of the POSHACME_AVX directory by using the command below.

```
cd ..
```

7. Create a new zip archive named **AppViewX_ACME_PoshACME_Client.zip** for the POSHACME_AVX directory with the command below:

   For Linux:

```
zip -r AppViewX_ACME_PoshACME_Client.zip POSHACME_AVX
```

   For Windows:

```
tar -a -c -f AppViewX_ACME_PoshACME_Client.zip POSHACME_AVX
```

   The resulting zipped folder can be shared among the users.

Instructions for Linux Users Launching Posh-ACME

1. Download the latest version of Posh-ACME client received from the Administrator.
2. Open your terminal/command prompt and navigate into the directory where you downloaded the Posh-ACME ZIP file.
3. Unzip the downloaded Certbot client **AppViewX_ACME_PoshACME_Client.zip** using the command below.

```
unzip AppViewX_ACME_PoshACME_Client.zip
```

4. Navigate into the extracted folder named POSHACME_AVX using the command below.

```
cd POSHACME_AVX
```

5. Ensure the following permissions have been granted.
   - Port 80 access to a non-root user for HTTP challenge.
   - Presence of server trust chain certificates in the system trust store for SSL verification.



Note: Refer to the section Providing Sudo Permissions in Linux for more details

6. Run the install command below.

```
./install.sh
```

   Executing this command relocates the **Powershell** folder from the current directory to the current user's local/share/ directory.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. Before performing CLM Actions, run the command below.

```
./pwsh
```

   This command initiates the PowerShell environment. Also, ensure that you are in the POSHACME_AVX directory.

Instructions for Windows Users Launching Posh-ACME

1. Download the latest version of Posh-ACME client received from the Administrator.
2. Open your command prompt as an administrator and navigate into the directory where you downloaded the Posh-ACME ZIP file.
3. Unzip the downloaded Posh-ACME client **AppViewX_ACME_PoshACME_Client.zip** using the command.

```
tar -xf AppViewX_ACME_PoshACME_Client.zip
```

4. Navigate into the extracted folder named **POSHACME_AVX** using the command below.

```
cd POSHACME_AVX
```

5. Ensure to add custom CA certificates to the TrustStore.
   In Windows, you can add the root CA and intermediate CA certificates located within the **RootCA** and **Intermediate CA** directories found in the **POSHACME_AVX** directory to the *Trusted Root Certification Authorities* and *Intermediate Certification Authorities* stores, respectively. Access to these stores can be achieved through the **Manage Computer Certificates** control panel.
6. Run the install command below.

```
install.bat
```

   Executing this command relocates the **Posh-ACME** folder and **Posh-ACME.Deploy** folder from the current directory to the C:\Program Files\WindowsPowerShell\Modules\ directory.

7. Before performing CLM Actions, initiate Windows PowerShell environment as an administrator and ensure you are in the POSHACME_AVX directory.

Executing Posh-ACME

- Enrolling Certificates
- Revoking Certificates
- Renewing Certificates

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Enrolling Certificates

Prerequisites

1. Before you begin enrollment of certificates ensure to run the following command to import Posh-ACME:

   ```
   Import-Module Posh-ACME -Force
   ```

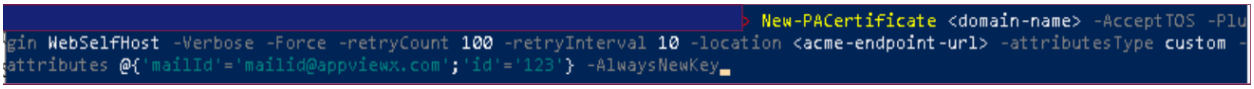
2. Open PowerShell with admin privileges.
3. Ensure that you are in the POSHACME_AVX directory before you run the http-01 and dns-01based challenge validation commands (described below) to enroll a certificate.

http-01 Based Challenge Validation

The command for an http-01 based challenge validation is as follows:

```
New-PACertificate <Domain_Name> -AcceptTOS -Plugin WebSelfHost -Verbose -Force -retryCount <retryCount> -retryInterval <retryInterval> -location <ACME server endpoint URL> -attributes <Attributes> -attributesType <AttributesType> -AlwaysNewKey
```

A sample certificate enrollment command for HTTP validation is shown below.

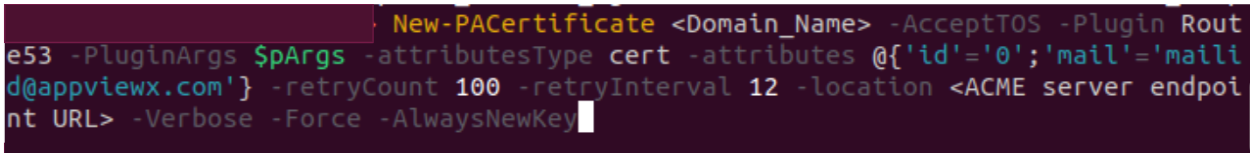


dns-01 Based Challenge Validation

The command for an dns-01 based challenge validation is as follows:

```
New-PACertificate <Domain_Name> -AcceptTOS  -Contact <mail.id> -Plugin Route53 -PluginArgs $pArgs -verbose -retryCount <retryCount> -retryInterval <retryInterval> -location <ACME server endpoint URL> -attributes <Attributes> -attributesType <AttributesType> -AlwaysNewKey -Force
```

A sample certificate enrollment command for DNS validation using route53 is shown below, similarly other DNS plugins can be used.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameter Description

Parameters used in the http-01 and dns-01 based challenge validation

Parameter	Mandatory	Description
<ACME server endpoint URL>	Yes	Input the appropriate ACME endpoint, configured on the AppViewX GUI.
<Domain_Name>	Yes	Enter a valid domain name for which the certificate needs to be enrolled. • Provide a **single domain name** to acquire a certificate for a particular domain. The domain name would be the name of the order. Sample input for single domain name - *test1.appviewx.com* • Provide comma separated **multiple domain names** to acquire a certificate for all the given domains. The first domain name would be the name of the order and is considered as the **main domain**, while the remaining domains would be reflected in the Subject Alternative Names (SAN) of the certificate. Sample input for multiple domain names - *test2.appviewx.com,test3.appviewx.com*
-attributes <Attributes> and **-attributesType <AttributesType>**	No	Posh-ACME can be run with **attributes**. These parameters allows users to provide multiple attributes. These attributes can include multiple name-value pairs, which are then included in the "Finalize Order" call along with the CSR. The values for these fields will be provided as a JSON name/value pair, which we can retrieve and map to the attributes in our application. This mapping will enable us to include the attribute information in the certificate request for reporting purposes. For more information on the usage of attributes in Posh-ACME refer to Defining Custom and Certificate Attributes.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	No	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Parameters used in the http-01 and dns-01 based challenge validation (continued)

Parameter	Mandatory	Description
		For more information on polling in Posh-ACME, refer to Polling during Enrollment/Renewal.

For more information on the keywords used in the Posh-ACME commands refer to the Keywords in Posh-ACME commands.

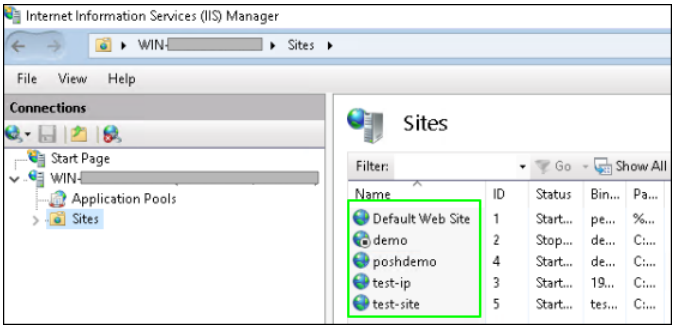
- Binding Certificate to IIS Server in Windows
- Working Behavior Of Enrollment

Binding Certificate to IIS Server in Windows

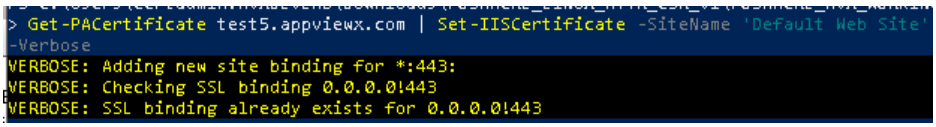
Posh-ACME supports issuance of certificates on their local IIS instance. To bind the certificate generated to local IIS instance, run the command below.

```
Get-PACertificate <Main_Domain_Name> | Set-IISCertificate -SiteName '<Site_Name>' -Verbose
```

Parameters used in the http-01 and dns-01 based challenge validation

Parameter	Mandatory	Description
<Main_Domain_Name>	Yes	Enter a valid 'main domain' name of the certificate to be bound.
<Site_Name>	Yes	Enter a valid IIS site name as shown below. 

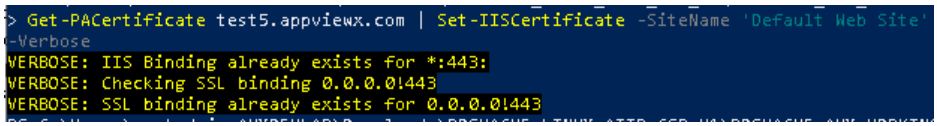
A sample command to bind a certificate to the IIS server is shown below.



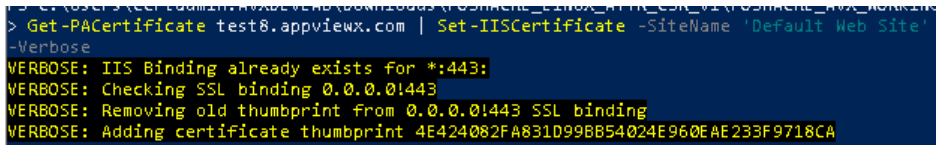
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

The certificate binding process only checks for the existence of an associated site binding.

- If a binding with the same domain name already exists, it will skip the binding process.



- However, if no such binding is found, it will proceed to bind the new certificate.



For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

Working Behavior Of Enrollment

Assuming there are multiple agents configured to the same server with distinct Endpoint URLs. An example of the Agent X's Endpoint URL is `https://<server_hostname>:31443/avxapi/<acme_agent_x>/acme/directory`. Several scenarios can occur when enrolling a certificate for a domain name using ACME Agent X's Endpoint URL as described below

Scenario 1: No Previous Order Exists

If the domain-associated older order doesn't exist, indicating that certificate enrollment for that domain has never been triggered:

- **Successful enrollment**: In the case of a successful enrollment, an order is created for that domain using Agent X's Endpoint URL, and the certificate is successfully generated.
- **Interrupted/Failed enrollment**: If the enrollment process was interrupted or failed, an order may or may not be created for that domain using Agent X's Endpoint URL, and the certificate is not generated.

Scenario 2: Previous Order Exists

If the domain-associated older order exists, indicating that certificate enrollment for that domain was initiated earlier, this could be due to a previously successful enrollment or a previously interrupted enrollment call.

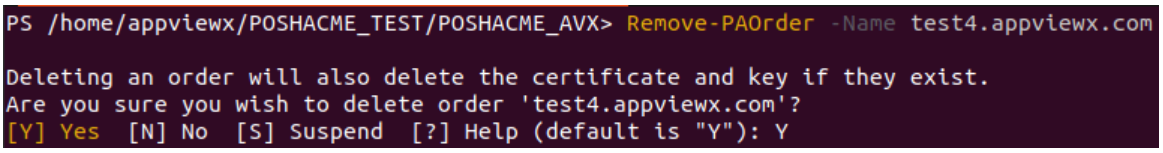
Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- **Successful enrollment**: In the case of a successful enrollment, the domain-associated older order is used which was configured with a different Agent's Endpoint URL even though if it is tried with Agent X's Endpoint URL, to create a new certificate. The domain-associated older order remains in place, the older certificate cannot be used and it will be backed up as a **.bak** file and a new certificate is created.
- **Interrupted/Failed enrollment**: If the enrollment process was interrupted or failed, the domain-associated older order remains in place, the older certificate if present cannot be used and it will be backed up as a **.bak** file and a new certificate is not created.

To address situations where the domain-associated older order's Endpoint URL is being used instead of creating a new order with Agent X's Endpoint URL, a proposed solution is as follows:

1. Remove the domain-associated older order and associated certificate-related files. This deletion action allows for a fresh certificate issuance process using ACME Agent X's Endpoint URL.
2. To delete the domain-associated older order, use the following command in the PowerShell environment:

```
Remove PA-Order -Name <Domain_Name>
```

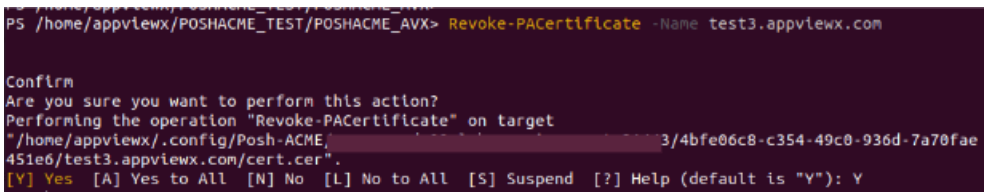


Revoking Certificates

Certificates can be revoked either by providing the certificate **main domain** name or the **certificate file path**.

1. Open PowerShell with admin privileges.
2. Ensure that you are in the POSHACME_AVX directory before you run any commands to revoke certificates.
3. To revoke certificates
   - By specifying the **main domain** name.

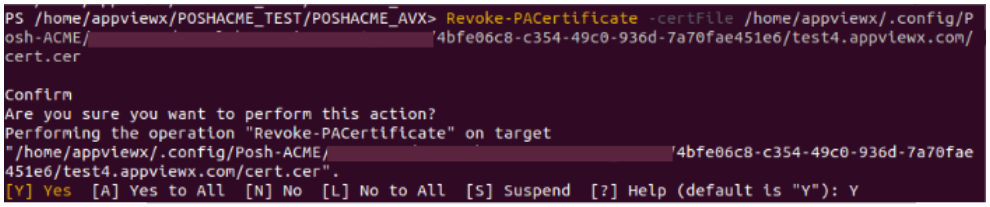
```
Revoke-PACertificate -Name <Main_Domain_Name>
```



Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- By specifying the **certificate file path**.

```
Revoke-PACertificate -certFile <certFilePath>
```



> **Tip:** To skip the revocation confirmation prompt, use the flag **-Force** along with the command.

Using the Revoke-PACertificate command does not automatically delete the order associated with the revoked certificate. Consequently, Posh-ACME makes renewal attempts for revoked certificates during the next scheduled renewal process. To avoid this, it is necessary to manually delete that specific domain-associated order.

For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

- Working Behaviour of Renewal

Working Behaviour of Renewal

- **Successful Renewal:** When the renewal of a domain certificate is successfully completed, the older certificate cannot be used and is backed up as a **.bak** file and is then replaced with the newly generated certificate. This ensures that a copy of the older certificate is preserved while the updated certificate takes its place.
- **Interrupted Renewal:** If the renewal process is prematurely interrupted, the older certificates may not be successfully renewed. In such cases, the older certificates become unusable, and they are backed up as a consequence of the interrupted renewal process.

Renewing Certificates

Certificates generated by POSH-ACME are renewed selectively based on necessity. The system assesses the validity of all the certificates to identify those requiring renewal. This depends on the threshold specified during the execution of the **renewal.ps1** script using the **renewalDaysThreshold**

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

parameter. Certificates with a remaining validity period (measured in days) less than the specified threshold will only be considered for renewal.

To renew certificates,

1. Open PowerShell with admin privilege.
2. Ensure that you are in the 'POSHACME_AVX' directory before you run any commands to renew certificates.
3. Run the below command.

```
./renewal.ps1 -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold>
```

```
PS /home/appviewx/POSHACME_TEST/POSHACME_AVX> ./renewal.ps1 -retryCount 5 -retryIn
terval 4 -renewalDaysThreshold 20
```

The above command implies that certificates with a validity of less than 20 days will be considered for renewal.

Parameters used in the renew command

Parameter	Mandatory	Description
-retryCount <retryCount> and **-retryInterval <retryInterval>**	No	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, refer to Polling during Enrollment/Renewal.
<renewalDaysThreshold>	No	Specify the threshold number of days. The default value is set to 30.

Note: When there is an incomplete renewal, the old certificate which is being renewed will be deleted from the client's machine.

For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

Scheduling Tasks For Automated Certificate Renewal in Linux

A single scheduled task runs every day at a specified time and checks the validity of all the certificates to determine if any of them should be renewed based on the threshold **renewalDaysThreshold** specified.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

To automate renewal for Posh-ACME through cron job, exit PowerShell environment and run the command below in the terminal.

```
(crontab -l ; echo "MM HH * * * <path to renewal.sh file> -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold>
 -poshACMEDirectoryPath <poshACMEDirectoryPath> >> <path_to_renewal_log_file> 2>&1") | crontab -
```

Parameters used in the schedule task renew command (Linux)

Commands	Description
MM HH	Specify time for renewal in **HH** (hours), **MM** (minutes).
<path to renewal.sh file>	Specify the path to the renewal.sh file which is present in the POSHACME_AVX directory.
<poshACMEDirectoryPath>	Specify the path to the folder 'POSHACME_AVX
<path_to_renewal_log_file>	Specify the path to a text file where automated renewal activities will be logged. This file can be used to track renewal processes.
<renewalDaysThreshold>	Specify the threshold days renewal. The default value is set to 30.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, refer to Polling during Enrollment/Renewal.

Example:

```
[appviewx@i POSHACME_AVX]$ crontab -l
[appviewx@i POSHACME_AVX]$ (crontab -l ; echo "30 14 * * * /home/appviewx/nov_22
/posh/POSHACME_AVX/renewal.sh -retryCount 100 -retryInterval 10 -renewalDaysThre
shold 6000 -poshACMEDirectoryPath /home/appviewx/nov_22/posh/POSHACME_AVX/ >> /h
ome/appviewx/nov_22/posh/POSHACME_AVX/re.log 2>&1") | crontab -
[appviewx@i POSHACME_AVX]$ crontab -l
30 14 * * * /home/appviewx/nov_22/posh/POSHACME_AVX/renewal.sh -retryCount 100 -
retryInterval 10 -renewalDaysThreshold 6000 -poshACMEDirectoryPath /home/appview
x/nov_22/posh/POSHACME_AVX/ >> /home/appviewx/nov_22/posh/POSHACME_AVX/re.log 2>
&1
```

In the above example, the scheduled renewal task is triggered at 01:07 pm daily. Certificates that have less than 100 days of remaining validity will qualify for renewal.

Note: Refer to the **renewalLogs.log** file located in the POSHACME_AVX directory for logs of the scheduled certificate renewal process

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Some helpful commands to use for the renewal process.

Parameters used in the schedule task renew command (Linux)

Command	Description
date	Cron jobs operate according to the server's predefined timezone, typically set to UTC by default. You can verify this timezone by running the ***date*** command in the terminal. Scheduled tasks will commence in accordance with the cron system's understanding of time and time zones.
crontab -e	If you need to modify the time for a cron job that you've previously set up, you can adjust it by editing the time in the crontab file.
crontab -l	Used to check the scheduled cron jobs.

For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

Scheduling Tasks For Automated Certificate Renewal in Windows

A single scheduled task runs every day at a specified time and checks the validity of all the certificates to determine if any of them should be renewed based on the threshold **renewalDaysThreshold** specified.

To automate renewal for Posh-ACME through a scheduled task, open PowerShell with admin privilege, ensure that you are in the POSHACME_AVX directory and run the command below in the command prompt.

```
.\renewal_schedule_windows.ps1 -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold> -time HH:MM
```

Parameters used in the schedule task renew command (Windows)

Commands	Description
HH:MM	Specify time for renewal in **HH** (hours), **MM** (minutes).
<renewalDaysThreshold>	Specify the threshold days renewal. The default value is set to 30.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, refer to Polling during Enrollment/Renewal.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Example:

```
> .\renewal_schedule_windows.ps1 -retryCount 5 -retryInterval 2 -renewalDaysThres
hold 40 -time 14:30

Scheduled task named 'Posh-ACME Renewal' has been successfully created. It will r
un daily at 14:30 with a renewal days threshold of 40.
```

As per the above command, the scheduled renewal task is triggered at 02:30 pm on a daily basis. Certificates that have less than 40 days of remaining validity will be subject to renewal.

For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

Executing Posh-ACME with Enhanced Data

- Accessing Orders and Certificates
- Defining Custom and Certificate Attributes
- Polling during Enrollment/Renewal
- Providing CSR and EAB Fields

Accessing Orders and Certificates

The following set of commands are used for accessing orders and certificates:

- To return details such as domains, key length, expiration, and status for one or more ACME orders previously created, execute the command below.

```
Get-PAOrder -List
```

```
PS /home/appviewx/POSHACME_TEST/POSHACME_AVX> Get-PAOrder -List

Name               MainDomain         status KeyLength SANs CertExpires           Plugin
----               ----------         ------ --------- ---- -----------           ------
test2.appviewx.com test2.appviewx.com valid  2048      {}   01/12/2023 5:29:59 AM {WebSelfHost}
test3.appviewx.com test3.appviewx.com valid  2048      {}   01/12/2023 5:29:59 AM {WebSelfHost}
test4.appviewx.com test4.appviewx.com valid  2048      {}   01/12/2023 5:29:59 AM {WebSelfHost}
```

- To return details such as thumbprint, subject, validity, SANs, and file locations for one or more ACME certificates previously created, execute the command below.

```
Get-PACertificate -List | Format-List
```

- To return details such as Thumbprint, Subject, Validity, SANs, and file locations for a specific certificate, execute the command below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

```
Get-PACertificate <Main_Domain_Name> | Format-List
```

- The certificate directory paths are as follows:
  - **Linux**: /home/<user>/.config/Posh-ACME/<server-name>/<account-id>/<order(Main_Domain_Name)>/
  - **Windows**: C:\Users\<user>\AppData\Local\Posh-ACME\<server-name>\<account-id>\<order(Main_Domain_Name)>\

The files within this certificate directory should have the following contents:

- cert.cer (Base64 encoded PEM certificate)
- cert.key (Base64 encoded PEM private key)
- cert.pfx (PKCS12 container with cert+key)
- chain.cer (Base64 encoded PEM with the issuing CA chain)
- chainX.cer (Base64 encoded PEM with alternate issuing CA chains)
- fullchain.cer (Base64 encoded PEM with cert+chain)
- fullchain.pfx (PKCS12 container with cert+key+chain)

Note: The password protecting the PFX files is **poshacme**.

Defining Custom and Certificate Attributes

attributes and attribute-type

The ***-attributes <Attributes>*** parameter allows users to provide multiple attributes in the Posh-ACME command. To provide attributes, list each attribute in the format of **'attribute_name'='attribute_value'** and separate each attribute with a semicolon.

Sample input for **attributes**: *-attributes @{'id'='1098';'environment'='development';'Director'='director_id'}*

The ***-attributesType <AttributesType>*** parameter must be accompanied with the ***-attributes <Attributes>*** parameter which takes in one of the following inputs **cert/custom/both**.

Sample input for **attributesType**: *-attributesType custom*

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Usage of attributes with attributesType

- When ***attributesType*** is passed as **cert**, the attributes from the ***attributes*** field are taken as certificate attributes.

  Sample certificate attributes input: *-attributes @{'Id'='1';'eai'='test';'inScope'='yes';'environment'='envi1'} -attributesType cert*

  The image below shows the certificate attributes defined in the Posh-ACME command.

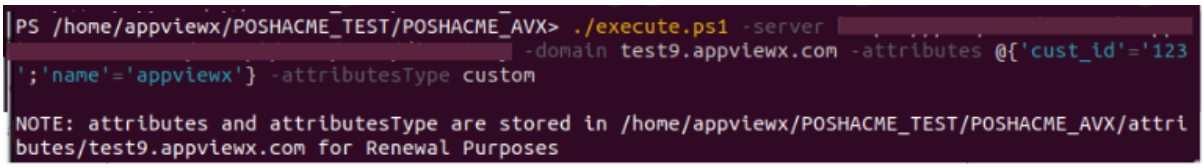


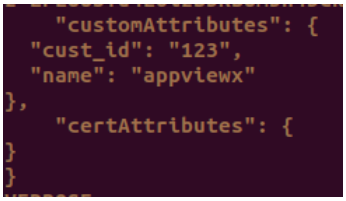


- When ***attributesType*** is passed as **custom**, the attributes from the ***attributes*** field are taken as custom attributes.

  Sample custom attributes input: *-attributes @{'cust_id'='123';'name'='appviewx'} -attributesType custom*

  The image below shows the certificate attributes defined in the Posh-ACME command.





- When ***attributesType*** is passed as **both**, a JSON mapping is expected by the AppViewX Posh-ACME. A json file in the name **attributesMapping.json** needs to be created inside the POSHACME_AVX directory. There is a template file named **attributesMappingTemplate.json** present within‘POSHACME_AVX’ directory, which can also be renamed to **attributesMapping.json**.

  A sample **attributesMapping.json** is given below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

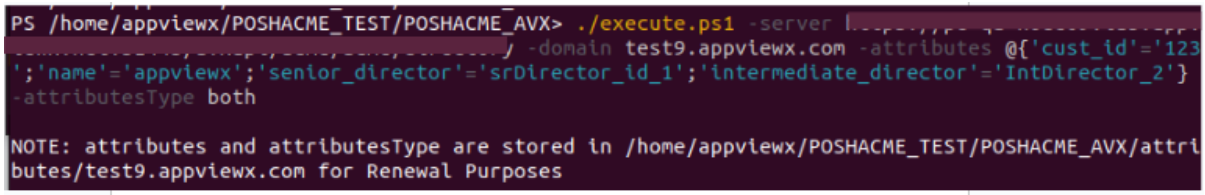
```
{
"senior_director" : "Sr Director",
"intermediate_director" : "Intermediate Director"
}
```

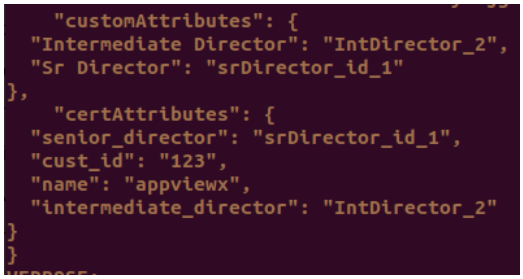
- The "key" [in the “key”:”value” pair from attributesMapping.json] refers to the certificate attribute key provided in the command, while the "value" corresponds to the custom attribute key where the value of the certificate attribute should be passed.
- The attributes passed as input will be sent as certificate attributes and for the attributes present in the attributesMapping.json, the mapped value is being used as attribute name and sent as custom attribute.

Sample certificate attributes input: *-attributes*

@{'cust_id'='123';'name'='appviewx';'senior_director':'srDirector_id_1','intermediate_director':'IntDirector_2'} -attributesType both

The image below shows the custom and certificate attributes defined in the Posh-ACME command.





Some important points to note are:

- The use of *‘-attributes <Attributes> -attributesType <AttributesType>’* is optional.
- Omitting this parameter will not disrupt the current flow of certificate creation. You may proceed with the certificate generation process without any issues.
- The values provided in the ‘attributes’ field and ‘attributesType’ field while enrolling would be stored in a folder named **attributes** inside the directory ‘POSHACME_AVX’ under the name of the certificate’s domain.
- These values would be fetched and used when the certificate of that domain name is being renewed.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Polling during Enrollment/Renewal

Polling can be activated when manual approval is configured for certificate generation. In this scenario, the client conducts polling for the certificate within a specified timeframe, as determined by the configured parameters. If the certificate is approved before the polling duration expires, it will be retrieved. To enable polling in the certbot client, you can pass the following parameters as mentioned below.

Parameters to be passed with Posh-ACME commands

Parameters	Type	Mandatory	Description
-retryInterval	Integer	No	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 2]
-retryCount	Integer	No	The number of times for which the certificate is polled from the client side. [Default value : 30]

A sample usage of the above parameters: `-retryCount 8 -retryInterval 5`

In this example, the *-retryInterval* is set to 5 seconds, and the *-retryCount* is set to 8. Hence, the certificate will be polled 8 times (retryCount) with a 5 second interval (retryInterval) for each polling attempt. The polling process will take a total of 8 * 5 = 40 seconds to complete.

Points to note:

- The use of *-retryCount <retryCount>* and *-retryInterval <retryInterval>* is optional and is required only when the attribute ‘Certificate Requests Need Approval’ is enabled in the CA policy settings of the ACME Server.
- Omitting these parameters will not disrupt the current flow of certificate creation.
- If necessary, the default values for polling will be utilized. You may proceed with the certificate generation process without any issues.

Providing CSR and EAB Fields

Fields to be provided in the CSR and for External Account Binding (EAB) can be configured in a json file. A json file in the name **certConfig.json** with the configured fields needs to be created inside the

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

POSHACME_AVX directory. There is a template file named **certConfigTemplate.json** present within POSHACME_AVX directory, which can be renamed to **certConfig.json**.

CSR fields that can be provided:

1. Subject fields:
    a. Organization
    b. Organization unit
    c. Country
    d. State
    e. Locality
2. Hashing algorithm (when using RSA)
3. Key-Size

EAB fields that can be provided:

1. EAB hmac
2. EAB kid
3. EAB Algorithm

A sample **certConfig.json** is given below:

```
{
"csr_params": {
        "organization" : "cert_appviewx",
        "organization_unit" : "crypto_avx",
        "country" : "IN",
        "state" : "Andhra Pradesh",
        "locality" : "Rajahmundry",
        "hashing_algorithm":"SHA384",
        "key_size":"2048"
        },
"eab": {
        "kid":"",
        "mac":"",
        "alg":"hs256"
}
}
```

Points to note:

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

- When EAB is not configured on the server side, the fields for ‘kid’ and ‘mac’ and ‘alg’ can be configured to empty strings ("").
- If you intend using the default configuration of Posh-ACME, you may set the fields in the certConfig.json file to empty strings ("").

For more information on the keywords used in the Posh-ACME commands, refer to the Keywords in Posh-ACME commands.

Troubleshooting Client-Side Errors

General errors that can be encountered.

1. Invalid End-point URL	
Description	When an invalid ACME endpoint URL is provided in Posh-ACME, it will result in the following error.
Error	`Set-PAServer: Name or service not known`
Troubleshooting	Ensure that the provided URL is valid and set up through the AppViewX GUI.
2. CA Certificate not configured in the client’s trust store	
Description	When the CA certificate of the ACME server is not configured in the client’s trust store, the following error is expected.

Error	`Set-PAServer: The remote certificate is invalid because of errors in the certificate chain: PartialChain`
	or
	`Set-PAServer: The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.`

Troubleshooting	Refer point 2 (To add custom CA certificates to TrustStore) in the section Providing Sudo Permissions in Linux.
3. Invalid Acme Agent	
Description	When the specified ACME agent name in the endpoint URL does not match any configured agent in the AppViewX GUI, it will trigger the following error.
Error	`Set-PAServer: {"detail":"Unable to fetch acme server url. - Agent Settings name given is invalid","type":"urn:ietf:params:acme:error:serverInternal"}`

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered. (continued)

Troubleshooting	Ensure that the provided URL is valid and set up through the AppViewX GUI.
4. Invalid Port in the End-point URL	
Description	This error is expected when invalid port details are provided in the acme end-point URL.
Error	InvalidArgument: /home/<user>/.local/share/powershell/Modules/Posh-ACME/4.18.0/Public/Set-PAServer.ps1:53 Line | 53 | $uri = [uri]$DirectoryUrl | ~~~~~~~~~~~~~~~~~~~~~~~~ | Cannot convert value "https://<server_hostname>:31443234/avxapi/<acme_agent>/acme/directory" to type "System.Uri". | Error: "Invalid URI: Invalid port specified."
Troubleshooting	Ensure that the port specified in the URL is valid.
5. Port 80 permission is missing for PowerShell	
Description	When PowerShell ‘pwsh’ executable lacks the capability to bind to port 80 without requiring root privileges, it will result in the following error.
Error	MethodInvocationException: Exception calling "Start" with "0" argument(s): "Permission denied" or Exception calling "Start" with "0" argument(s): "Access is denied"
Troubleshooting	Refer point 1 (To provide access to port 80 for a non-root user) in the section Providing Sudo Permissions in Linux.
6. Invalid Domain Name	
Description	When an enrollment call is made for an invalid domain name, the certificate issuance process will not proceed.
Error	Exception: /home/<user>.local/share/powershell/Modules/Posh-ACME/4.18.0/Public/New-PACertificate.ps1:271 Line | 271 | Submit-ChallengeValidation | ~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered. (continued)

	`| Authorization invalid for example.appviewx.com:`
Troubleshooting	In order for the domain to be considered valid and for the certificate issuance to succeed, a proper DNS entry must be made for the server corresponding to the domain before attempting to enroll a certificate for it.
7. Incorrect usage of attributes and attributesType fields	
Description	When only one field - either the 'attributes' or 'attributesType' is provided in the arguments of the enrollment command, it results in the following error.
Error	`Submit-OrderFinalize: Attribute type must be one of the following values : cert/custom/both)` `Both attributes and attributesType must be provided to add attributes in the certificate request...`
Troubleshooting	The 'attributesType' field must be accompanied with the 'attributes' field. Refer to the Accessing Orders and Certificates section for more information.
8. Incorrect attributeType	
Description	An incorrect value is provided for the field -attributesType.
Error	`Submit-OrderFinalize: Attribute type must be one of the following values : cert/custom/both)`
Troubleshooting	The 'attributesType' field must be one of the following values : cert/custom/both). Refer to the Accessing Orders and Certificates section for more information.
9. Incorrect IIS Site Name	
Description	An incorrect IIS site name is used for the field -SiteName.
Error	`Set-IISCertificate : Site <Site_Name> not found.`
Troubleshooting	The 'SiteName' field must be valid (present in the Sites of IIS Manager of the machine).
10. Missing EAB Credentials	
Description	EAB Credentials ('eab:hmac' and 'eab:key' fields) are set to empty string ("") in the 'certConfig.json' file, while the end-point server requires external account credentials.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered. (continued)

Error	`New-PACertificate : The current ACME server requires external account credentials to create a new ACME account. Please run New-PAAccount with the ExtAcctKID and ExtAcctHMACKey`
Troubleshooting	Provide valid EAB credentials for the ‘eab:hmac’ and ‘eab:key’ fields in the ‘certConfig.json’ file.
11. Invalid EAB Kid	
Description	Incorrect EAB kid is provided in the ‘certConfig.json’ file.
Error	`New-PACertificate: The "externalAccountBinding.protected" field is invalid.:: kid is invalid`
Troubleshooting	Provide a valid EAB kid which is configured in AppViewX ACME configuration settings.
12. Invalid EAB Algorithm	
Description	Incorrect EAB Algorithm is provided in the ‘certConfig.json’ file.
Error	`New-PACertificate : Some of the errors was found in request.`
Troubleshooting	Provide a valid EAB Algorithm which is configured in AppViewX ACME configuration settings.
13. Invalid Key Length	
Description	Incorrect key length is provided in the ‘certConfig.json’ file.
Error	`New-PACertificate : Cannot validate argument on parameter 'CertKeyLength'. Must be 'ec-256','ec-384','ec-521' for EC keys or between 2048-4096 (divisible by 128) for RSA keys`
Troubleshooting	Provide valid key length value. Must be 'ec-256','ec-384','ec-521' for EC keys or between 2048-4096 (divisible by 128) for RSA keys.

Glossary

- Keywords in Posh-ACME certConfig.json
- Keywords in Posh-ACME commands

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keywords in Posh-ACME certConfig.json

Json keys used in the Posh-ACME certConfig.json file

Json keys	Type	Comments
csr_params:organization **csr_params:organization_unit** **csr_params:country** **csr_params:state** **csr_params:Locality**	String	Choose the appropriate subject fields for the CSR. (Optional)
csr_params:hashing_algorithm	String	Hashing algorithm for signing (RSA). Specify any one algorithm from {SHA256, SHA384, SHA512}. [Default value: SHA384] (Optional)
csr_params:key_size	String	The type and size of private key to use for the certificate. For RSA keys, specify a number between 2048-4096 (divisible by 128). For ECC keys, specify either 'ec-256'\'ec-384'\'ec-521'. [Default value: 2048] (Optional) Whenever ECC keys are used, the hashing algorithm is set internally and cannot be changed from configuration file.
eab:kid	String	The value of Key Identifier for External Account Binding. (Optional)
eab:hmac	String	The value of HMAC key for External Account Binding.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Json keys used in the Posh-ACME certConfig.json file (continued)

Json keys	Type	Comments
		(Optional)
eab:alg	String	Signature Algorithm for External Account Binding. Specify any one algorithm from {HS256, HS384, HS521}. [Default value: HS256] (Optional)

Keywords in Posh-ACME commands

Keywords used in the Posh-ACME commands

Keyword	Expected Input	Comments
-domain	<Domain_Name> (Type: String) **domain1.com** (or) **domain1.com, domain2.com, domain3.com**	Comma-separated list of domains to obtain a certificate for.
-server	<Acme Server Endpoint URL fetched from AppViewX GUI> (Type: String)	ACME Directory Resource URI.
-attributes	[format: @{'id'='1098';'environment'='development';'Director'=' director_id'}]	The -attributes field allows users to provide multiple attributes in the format of **'attribute_name'='attribute_value'** and separate each attribute with a semicolon in the Posh-ACME command.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keywords used in the Posh-ACME commands (continued)

Keyword	Expected Input	Comments
		[optional, but **-attributes** field must be accompanied with the **-attributesType** field]
-attributesType	Any one of the following : **cert/ custom/both** (Type: String)	Takes in one of the following inputs **cert/custom/both**. [optional, but must be included when **-attributes** is passed]
-retryInterval	<retryInterval> (Type: Integer)	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 2] (Optional)
-retryCount	<retryCount> (Type: Integer)	The number of times for which the certificate is polled from the client side. [Default value : 30] (Optional)
-renewalDaysThreshold	<renewalDaysThreshold> (Integer)	Threshold value for renewal. Certificates with a remaining validity period (measured in days) less than the specified threshold will only be considered for renewal. [Default value: 30] (Optional)
-poshACMEDirectoryPath	<poshACMEDirectoryPath>	Path to the POSHACME_AVX folder.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Keywords used in the Posh-ACME commands (continued)

Keyword	Expected Input	Comments
-Name	<Main_Domain_Name> (Type: String)	The main domain name of the certificate. It is the same as the order name.
-SiteName	<Site_Name> (Type: String)	Name of the site in IIS
-certFile	<certFile> (Type: String)	Path to the certificate to be revoked.

MSIntune Integration Guide

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Intune is integrated with the Microsoft's Enterprise Mobility + Security (EMS) suite, it manages the application and protects the organization data. Users can configure specific policies to control the applications. It makes sure that the organization data is protected and isolated from the personal data.

• Overview
• Simple Certificate Enrollment Protocol (SCEP)
• MS Intune AppViewX Connector
• Prerequisites
• Configuring the AppViewX SCEP MS Intune Agent
• Testing on the Windows v10.0 Device
• References

Overview

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Intune is integrated with the Microsoft's Enterprise Mobility + Security (EMS) suite, it manages the application and protects the organization data. Users can configure specific policies to control the applications. It makes sure that the organization data is protected and isolated from the personal data.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Simple Certificate Enrollment Protocol (SCEP)

Simple Certificate Enrollment Protocol (SCEP) is a protocol that allows devices to enroll for a certificate using URL and a shared secret to communicate with a PKI. It uses the CA certificate to secure the message exchange for the CSR. SCEP is used for Certificate-based authentication, whereby access to services such as Wi-Fi, VPN, and securing e-mail through encryption is carried out using certificates.

MS Intune AppViewX Connector

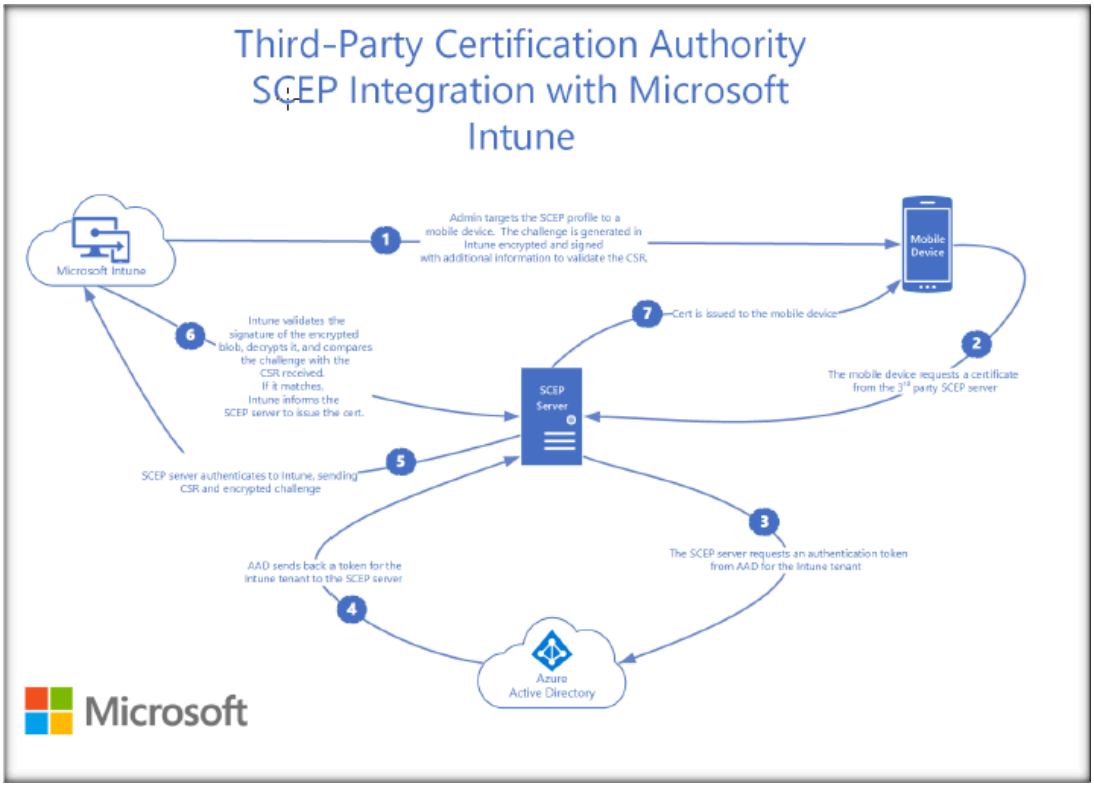
MS Intune AppViewX Connector is a SCEP server that handles certificate request validation through Microsoft Intune and certificate enrollment through AppViewX. To use the SCEP for certificates in Intune

1. In Intune, the an administrator creates a SCEP certificate profile, and then targets the profile to users or devices.
2. The device checks in to Intune.
3. Intune creates a unique SCEP challenge. It adds the additional integrity-check information, such as, what the expected subject and SAN should be.
4. Intune encrypts and signs both the challenge and integrity-check information, and then sends this information to the device with the SCEP request.
5. The device generates a certificate signing request (CSR) and public/private key pair on the device based on the SCEP certificate profile that's pushed from Intune.
6. The CSR and encrypted/signed challenge are sent to the third-party SCEP server endpoint.
7. The SCEP server sends the CSR and the challenge to Intune. The Intune then validates the signature, decrypts the payload, and compares the CSR to the integrity-check information.
8. Intune sends back a response to the SCEP server, and states whether the challenge validation is successful or not.
9. If the challenge is successfully verified, then the SCEP server issues the certificate to the device.

The figure below shows the end to end flow of the device certificate enrollment via microsoft intune with help of SCEP server and third party CA.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Figure 6. End to End Flow of the Device Certificate Enrollment



MSIntune AppViewX connector plays the role of the third party SCEP server that enables certificate enrollment through AppViewX. This SCEP server performs as follow:

1. Handles the GetCACaps SCEP request by providing the capabilities that are supported by the CA.
2. Handles the GetCACert SCEP request by providing the SCEP server certificate.
3. Handles the certificate enrollment SCEP request by performing the below steps:
   a. Validates the incoming enrollment requests using the Microsoft java library.
   b. If the validation is successful, get the certificate issued by AppViewX and send it back to the device.
   c. Send appropriate (success/failure) notifications to Intune using the Microsoft library.

Prerequisites

- Before you begin
- Configuring the Intune
- Creating the Certificate Profiles

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Before you begin

The certificates are required for device enrollment

- Root CA certificate for the selected CA
- Intermediate CA (Issuing Authority) certificate for the selected CA
- Server certificate with Root CA and Intermediate CA as a chain needs to be available in AppViewX. This has to be issued by the CA selected for enrollment
- Software requirements

S/No	Operating System	Versions

Configuring the Intune

The Intune application registration and certificate profile creation are to be done in the Azure portal (portal.azure.com)

Registration of the Intune Application

1. In the Azure portal,go to **Azure Active Directory > App Registrations**, and then select **New registration**.
2. On the Register an application page, specify the following details:
   a. In the Name section, enter the application name as required.
   b. In the Supported account types section, select the **Accounts in this organizational directory only** from the dropdown list.
   c. For Redirect URL, leave the default of Web, and then specify the sign-on URL for the third-party SCEP server.
3. Select **Register** to create the application and to open the Overview page for the new app.
4. On the app Overview page, copy the Application (client) ID value. (Record the value for later use)
5. In the navigation pane for the app, go to **Certificates& secrets > Manage**
   a. Select the New client secret button.
   b. Enter a value in Description, select any option for Expires, and then choose Add to generate a value for the client secret.
   c. Copy the value for the client secret and record it for later use.
6. Record your Tenant ID. The Tenant ID is the domain text after the @ sign in your account.
   For example, if your account is *admin@name.onmicrosoft.com*, then your tenant ID is name.onmicrosoft.com.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

7. In the navigation pane, go to **API permissions > Manage**, and then
   a. On the *Request API permissions* page, select **Microsoft APIs**.
   b. In the search field, type 'Intune' and then select **Intune**
   c. Select **Application Permission**, expand Application and select the checkbox for **Application.Read.All (Read all applications)**.
   d. Select **Add permissions** to save this configuration
8. Select **Add a permission** again
   a. On the *Request API permissions* page, select **Microsoft APIs**.
   b. In the search field, type 'Microsoft Graph' and then select **Microsoft Graph**
   c. Select **Application Permission**, expand Application and select the checkbox for **Application.Read.All (Read all applications)**.
   d. Select **Add permissions** to save this configuration
9. Remain on the API permissions page, and select **Grant admin consent** for <*your tenant*>, and then select **Yes**.
10. Make sure that the app registration process in Azure AD is completed.

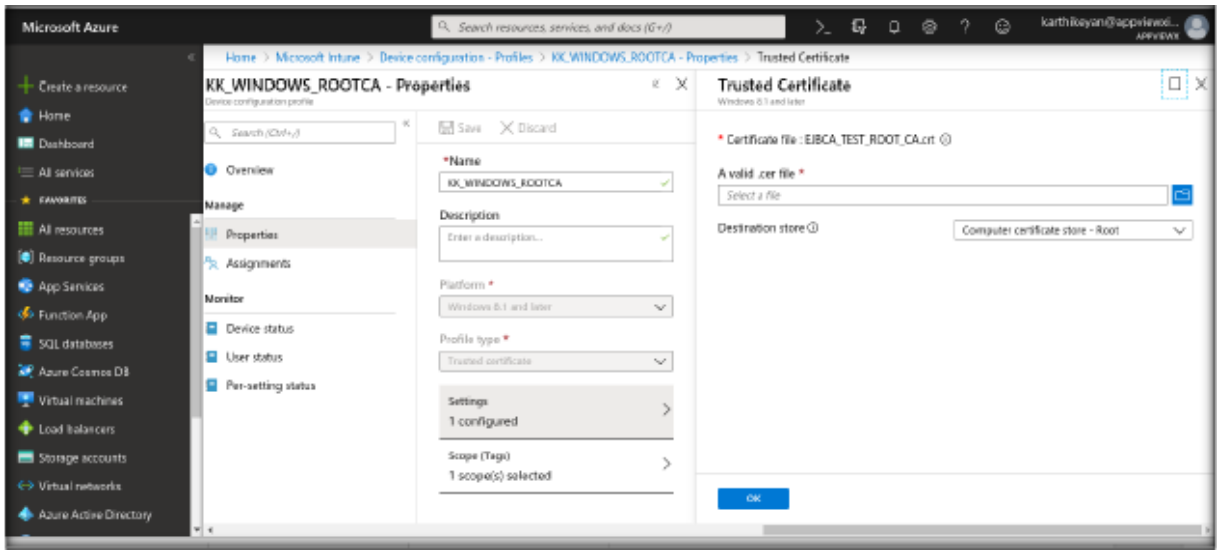
Creating the Certificate Profiles

- Creating the Trusted Certificate Profile for Root CA
- Creating the Trusted Certificate Profile for Intermediate CA
- Creating the SCEP Certificate Profile

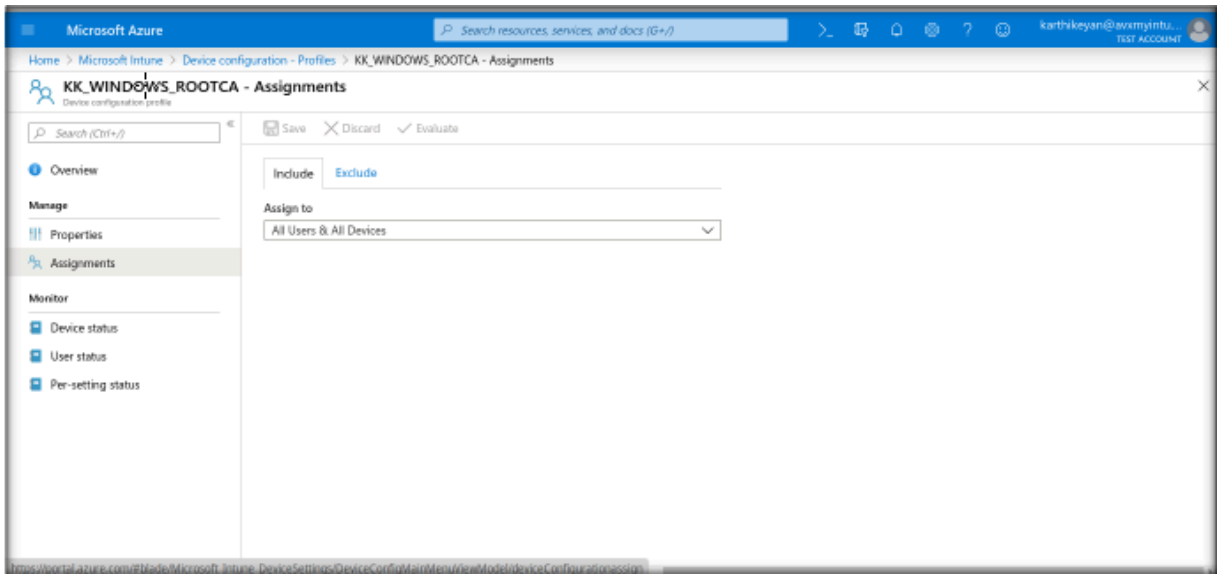
Creating the Trusted Certificate Profile for Root CA

1. Log in to the Azure portal.
2. In Azure portal, select **Intune > Device Configuration > Profiles > Create Profile**
3. Create the trusted certificate profile for Root CA with the properties as shown in the figure below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



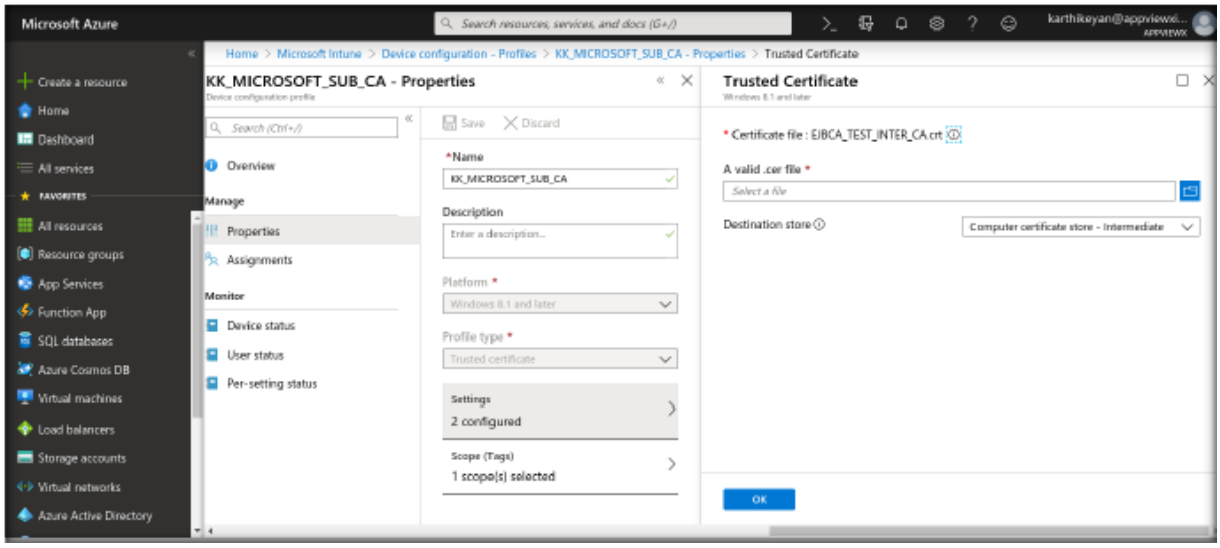
4. Upload the root CA certificate of the selected CA for the profile configuration.
5. Assign the Root CA profile to specific users/groups or all users/devices as required.



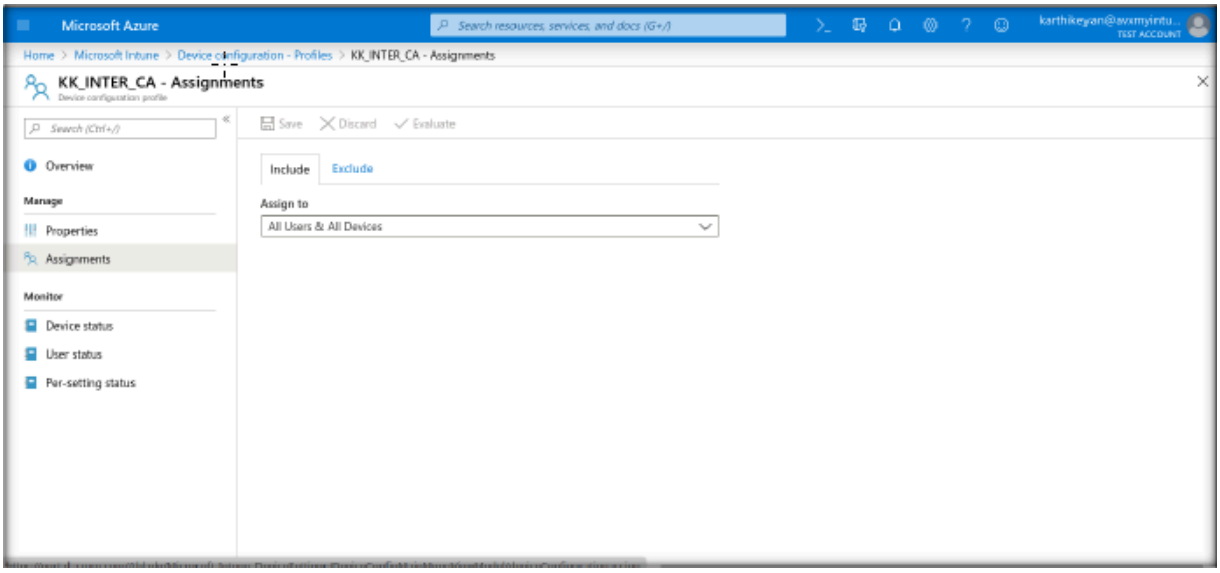
Creating the Trusted Certificate Profile for Intermediate CA

1. In Azure Portal, select **Intune > Device Configuration > Profiles > Create Profile**.
2. Create the trusted certificate profile for Intermediate CA with the properties as shown in the figure below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



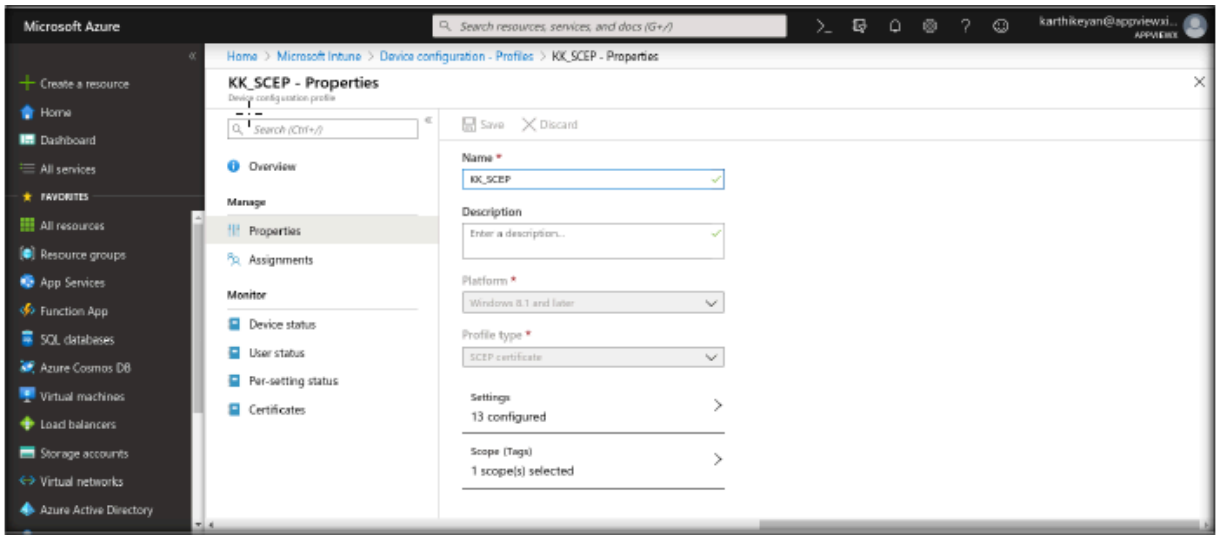
3. Upload the Intermediate CA certificate of the selected CA for this profile configuration.
4. Assign the Intermediate CA profile to specific users/groups or all users/devices as required.



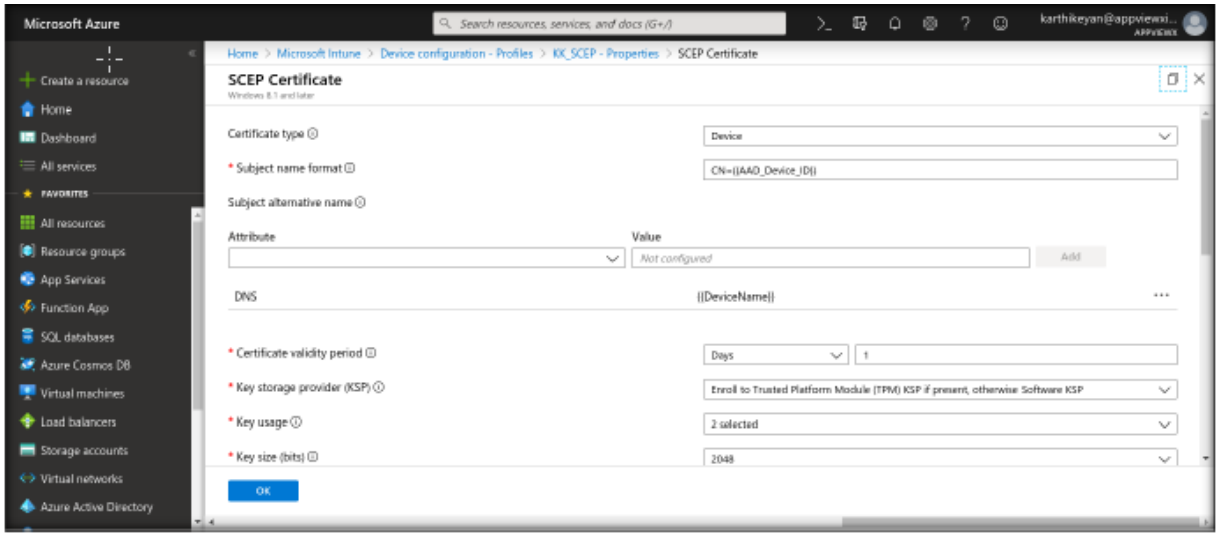
Creating the SCEP Certificate Profile

1. In Azure Portal, select **Intune > Device Configuration > Profiles > Create Profile**.
2. Create the SCEP certificate profile with the properties as shown in the figure below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

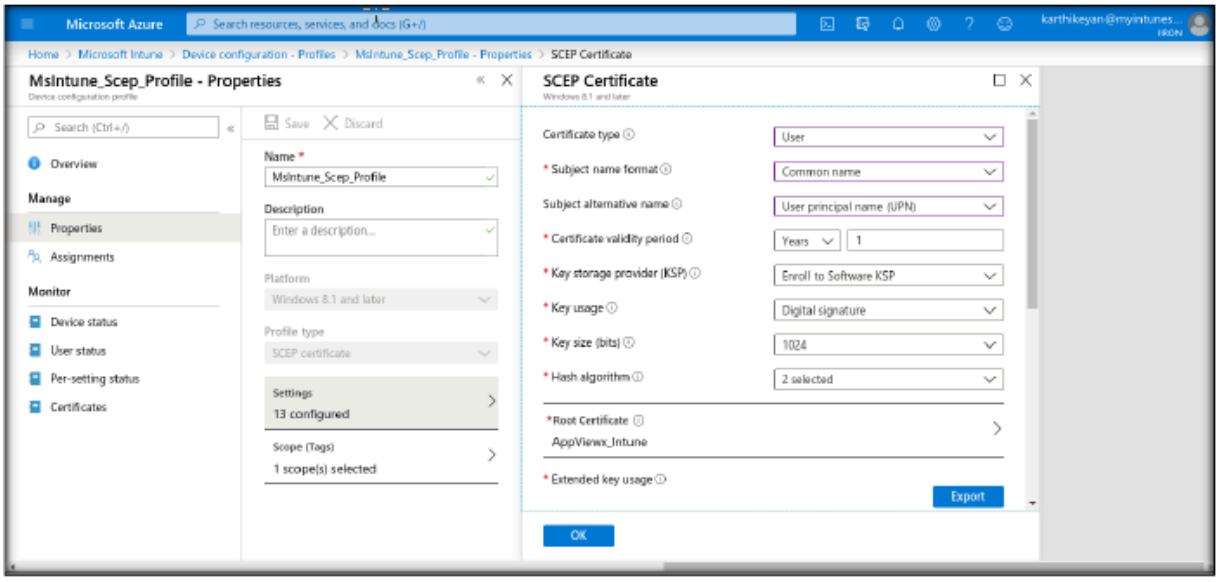


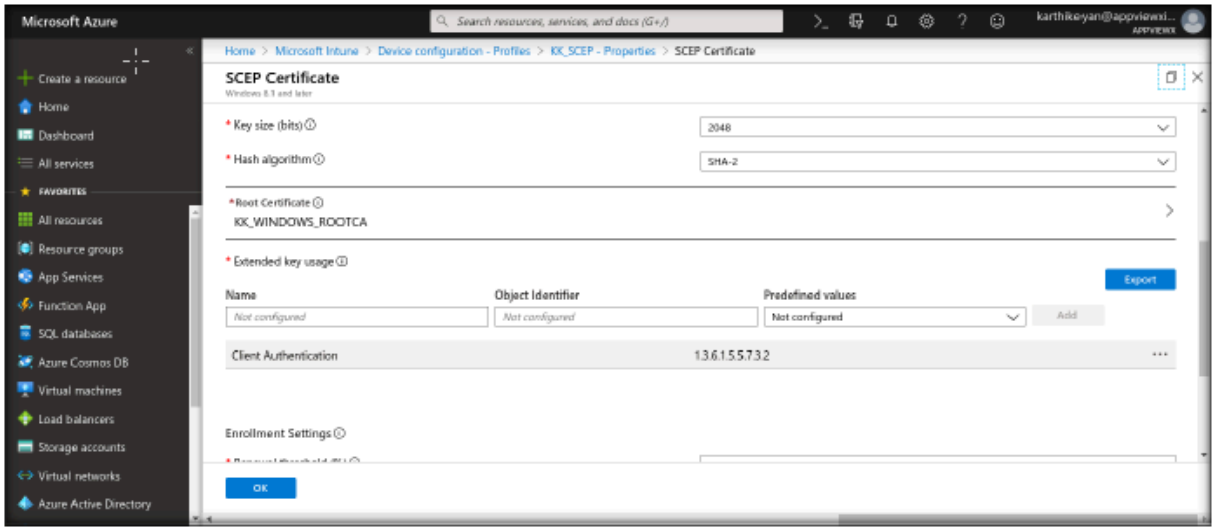
3. For Device certificate, configure the properties as shown in the figure below.



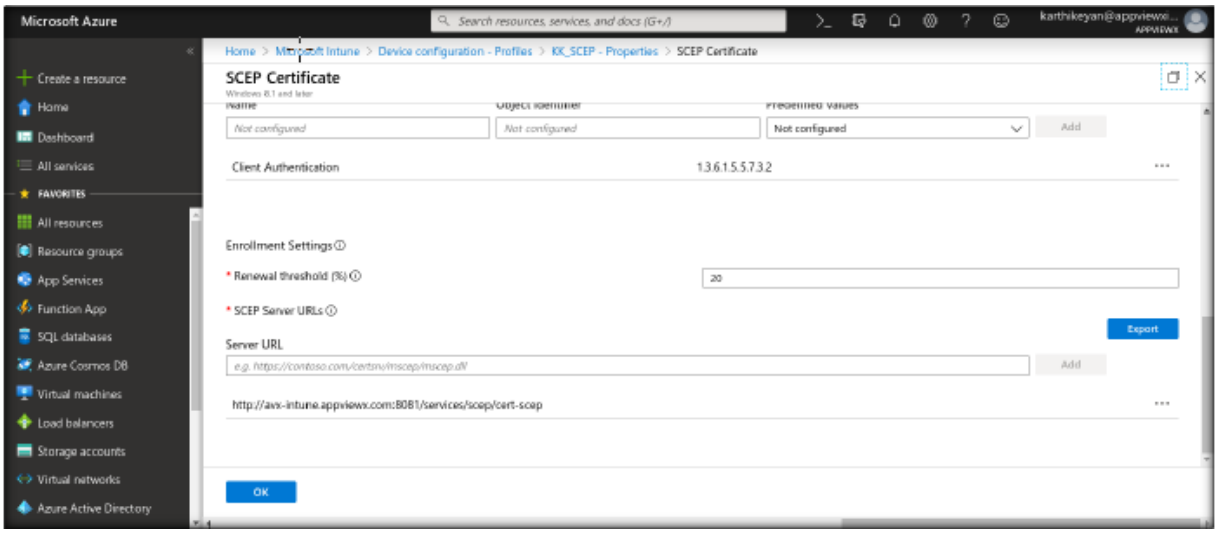
4. For User certificate, configure the properties as shown in the figure below.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

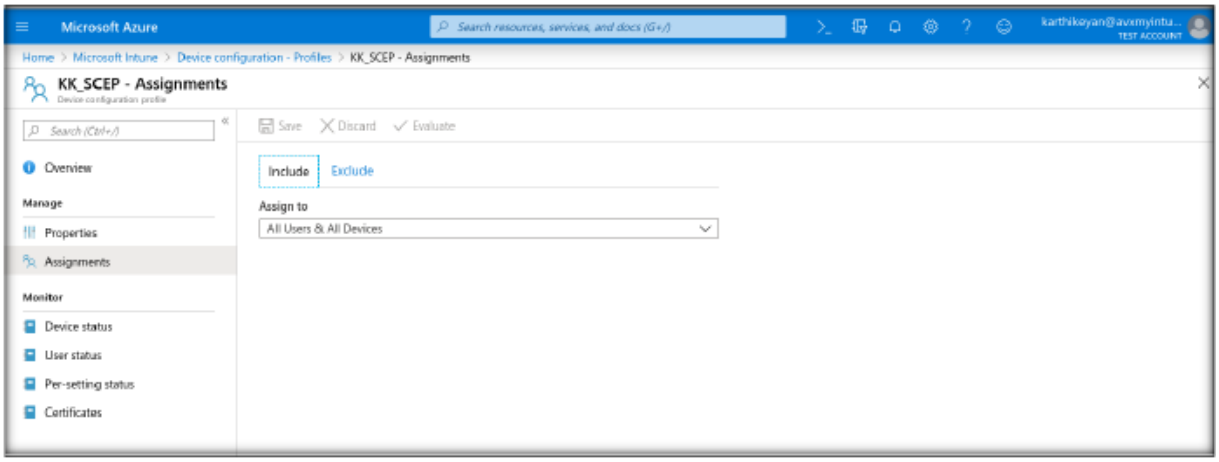




Copyright © 2024 AppViewX, Inc. All Rights Reserved.



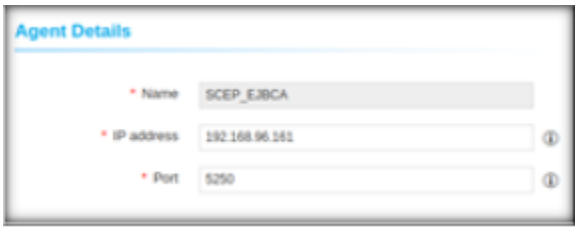
5. Assign the SCEP Certificate profile to specific users/groups or all users/devices as required.



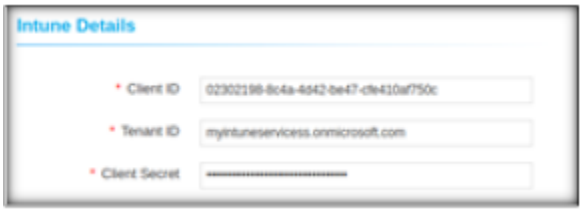
Configuring the AppViewX SCEP MS Intune Agent

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Certificate > Client > Settings > Auto enrolment > SCEP MS INTUNE**.
4. Enter the information in the **Agent Details**, **Intune Details**, **CA Settings**, **Vendor specific details**, and **Advanced Settings** sections
5. Under the **Agent Details** section, provide the **Name**, **IP address**, and **Port number** in which the SCEP Intune agent is running.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. Under the **Intune Details** section, provide the **Client ID**, **Tenant ID**, and **Client Secret**.



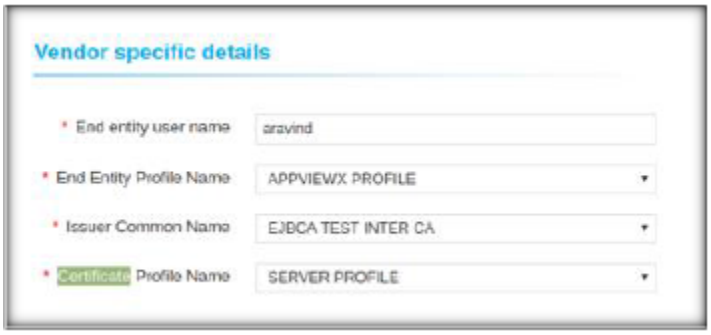
> **Note:** Port number varies depends on the AppViewX version
> - Version2019.3 through 2020.1 default port 5250
> - Version2020.2 default port 5014
> - Version2020.3 default port 5302

7. Under the **CA Settings** section, to select the **Certificate Type**, click the server check box
8. Select the CA from the Select CA dropdown list.
9. Select the CA account from the CA Account dropdown list.
10. Enter the required information in the **Server Certificate**, **CA Connector Name**, and **Certificate Validity** fields.

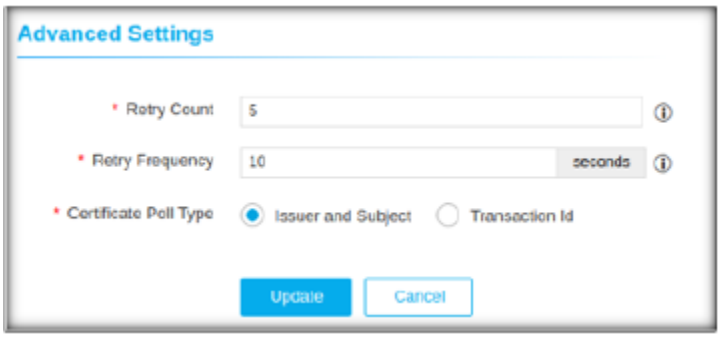


11. Under the **Vendor specific details** section, provide the **End entity user name**, and select the **End Entity Profile Name**, **Issuer Common Name**, and **Certificate Profile Name** from the respective field's dropdown list.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



12. Under the **Advanced Settings** section, enter the **Retry Count** and **Retry Frequency**.
13. To select the **Certificate Poll Type**, click **Issuer and Subject** checkbox.



14. Click**Update**.
15. Ensure that the server certificate contains the Root CA, Intermediate CA, and Server Certificate.

Testing on the Windows v10.0 Device

- Overview
- Configuring the Windows Accounts Setting
- Configuring the Company Portal
- Verifying the Enrollment Result

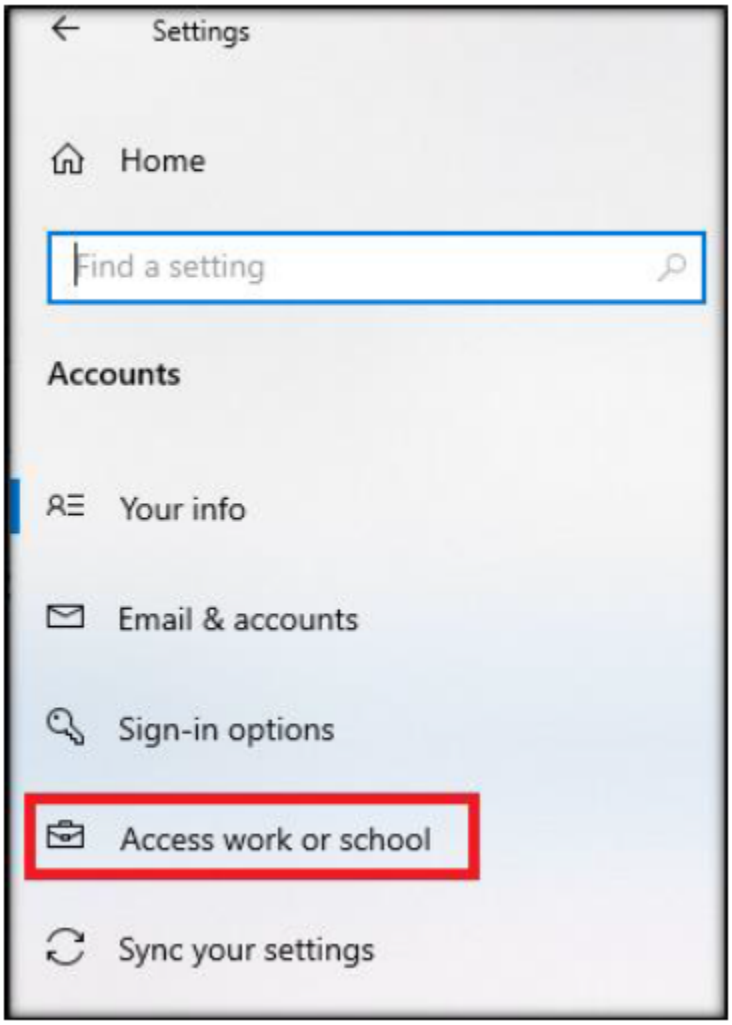
Overview

AppViewX MS Intune integration can be tested by enrolling in a Windows v10.0 device. To enroll in other devices, follow the same procedure. To enroll, the Windows v10.0 device must be installed with a **Company Portal** application from the Microsoft Store.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

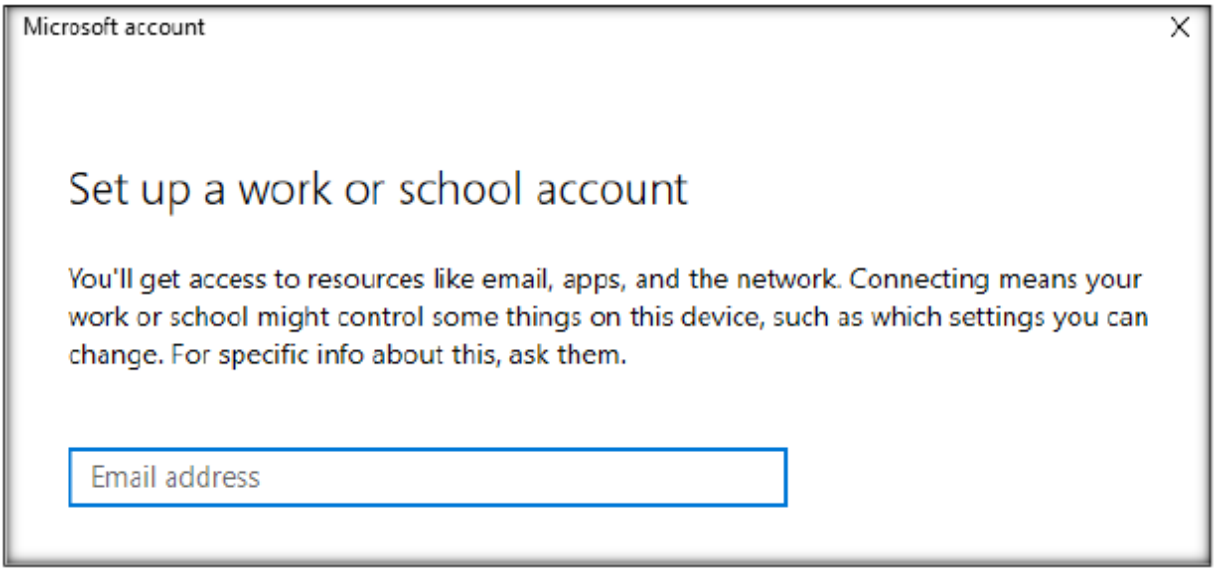
Configuring the Windows Accounts Setting

1. Log in to the system that has Windows v10.0 operating system.
2. Open **Settings**.
3. Click **Accounts > Access work or school**.

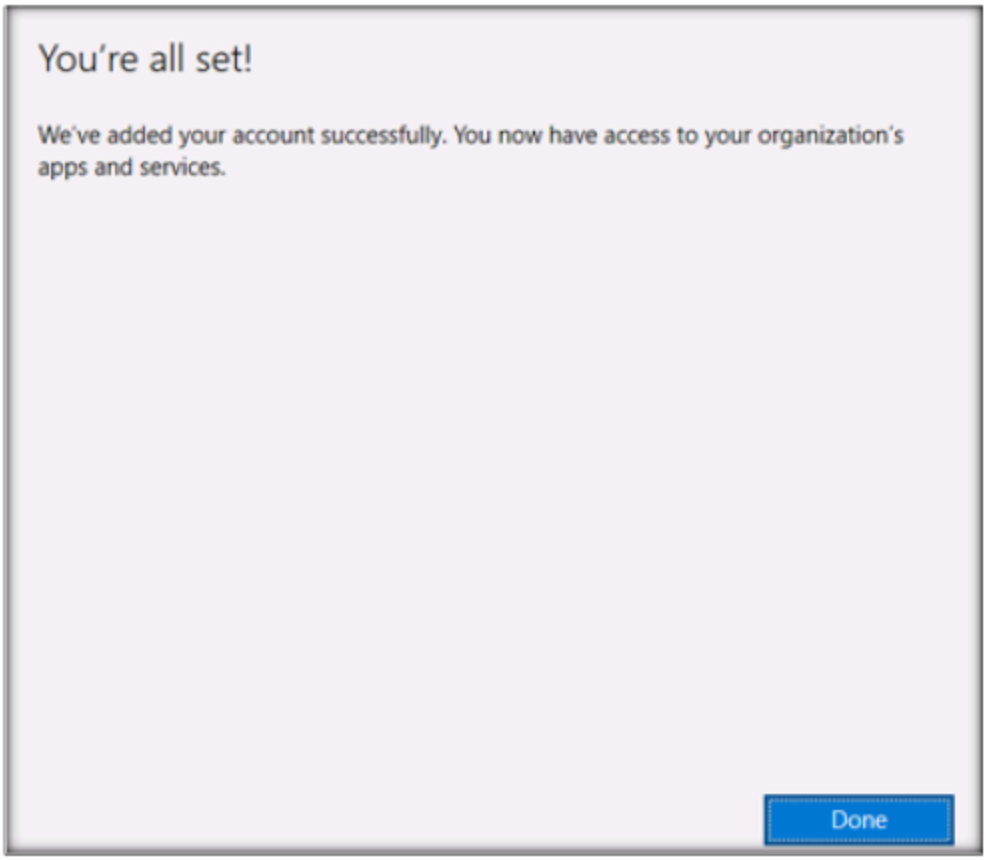


4. Click **Connect** and confirm your work or school account.
5. Click **Next** to proceed further by providing Azure subscription credentials.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.



6. Once account is set, the successful message window will be displayed.

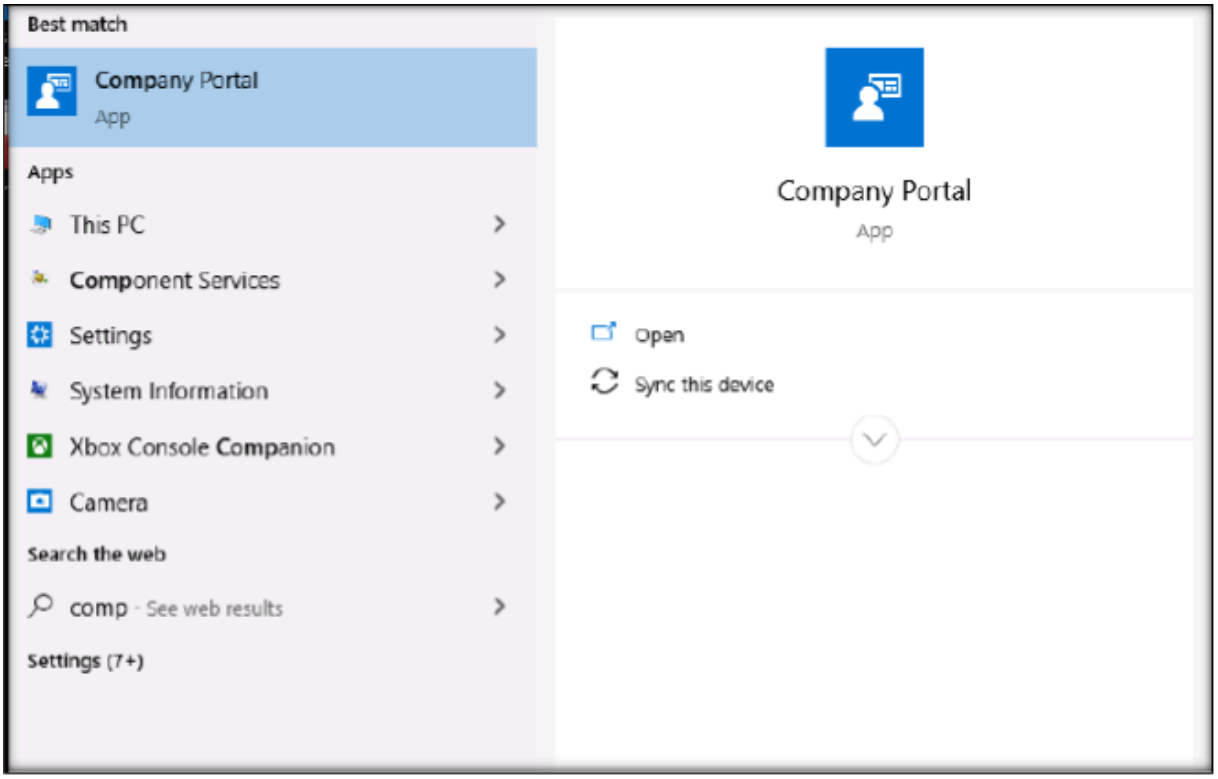


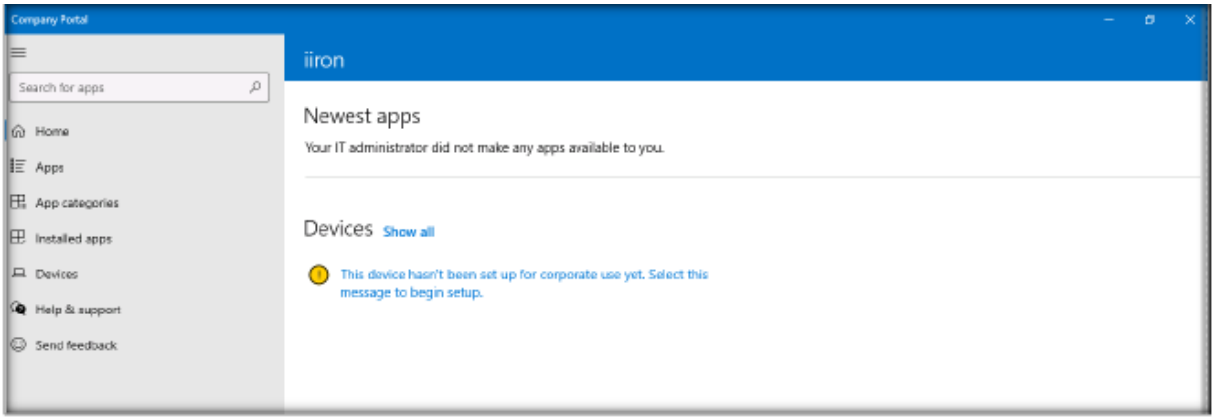
7. Click **Done**.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

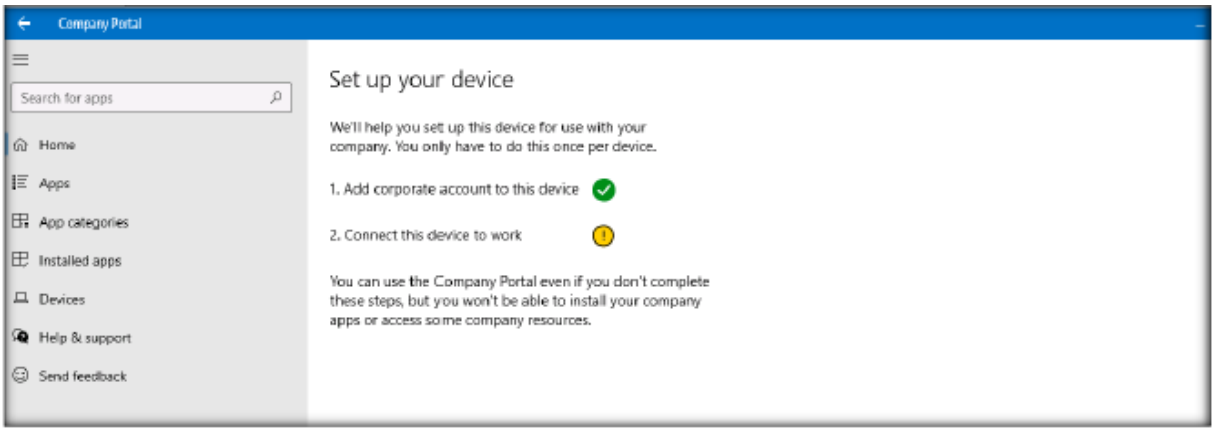
Configuring the Company Portal

1. Open the Company Portal application and proceed with the device set up by providing the azure subscription.

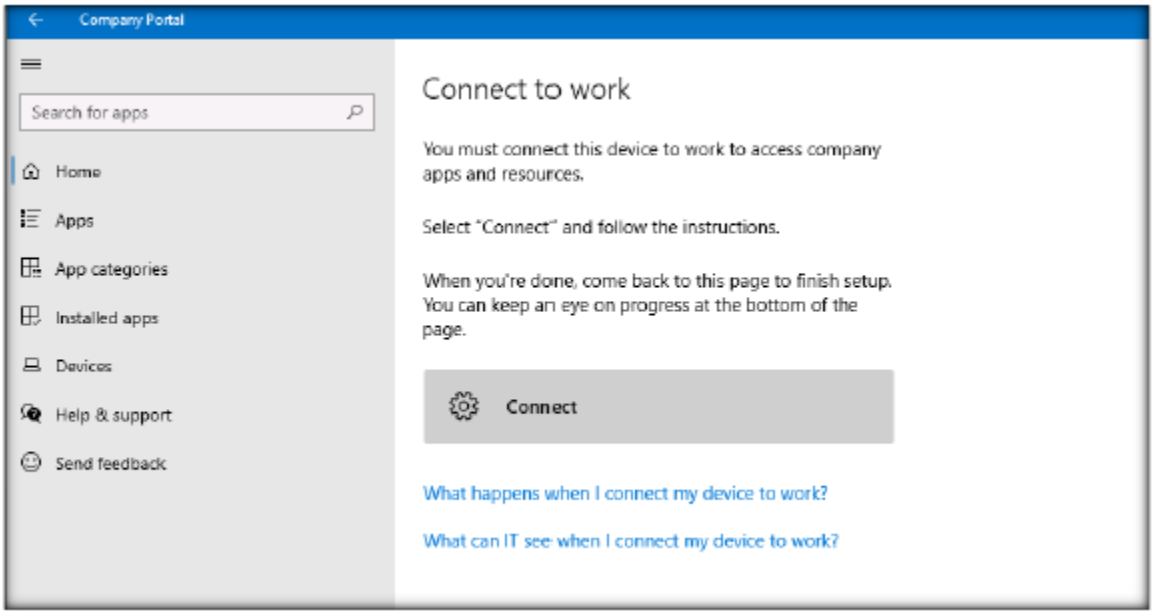




Copyright © 2024 AppViewX, Inc. All Rights Reserved.

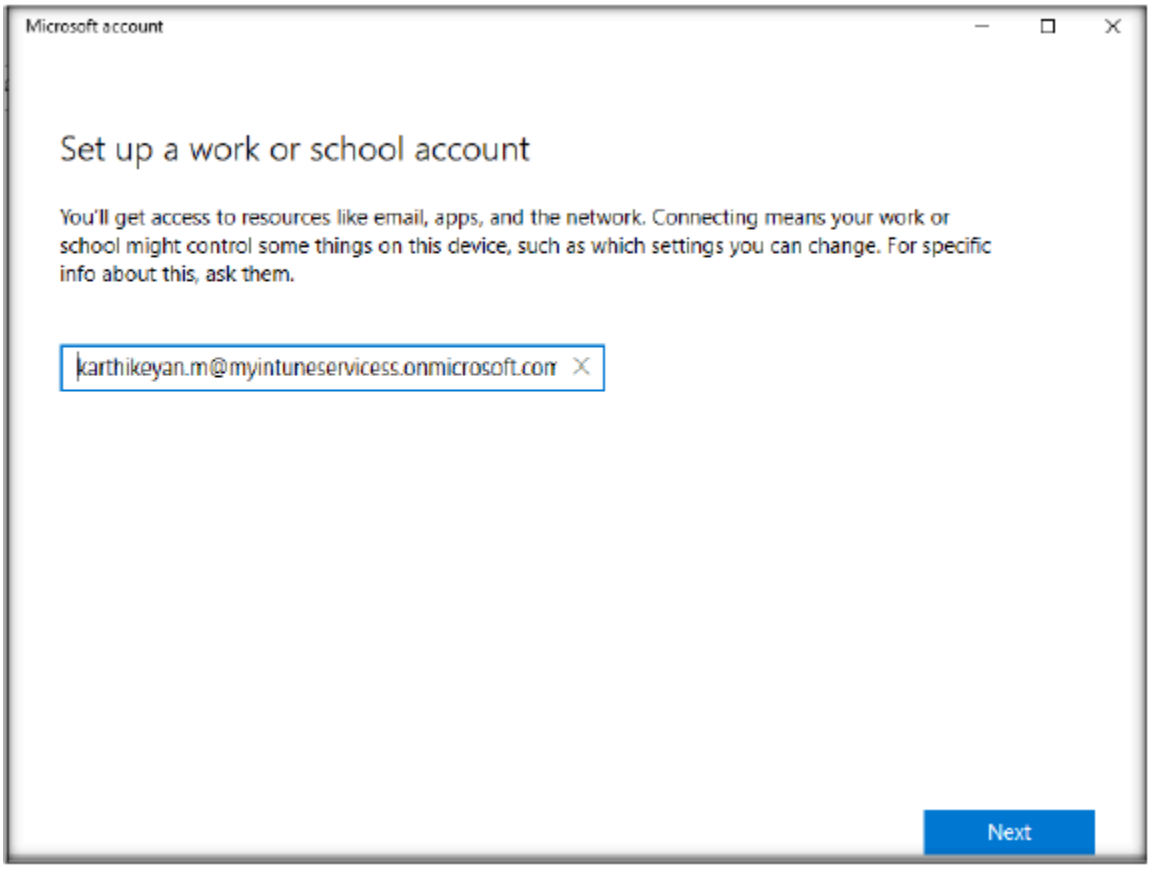


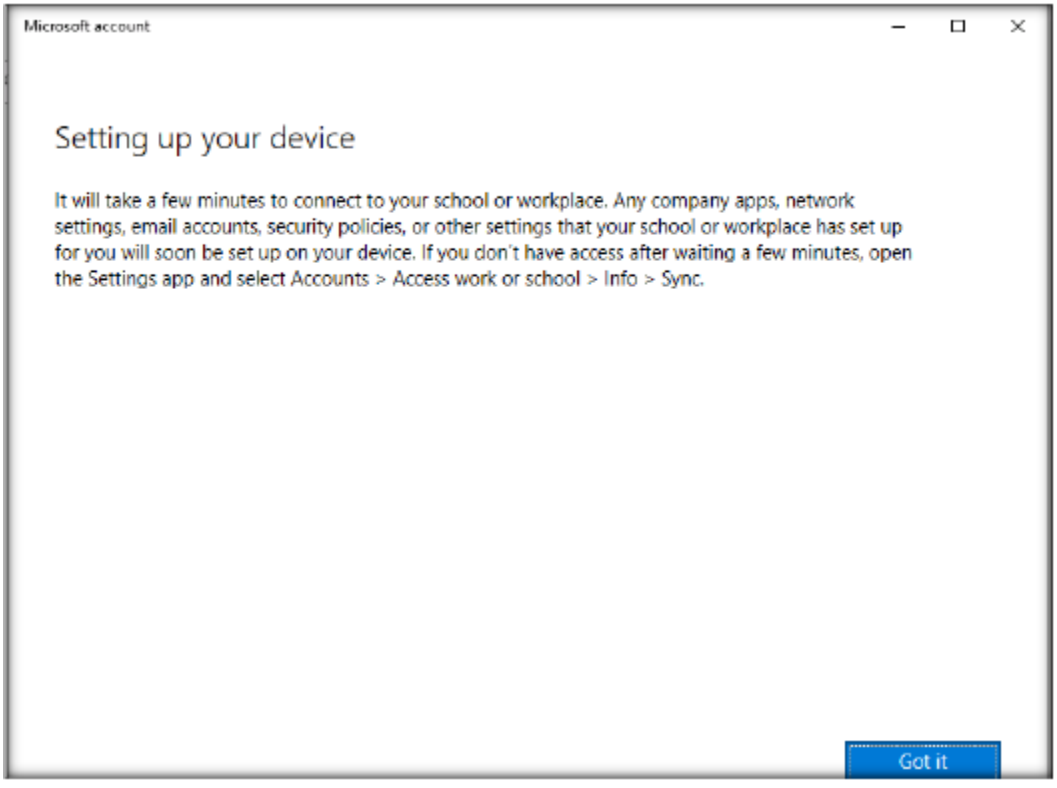
2. Click **Connect** and confirm your work or school account.



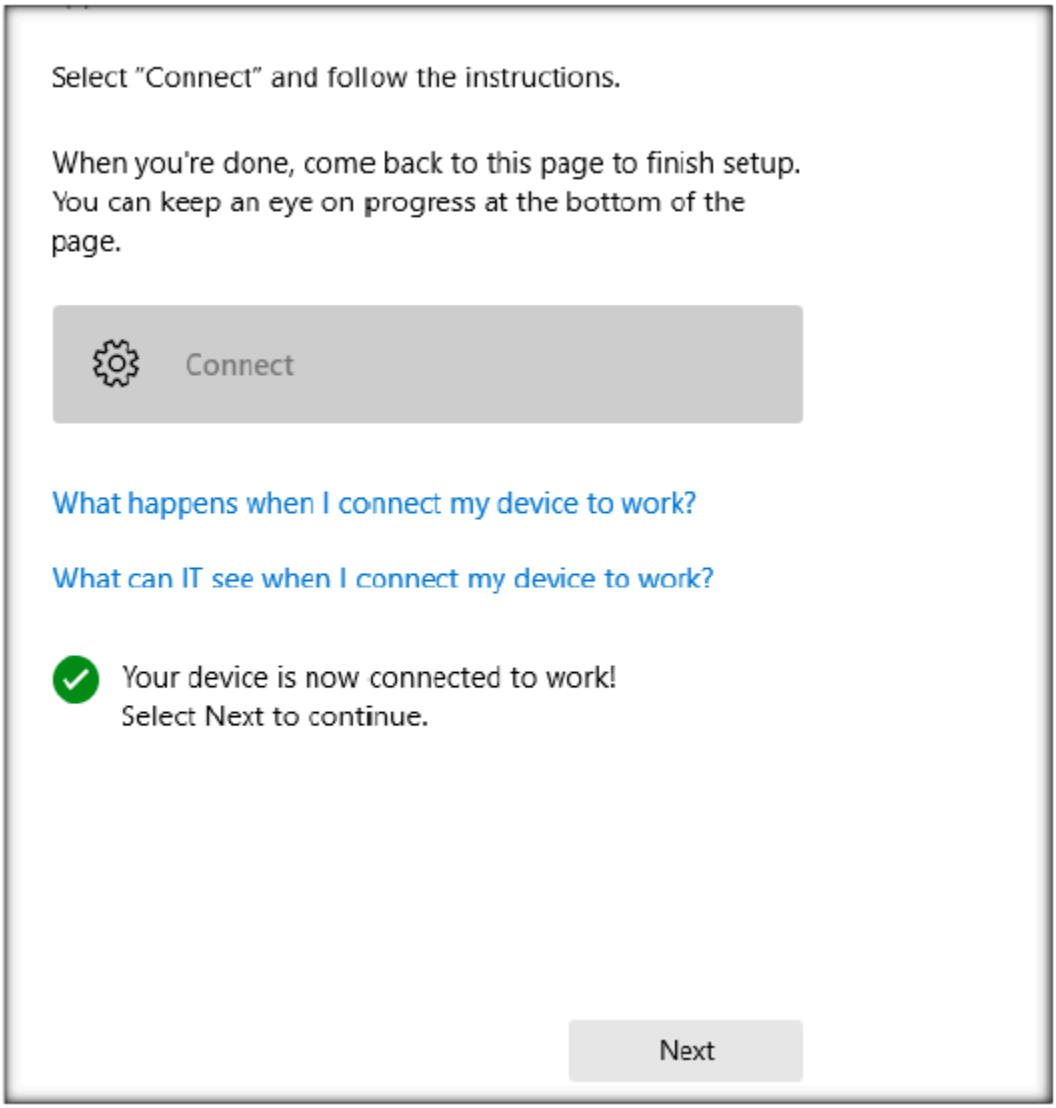
3. Provide valid e-mail address and click **Next** to proceed further to complete the set up.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

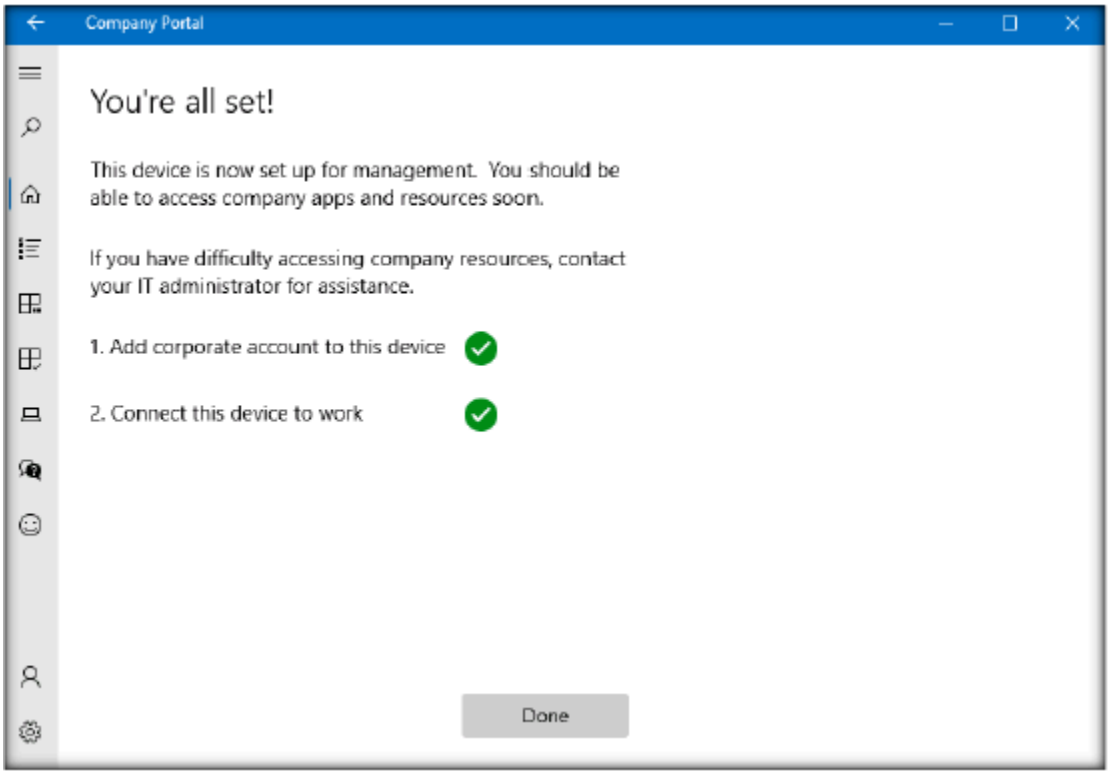




Copyright © 2024 AppViewX, Inc. All Rights Reserved.



Copyright © 2024 AppViewX, Inc. All Rights Reserved.



4. Click **Done**.

Verifying the Enrollment Result

1. Once configuration is completed, the device invokes the GetCACaps, GetCACerts, and PKIRequest (enrollment request) APIs to SCEP server.
2. Monitor the SCEP agent logs in AppViewX and verify that the message ‘AppviewxScepServicePostAction:49 - Response sent successfully for operation: PKIOperation’ occurs in the logs.
3. In AppViewX application, the newly generated certificate must be shown in the inventory.
4. If the certificate is requested, the device certificate newly generated certificate will be available in the **Server** tab in the certificate inventory.
5. If the certificate is requested user certificate, the new certificate will be available under the **Client** tab in the certificate inventory.
6. In the Windows device, open the cert store (Windows key+R -> certlm.msc) and make sure that the serial number of the certificate available in the personal cert store matches with the serial number of the certificate that is newly created in AppViewX.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

References

1. Micorsoft Docs - Add partner certification authority in Intune using SCEP
2. GitHub - Microsoft/Intune-Resource-Access
3. Simple Certificate Enrollment Protocol - draft-nourse-scep-23
4. Microsoft Docs - Set up Microsoft Intune
5. Microsoft Docs - Set up third-party CA integration

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Chapter 10: Glossary

Terms	Definition
ACME	Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating the certificate enrollment to the CA and provisioning the certificate on the requesting entity.
Certificate Authority (CA)	A certificate authority or certification authority is an entity that issues digital certificates. It certifies the ownership of the key pair belongs to the subject within the certificate.
CAA Record	A Certificate Authority Authorization Record specifies which certificate authority is allowed to issue certificate for a domain. If a certificate has CAA record, it means only the CAs listed in the CAA record are allowed to issue a certificate for the domain. If there is no CAA Record, it means any CA can issue certificate for the domain.
X.509 Digital Certificate	X.509 is a standard defining the format of public key certificates. An X. 509 certificate is using the widely accepted public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.
Identity	The digital certificate can also be called a Digital ID or Identity for the subject to whom it is certified.
PKI	A public key infrastructure (PKI) is a technology containing a set of roles, policies, and procedures needed to create, distribute, store and revoke digital certificates and manage public-key encryption.
KMIP	The Key Management Interoperability Protocol is a communication standard protocol that defines message formats for the management of cryptographic keys on a key management server.
MDM	Mobile Device Management (MDM) is the administration of mobile devices, such as smart phones, tablet computers, and laptops.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

Terms	Definition
EST	The **Enrollment** over Secure Transport or **EST** is a cryptographic protocol that describes an X. 509 certificate management protocol targeting public key infrastructure (PKI) clients that need to acquire client certificates and associated certificate authority (CA) certificates. **EST** is described in RFC 7030
SCEP	Simple Certificate Enrollment Protocol (SCEP) is an IETF RFC. This enables network user to request their digital certificate electronically and as simply as possible. Supported by most of the network devices.
SSL/TLS Certificates	SSL refers to Secure Sockets Layer whereas TLS refers to Transport Layer Security. Both are cryptographic protocols providing secure data communication in a network.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.