



CERT+ Admin Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

Copyright © 2022 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

Preface.....	8
Revision History.....	8
About this Guide	8
Audience.....	8
Text Conventions.....	8
Chapter 1. Getting Started.....	9
Overview.....	9
About AppViewX.....	9
CERT+ Overview.....	9
What is Certificate Lifecycle Management (CLM)?.....	10
What is x.509 Digital Certificate?.....	10
Certificate Authority.....	11
CERT Administration.....	11
Prerequisites.....	11
Supported Web Browsers.....	11
Accessing the CERT+.....	12
CERT+ Home Page.....	12
Chapter 2. Account Module.....	14
Overview.....	14
Resource.....	14
Overview.....	15
Create a Resource.....	15
Modify a Resource.....	20
Delete a Resource.....	22
Clone a Resource.....	24
Enable a Resource.....	27
Disable a Resource.....	29

Roles.....	31
Overview.....	31
Create a Role.....	32
Modify a Role.....	34
Delete a Role.....	36
Clone a Role.....	38
Enable a Role.....	40
Disable a Role.....	42
Birthright Role.....	44
User Group.....	47
Overview.....	47
Create a User Group.....	48
Modify a User Group.....	51
Delete a User Group.....	54
Clone a User Group.....	55
Enable a User Group.....	57
Disable a User Group.....	59
User.....	61
Overview.....	61
Create a User.....	61
Modify a User.....	65
Delete a User.....	69
Enable a User.....	71
Disable a User.....	72
Import Users.....	74
RBAC Configuration.....	76
Overview.....	76
Benefits of RBAC.....	76
Simplified RBAC Configuration in AppViewX.....	77

Accessing the Quick Config Option.....	77
Configuring RBAC using the Quick Config Option.....	77
Ways to Access Quick Config Wizard Flow.....	77
Chapter 3. CERT+ Setup.....	79
Configuring CA Settings.....	79
Amazon and Amazon Private CA.....	80
Custom CA.....	99
Digicert CA.....	105
Digicert MPKI	110
EJBCA CA.....	115
Entrust MPKI.....	120
GoDaddy CA.....	124
Google CA.....	132
InCommon CA.....	137
Let's Encrypt CA.....	143
Microsoft Enterprise CA.....	147
Microsoft Standalone CA.....	155
Symantec CA.....	163
Trustwave CA.....	169
GlobalSign MSSL.....	172
GlobalSign SSL.....	177
Nexus.....	181
Certificate Policy.....	187
Overview.....	188
Configuring Policy Details.....	188
Configuring Policy for Amazon CA.....	192
Configuring Policy for Amazon Private CA.....	198
Configuring Policy for Digicert CA.....	205
Configuring Policy for EJBCA CA.....	212

Configuring Policy for Entrust CA.....	219
Configuring Policy for Entrust MPKI CA.....	226
Configuring Policy for GlobalSign CA.....	233
Configuring Policy for GoDaddy CA.....	240
Configuring Policy for Google CA.....	246
Configuring Policy for Let's Encrypt CA.....	256
Configuring Policy for Microsoft Enterprise CA.....	263
Configuring Policy for Microsoft Standalone CA.....	270
Configuring Policy for OpenTrust CA.....	276
Configuring Policy for Sectigo CA.....	283
Configuring Policy for Symantec CA.....	289
Configuring Policy for Trustwave CA.....	297
Configuring Policy for GlobalSign MSSL CA.....	304
Configuring Policy for Nexus CA.....	310
Certificate Group.....	319
Overview.....	319
Assign Certificate to a Group.....	320
Create a Group.....	322
Delete a Group.....	326
Modify a Group.....	327
Unassign Certificate from a Group.....	327
Configuring Certificates.....	329
Configuring Certificate Settings.....	329
Configuring Certificate Attributes.....	331
Configuring Certificate Profiles.....	343
Managing Devices.....	348
Overview.....	348
Configuring Servers	348
Certificate Reports.....	381

Overview.....	381
Job Scheduler.....	385
Types of Scheduled Jobs.....	386
Device and Certificate Synchronization.....	387
CRL Certificate Revocation Check.....	388
Configuring Report Settings and Schedule.....	397
Report Routing.....	400
Validation Settings	402
Revocation Check Routing	403
Configure Certificate Authority	405
Securing CERT+.....	408
Auto Enrollment Protocols.....	408
Overview.....	408
ACME.....	409
EST.....	437
Microsoft Intune.....	470
SCEP.....	495
Chapter 4. Glossary.....	529

Preface

Revision History

Revision	Description	Date
3.0	Updated version of document for Release 2022.1.0 FP2 Beta	November 2022
2.0	Updated version of document for Release 2022.1.0 FP1	September 2022
1.0	Initial release of document for Release 2022.1.0	June 2022

About this Guide

This guide outlines the CERT+ administrative functionality. Also, learn about the new features and capabilities that make it easier to configure and administer your CERT+.

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Getting Started

- [Overview](#)
- [CERT Administration](#)
- [Prerequisites](#)
- [Accessing the CERT+](#)
- [CERT+ Home Page](#)

Overview

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 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.

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 requestors and associates them to a cryptographic key through the issuance of electronic documents known as digital certificates.

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.

Prerequisites

Supported Web Browsers

Web Browser	Version
Internet Explorer	11.0.9600.18817
Firefox	74.0.1 (64-bit)
Google Chrome	85.0.4183.83 (Official Build) (64-bit)

Related Documentation:

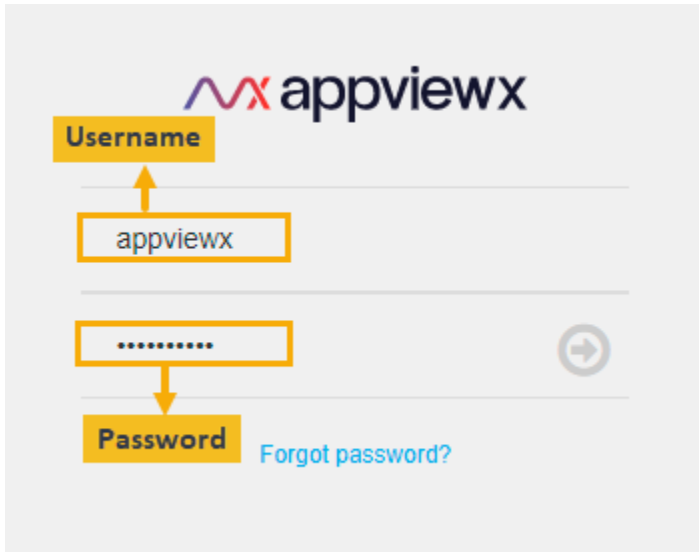
- License Management
- Logging & Alert Management.

Accessing the CERT+

Steps to access the CERT+,

1. Log in to AppViewX with a valid credential (URL provided by AppViewX).

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 as shown on the image. The following table describes the options available in the CERT+ home page:

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).

Options	Description	
Left Navigation Pane	Displays all the features available in the CERT+.	
Collapse/Expand	Hides/Displays the left navigation pane.	
Helps Tool Bar	Use the tool-bars for the additional options:	
	Options	Description
	Date	Displays Today Date
	Time	Displays the time based on the locale

Chapter 2: Account Module

- [Overview](#)
- [Resource](#)
- [Roles](#)
- [User Group](#)
- [User](#)
- [RBAC Configuration](#)
- [Accessing the Quick Config Option](#)

Overview

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.

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**).

Resource

- [Overview](#)
- [Create a Resource](#)
- [Modify a Resource](#)
- [Delete a Resource](#)
- [Clone a Resource](#)
- [Enable a Resource](#)
- [Disable a Resource](#)

Overview

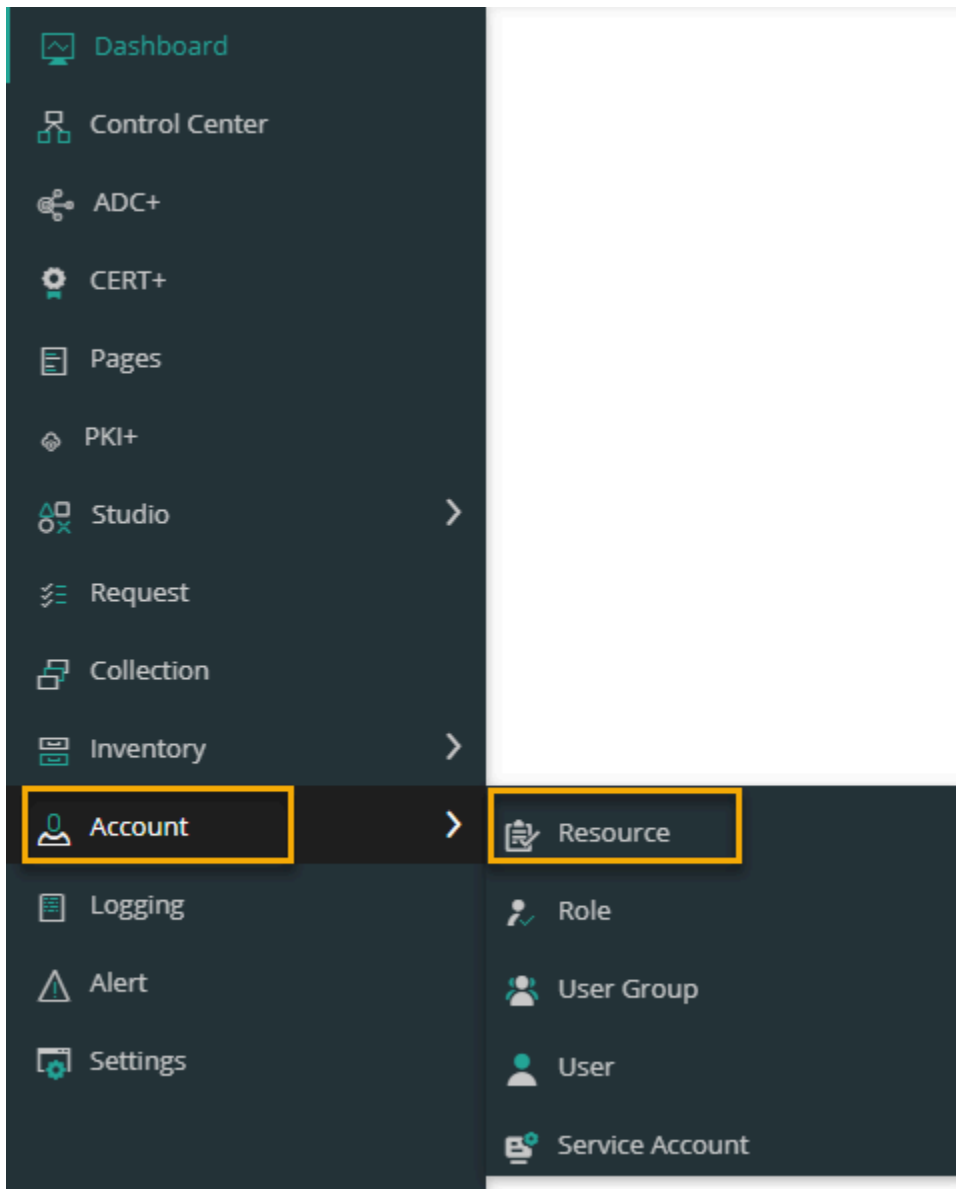
All the devices and objects that are configured within AppViewX are termed as Resources. The resource allows you to specify access at a granular level across all the devices and modules of AppViewX.

Resources can be assigned to a user group. Users within a user group will inherit resources assigned to that group. User groups can be assigned more than a resource. To enforce authorization policies on object levels such as for devices, certificates, and sub-objects such as wide-IP, virtual server, and so on users can configure resources and restrict user access to specific resources by mapping the resources to the respective user groups.

Create a Resource

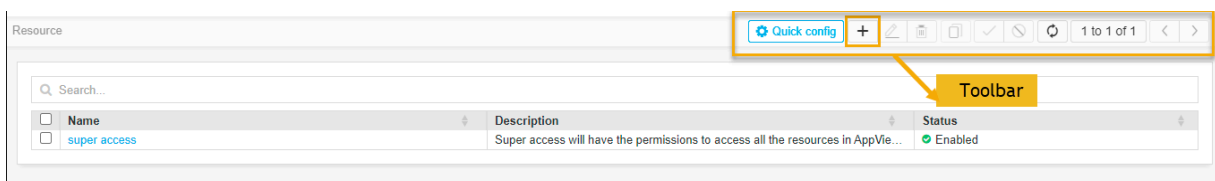
To create a resource,

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. Navigate to **Account**, and then click **Resource** from the list.



Note: AppViewX is packaged with default resource (super access) enabled. All the certificate groups have R (read) and RW (read and write) permissions to the super access resource.

The **Resource** page appears.





4. Click the **Add** icon in the command bar to create a new resource.

The **Add** page appears.

5. The following table describes the options available on the Add page:

Field	Description
* Name	Enter the name of the resource.
Description	Enter a brief description of the resource and granular-level access associated with the resource. Note: You can enter a maximum of 255 words in the field.
 Note: The asterisk (*) symbol indicates a mandatory field.	

6. Click **Save**.

The pop-up message appears as **Resource added successfully**.

7. Click **Access control** to associate the required resources and to provide permission.

8. The **Access control** tab lists the categories that can be controlled by RBAC using resources. Under the **Access control** tab, from the left pane, select one of the required categories. The available categories are,

- a. Device (to filter and select the devices that need to be assigned to a resource, click the  icon.)
- b. Certificate
- c. ADC (to filter the ADC objects that need to be assigned to the resource, click the  icon.)
- d. SSH
- e. Command Session Control
- f. Provisioning Templates
- g. Provisioning Requests
- h. Security Policy
 - i. Application Security Policy
- j. Proxy List
- k. Blueprint
- l. Application
- m. Workflow Studio
- n. Workflow Requests.



Note: AppViewX is packaged with default certificate groups (Certificate-Gateway and Default).

9. Associate the certificate groups to the resource and assign permission:

- Click R (Read-only) to assign read-only permissions.
- Click RW (Read and Write) to assign read and write permissions.
- On clicking R or RW the certificate group is associated with the resource.



Note: Provide RW (Read and Write) permission for the resource associate with the root user and R (Read-only) for others.

10. Use regular expression (regex) to identify and associate the certificate groups to the resource:

- a. Enter the regex in the Search field. For example, enter CA in the search field and click **R or RW** to assign Read-only or Read and Write permission respectively.
- b. Click the **Add as regex** button. All the certificate groups that match the regex will auto associate to the resource with the relevant permission. For example, all the certificate groups with CA in their name, such as CA-Digicert, CA-Entrust, CA-Sectigo will auto associate to the resource with R read permission.
- c. One or more than one regex can be added.



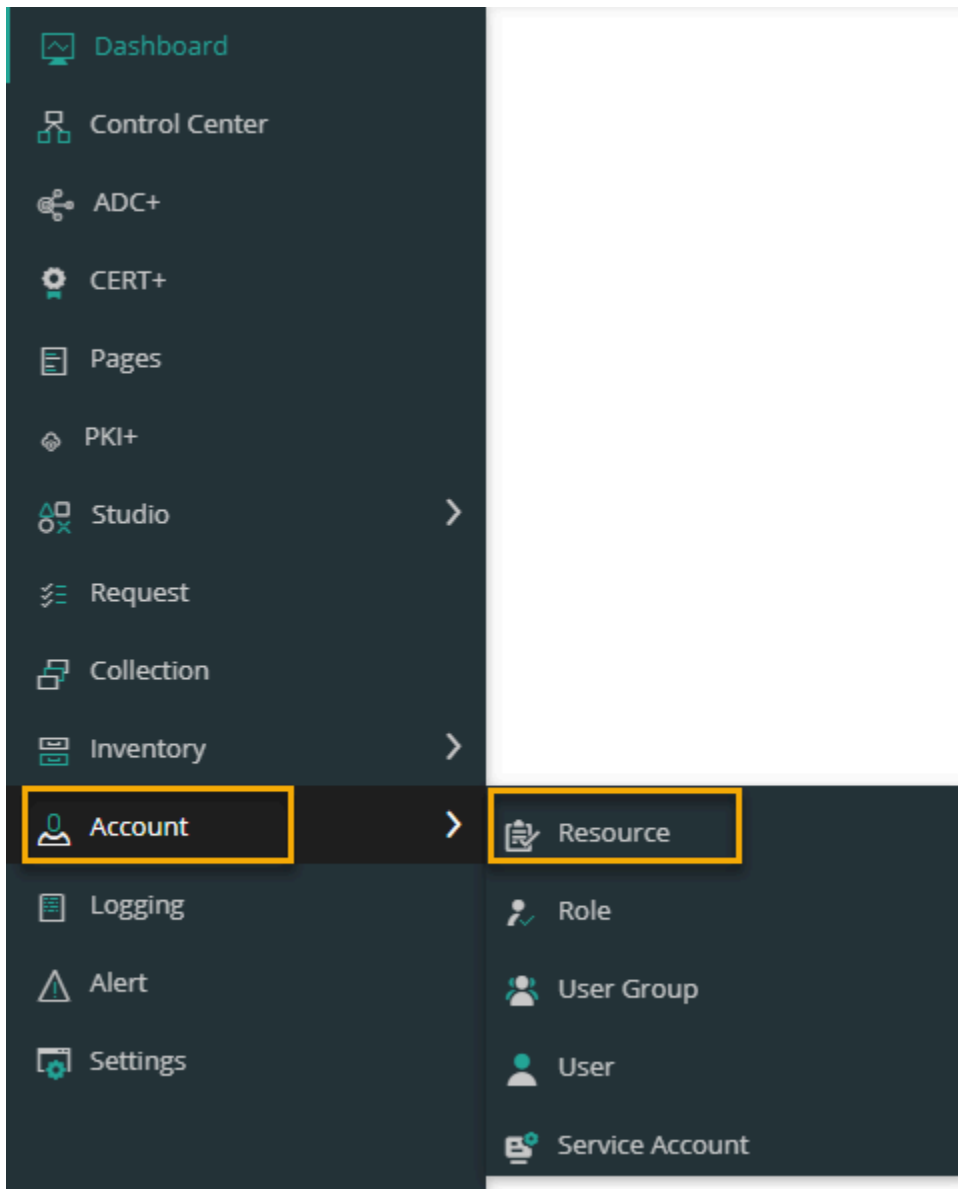
Note: The purpose of the regex is, the search string continues to work in the background and auto-associate all the new certificate groups to the resource when the certificate group matches the regex you created.

11. Click **Save**.

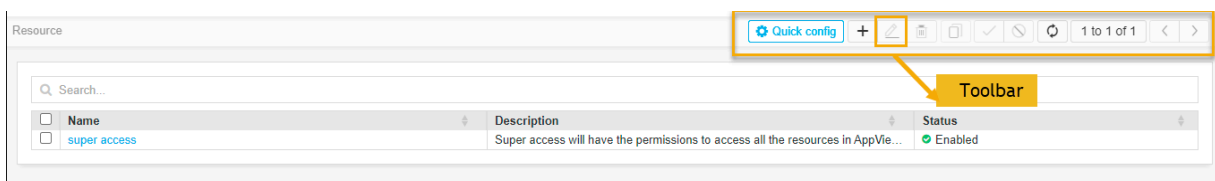
Modify a Resource

To modify Read (R) and Read/Write (R/W) permissions of devices, device objects, certificate groups, provisioning requests, or provisioning templates associated with a resource, modify a resource.

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. Navigate to **Account**, and then click **Resource** from the list.



The Resource page appears.



4. In the resource inventory, select the check box against the resource you want to modify.



5. Click the **Modify** icon in the command bar to modify a resource.

6. The **Information** tab appears. Click the **Access control tab** to add/ remove the certificate groups.
7. Click **Certificate** in the left pane. The list of Certificate groups appears.



Note: You can also modify Read (R) and Read/Write (RW) permissions for the certificate groups associated with a resource.

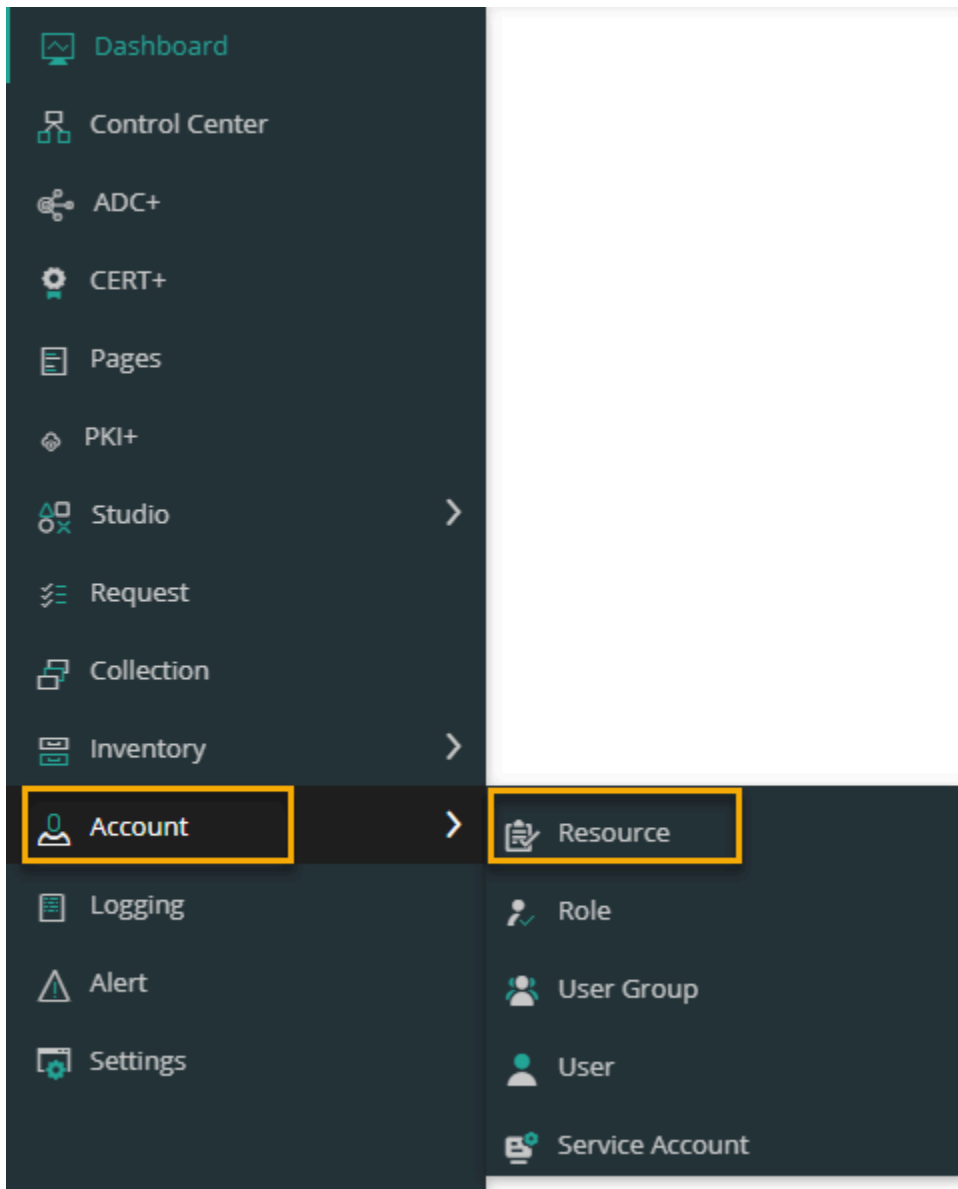
8. Select the check box against the certificate group you want to add.
 - a. Click **R (Read-only)** to assign read-only permissions.
 - b. Click **RW (Read and Write)** to assign read and write permissions.
9. Click **Save**, to associate the certificate group to the resource.
10. Unselect the check box against the certificate group you want to remove.
11. Click the **Save** button to disassociate the certificate group from the resource.

Delete a Resource

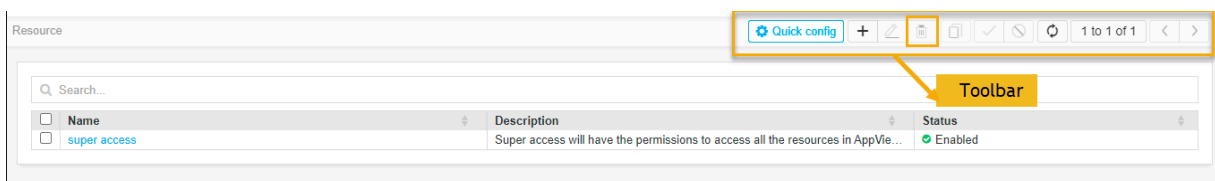
To delete a resource,

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. Navigate to **Account**, and then click **Resource** from the list.



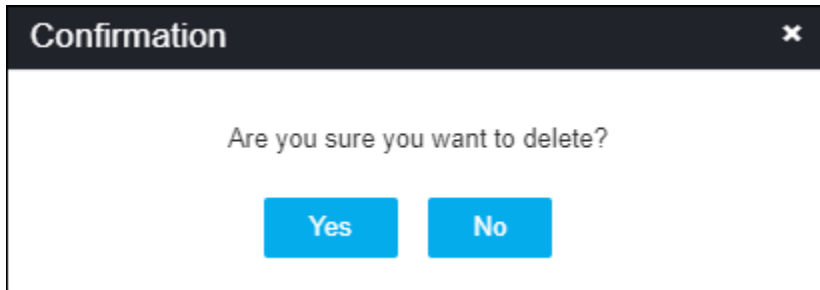
The **Resource** page appears.



4. In the resource inventory, select the check box against the resource you want to delete.



5. Click the  icon in the command bar to delete the resource.
6. A confirmation pop-up window appears.



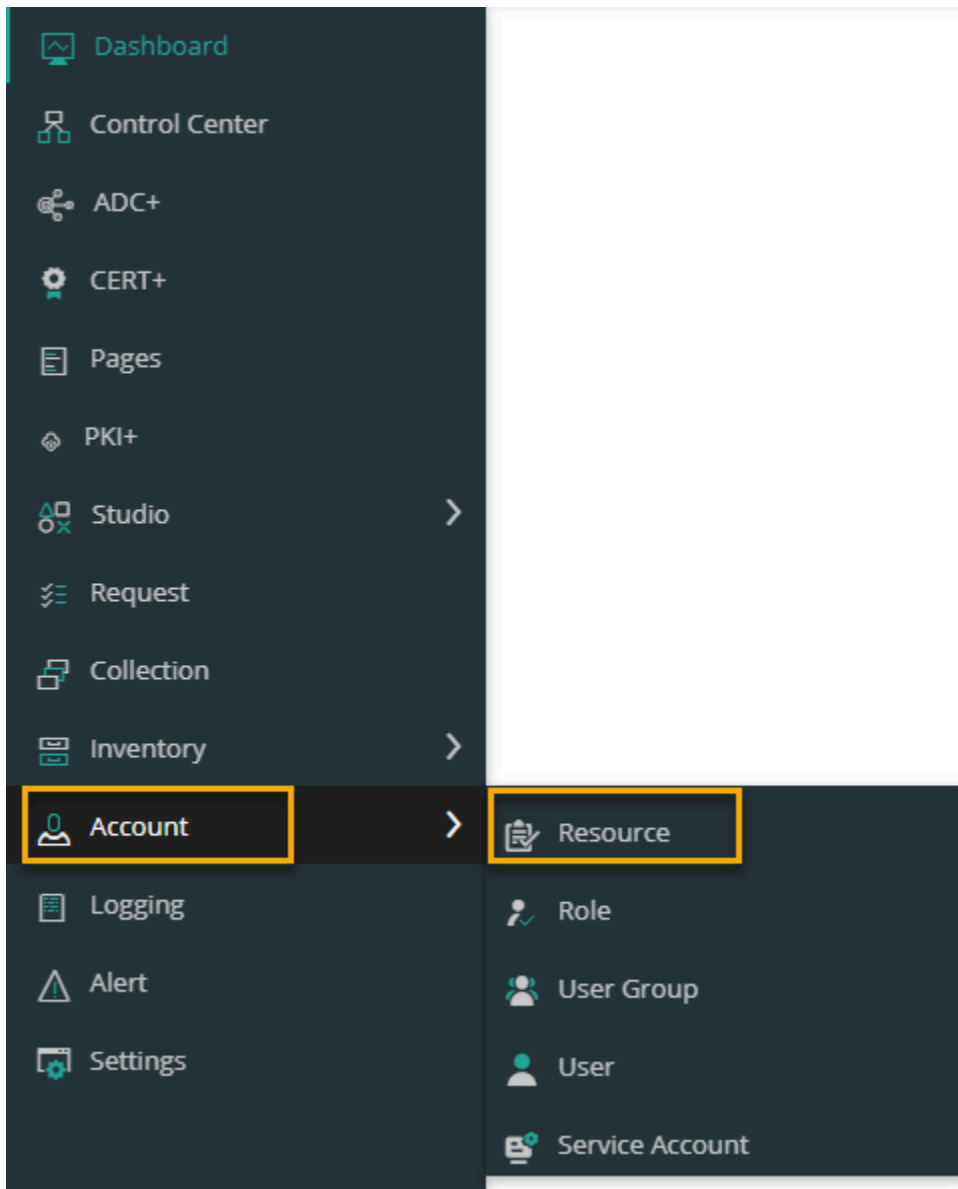
7. Click **Save**. The resource is deleted and a pop-up message displays as **Operation performed successfully**.

Clone a Resource

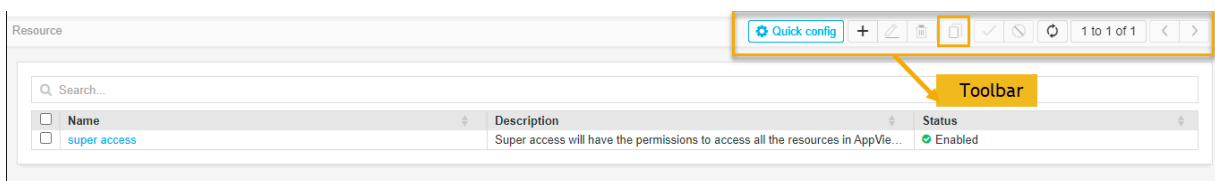
Clone allows you to create an exact copy of an existing resource with all the access control permissions.

To clone a resource,

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. Navigate to **Account**, and then click **Resource** from the list.



The **Resource** page appears.

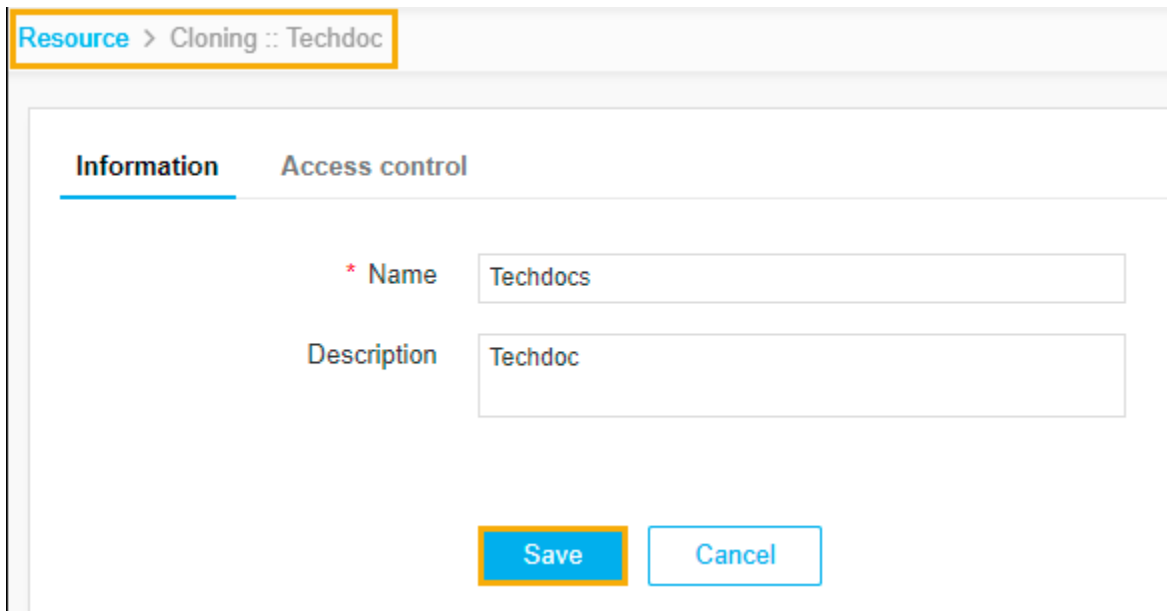


4. In the resource inventory, select the check box against the resource you want to clone.



5. Click the icon in the command bar to clone the resource.

The selected Cloning page appears.



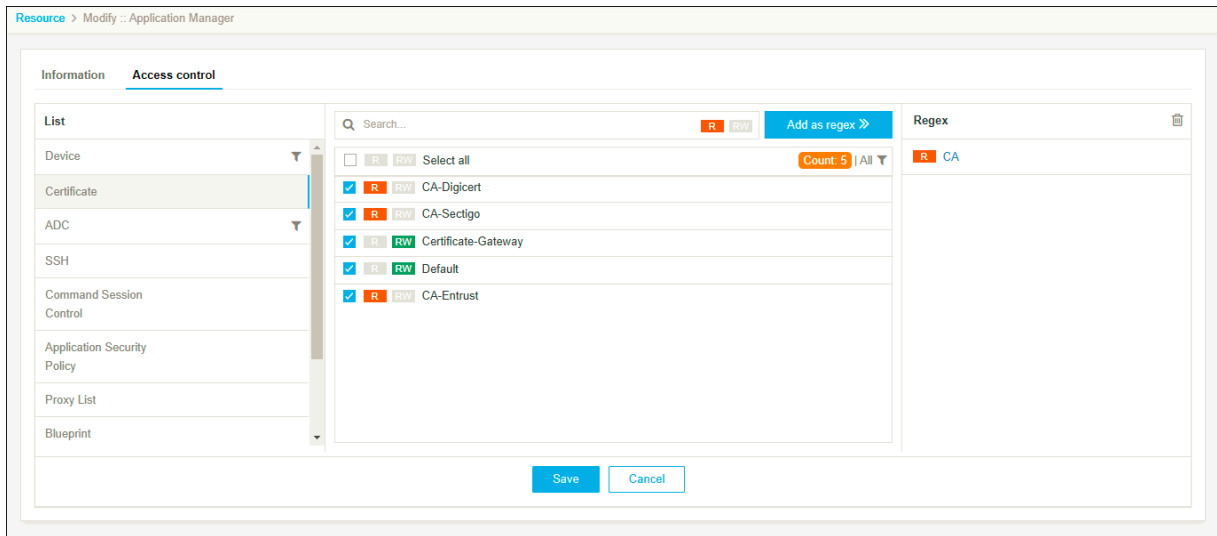
The screenshot shows a web interface for cloning a resource. At the top, a breadcrumb trail reads 'Resource > Cloning :: Techdoc'. Below this, there are two tabs: 'Information' (which is selected and underlined) and 'Access control'. Under the 'Information' tab, there are two input fields. The first is labeled '* Name' and contains the text 'Techdocs'. The second is labeled 'Description' and contains the text 'Techdoc'. At the bottom right of the form, there are two buttons: 'Save' and 'Cancel'.

6. The following table describes the options available on the Cloning page:

Field	Description
* Name	Enter the name of the resource.
Description	Enter a brief description of the resource and granular-level access associated with the resource. Note: You can enter a maximum of 255 words in the field.
Note: The asterisk (*) symbol indicates a mandatory field.	

7. Click **Save**.

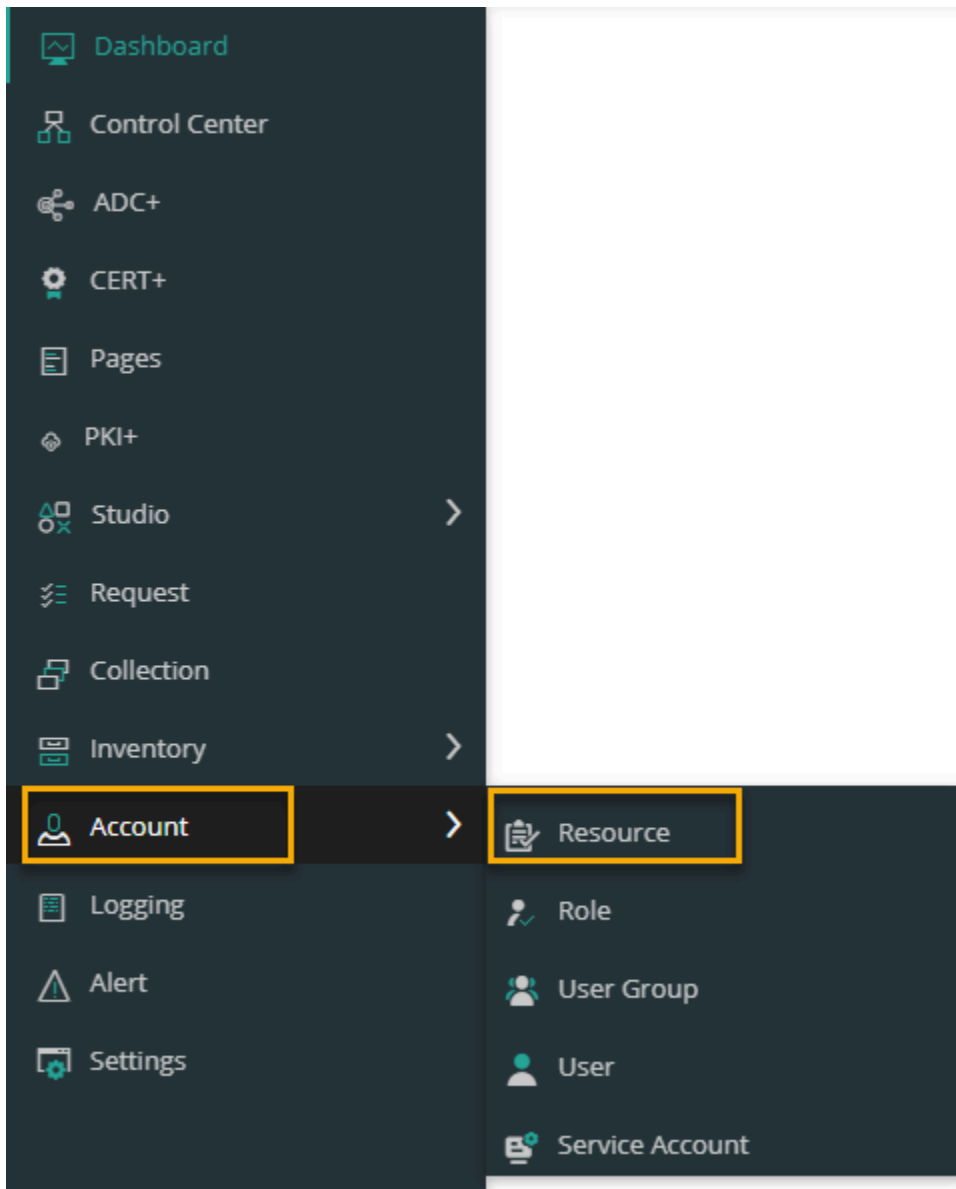
The resource is cloned and a pop-up message displays as **Resources has been cloned successfully**.



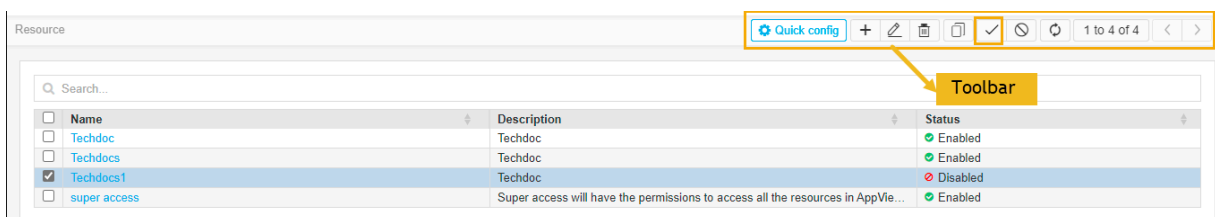
Enable a Resource

To enable a resource,

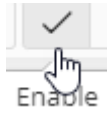
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **Account**, and then click **Resource** from the list.



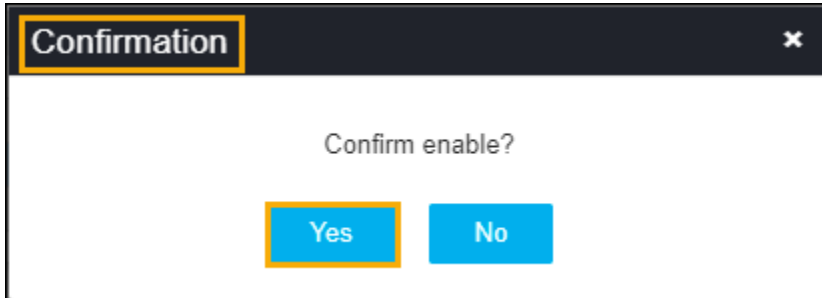
The **Resource** page appears.



4. In the resource inventory, select the check box against the resource you want to enable.



5. Click the **Enable** icon in the command bar to enable the resource.
6. A confirmation pop-up window, to confirm the operation.



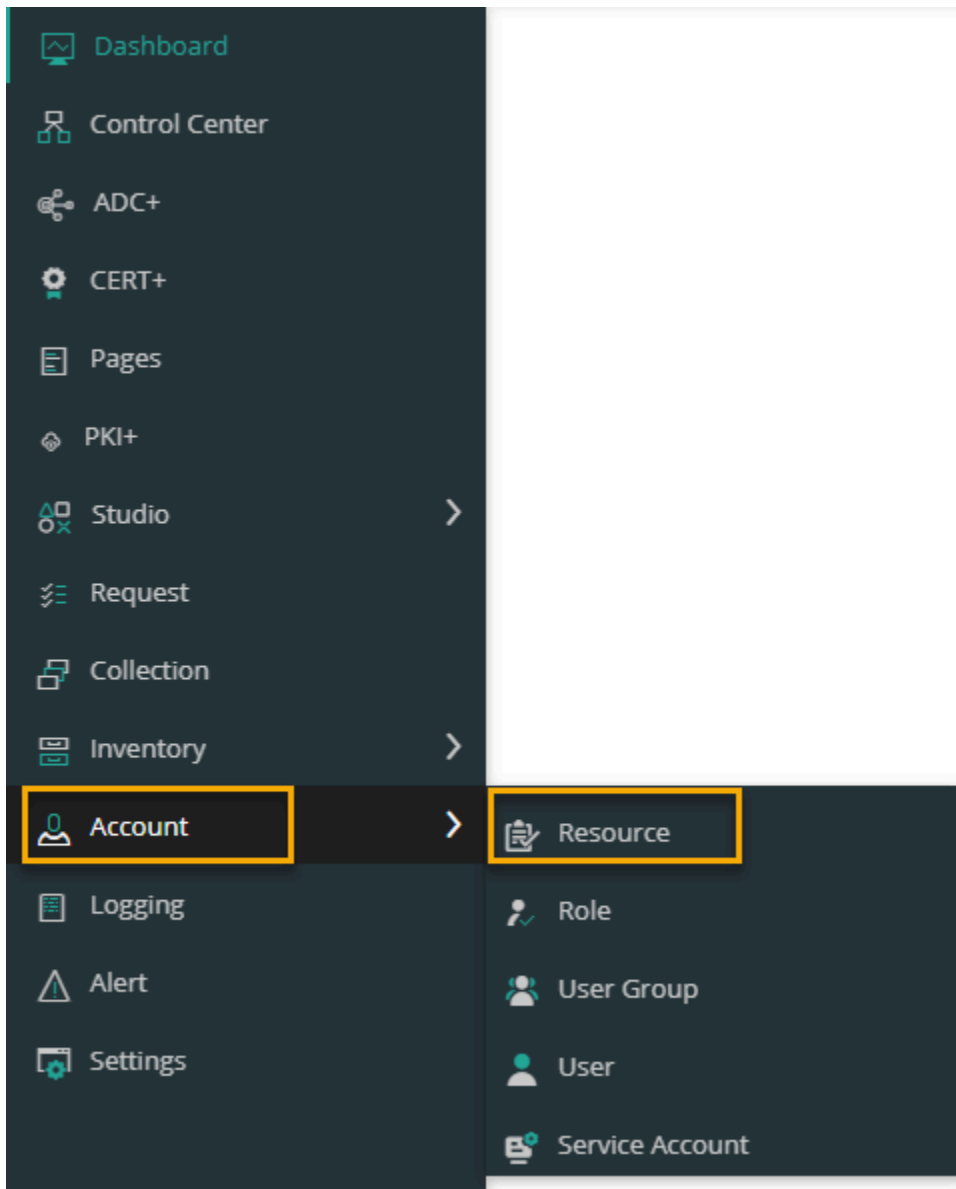
7. Click **Yes**.

The resource is enabled and a confirmation message displays as **Operation performed successfully**.

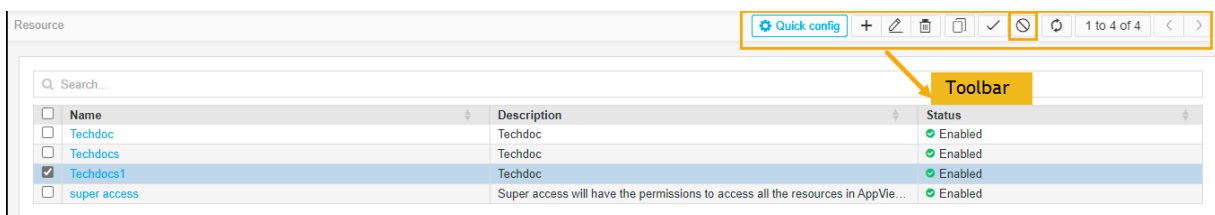
Disable a Resource

To disable a resource,

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. Navigate to **Account**, and then click **Resource** from the list.



The Resource page appears.



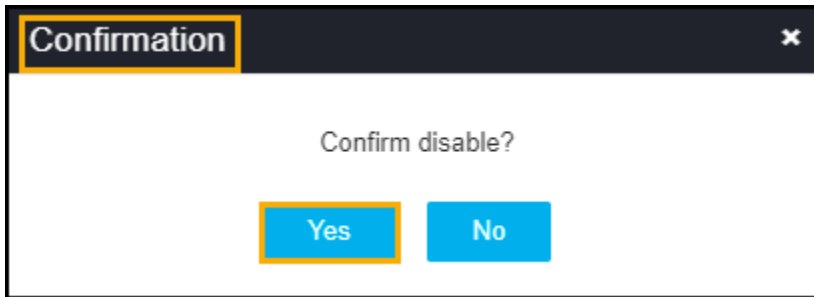
4. In the resource inventory, select the check box against the resource you want to disable.



5. Click the **Disable** icon in the command bar to disable the resource.

6.

A confirmation pop-up window, to confirm the operation.



7. Click **Yes**.

The resource is disabled and a confirmation message displays as **Operation performed successfully**.

Roles

- [Overview](#)
- [Create a Role](#)
- [Modify a Role](#)
- [Delete a Role](#)
- [Clone a Role](#)
- [Enable a Role](#)
- [Disable a Role](#)
- [Birthright Role](#)

Overview

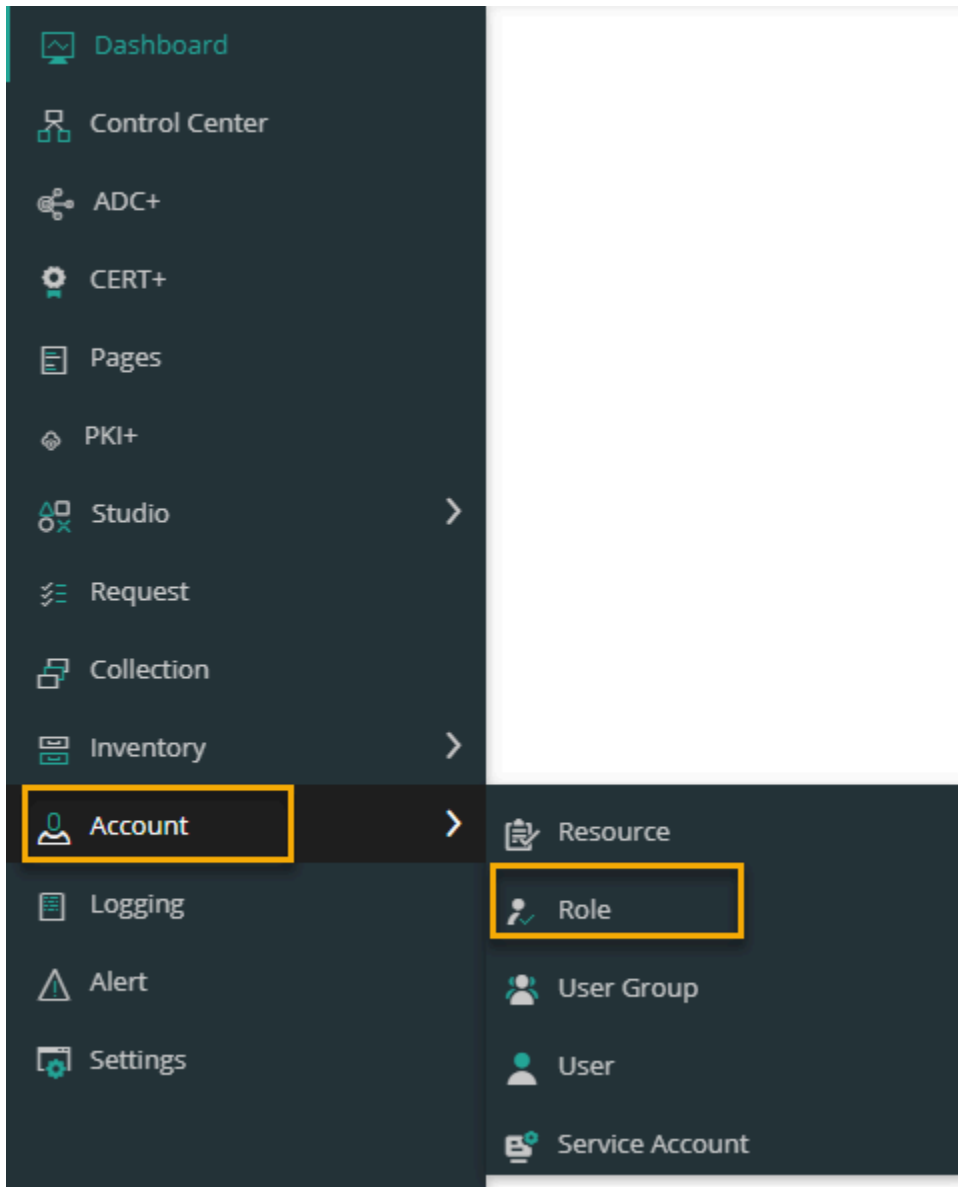
A set of permissions to execute specific tasks in the application is termed as Roles in AppViewX.

The roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role.

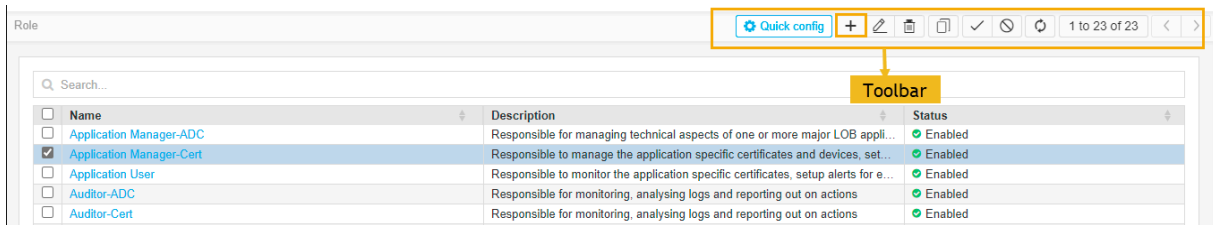
Create a Role

To create a role,

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. Navigate to **Account**, and then click **Role** from the list.



The **Role** page appears.



4. Click the  icon in the command bar to create a new role.

The **Add** page appears.

5. The following table describes the options available on the Add page:

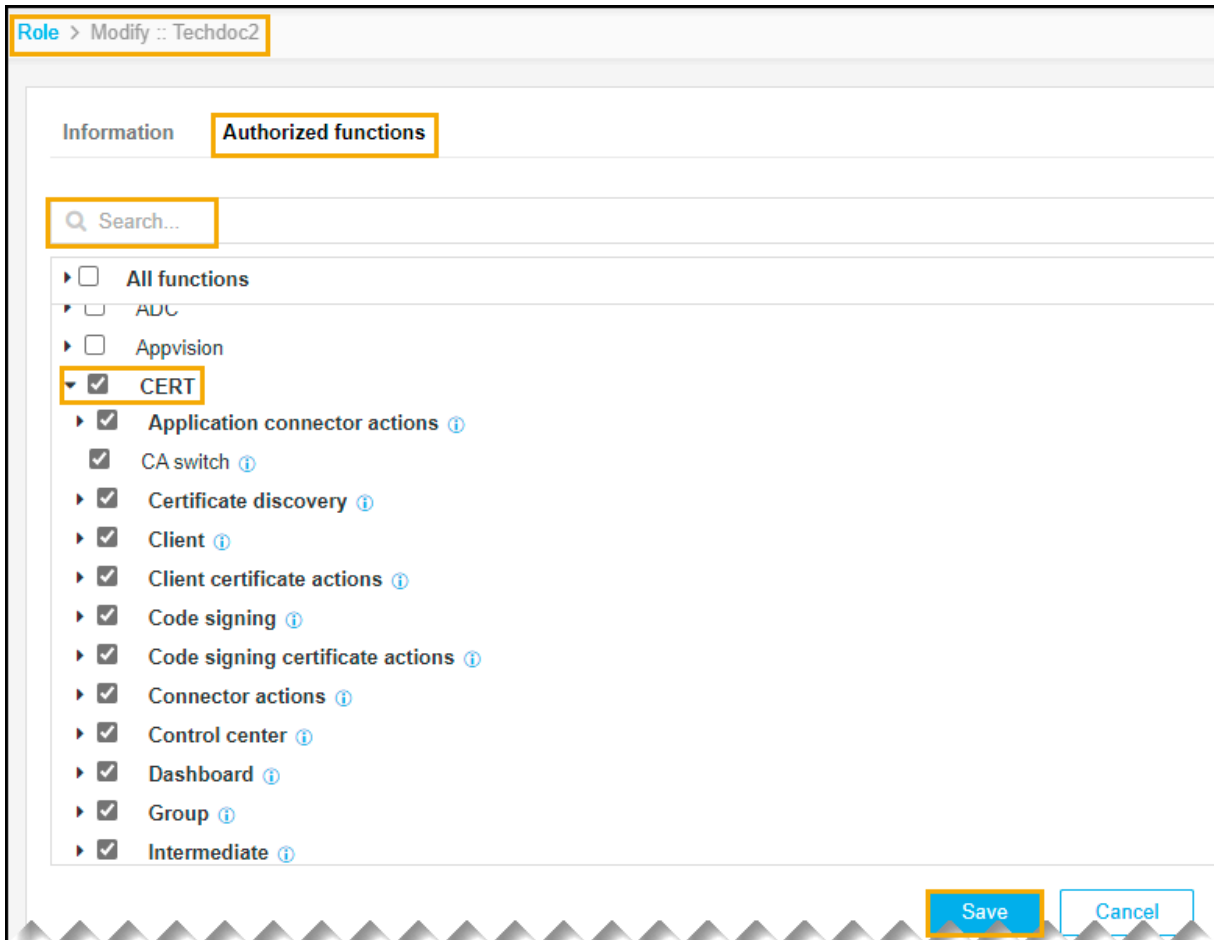
Field	Description
* Name	Enter the name of the role.
Description	Enter a brief description of the role and granular-level access associated with the resource. Note: You can enter a maximum of 255 words in the field.
 Note: The asterisk (*) symbol indicates a mandatory field.	

6. Click **Save**.

The pop-up message appears as **Role added successfully**.

7. Click the **Authorized functions** tab.

The **Authorized functions** page appears.



8. Select the checkboxes beside each of the functionalities that you want to associate with the role.

9. To assign the functions at a more granular level:

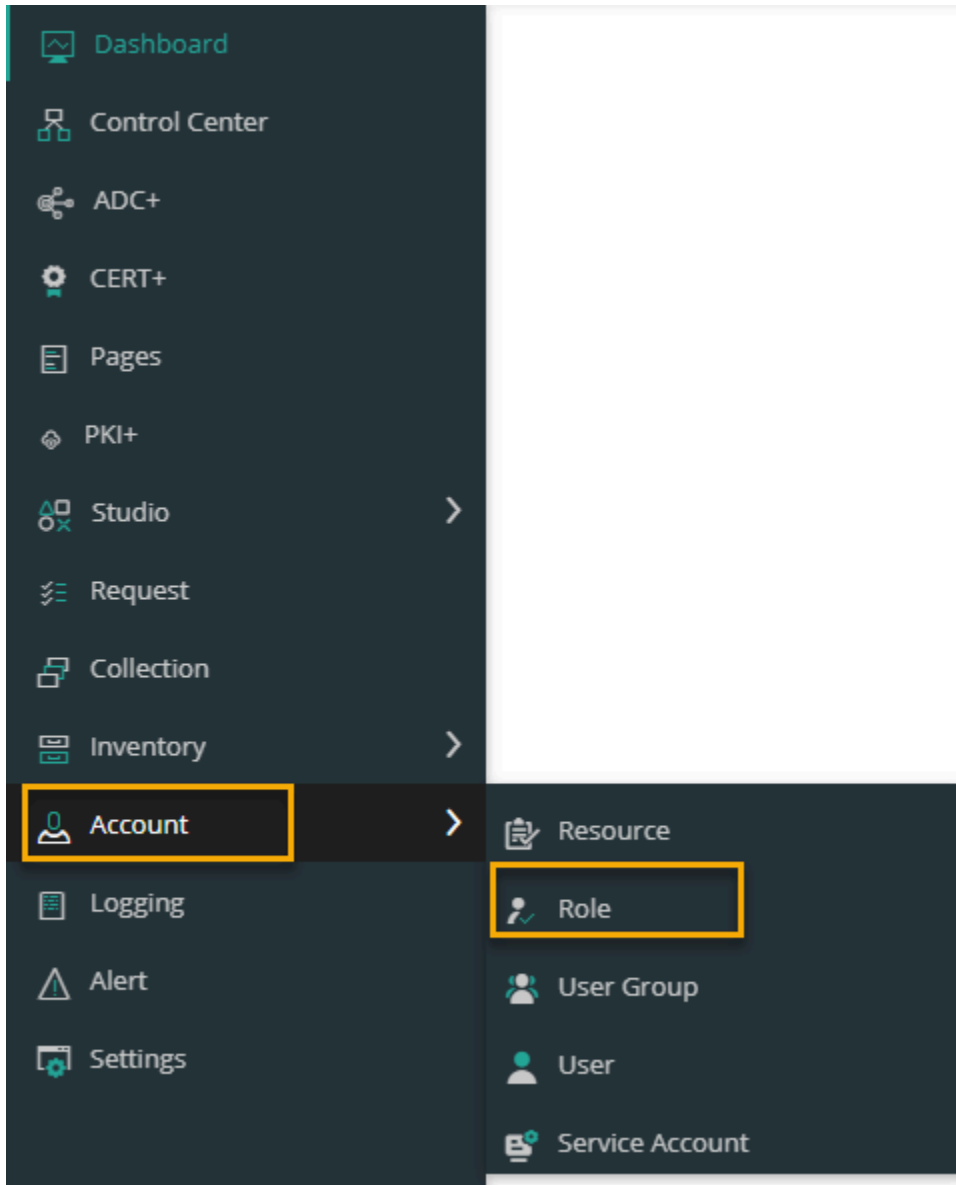
- Click the expand icon beside a function check box.
- Select the individual sub-options within that function.
- You can select **CERT**, which automatically assigns all sub-options or you can expand the **CERT** function and select only the sub-options you want to assign.

10. Click **Save**.

Modify a Role

To modify a role,

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. Navigate to **Account**, and then click **Role** from the list.



The **Role** page appears.

4. In the Roles list, select the check box beside the role you want to modify.



5. Click the icon in the command bar to modify a role.

The Modify screen appears.

6. Make the required changes in the Information and Authorized functions tabs.
7. Click **Save**.



Note: Fields that are grayed out, such as the Name field on the Information tab, cannot be edited.

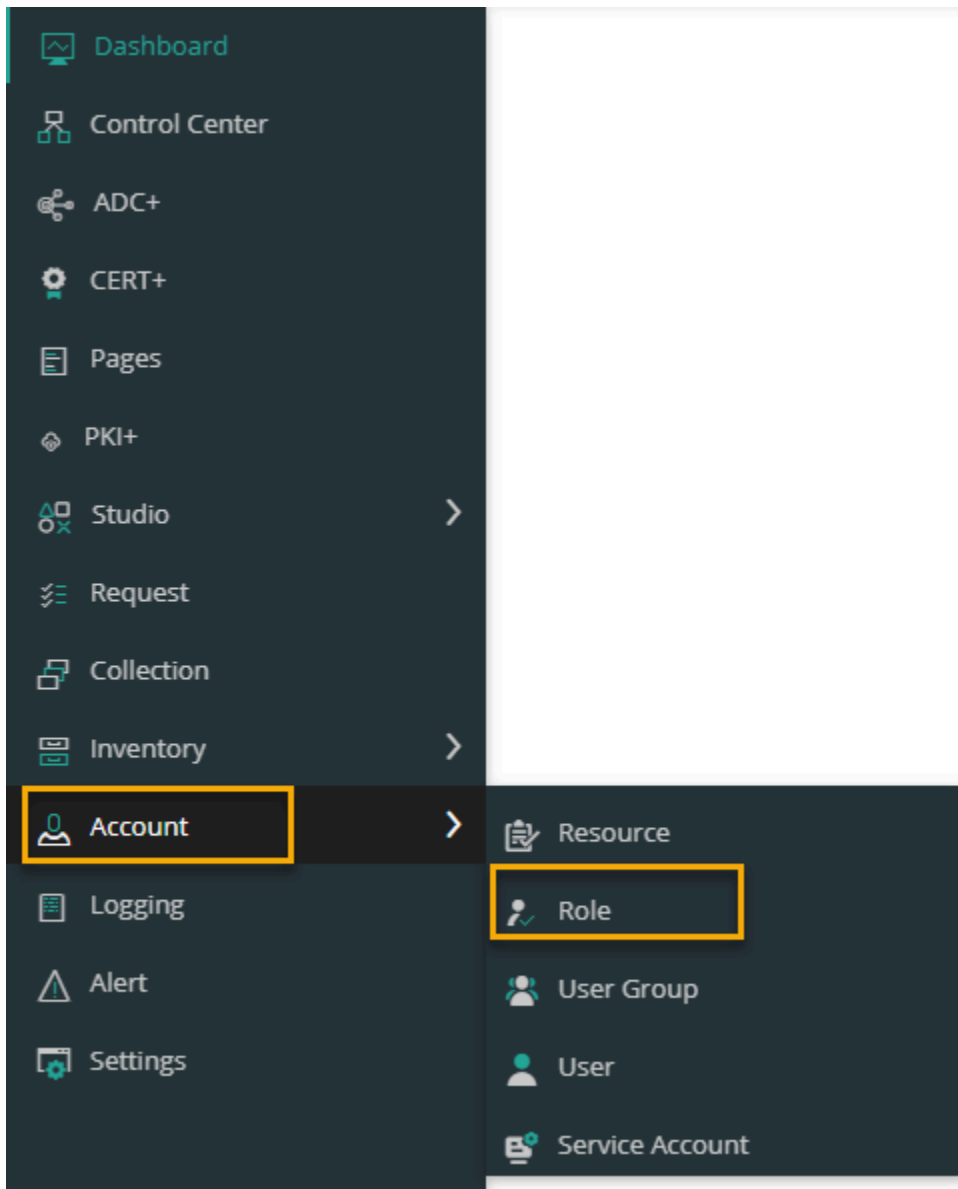
Delete a Role



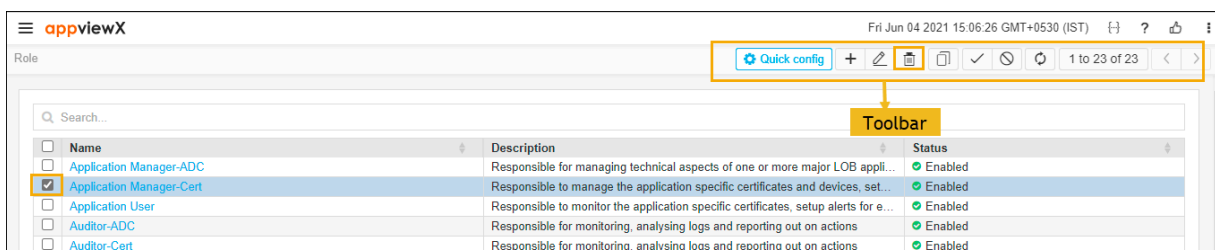
Note: A role that has active users belonging to it cannot be deleted.

To delete a role,

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. Navigate to **Account**, and then click **Role** from the list.



The **Role** page appears.



4. In the Roles list, select the check box beside the role you want to delete.



5. Click the  icon in the command bar to delete the role.

The confirmation pop-up window appears.

6. Click **Yes**.

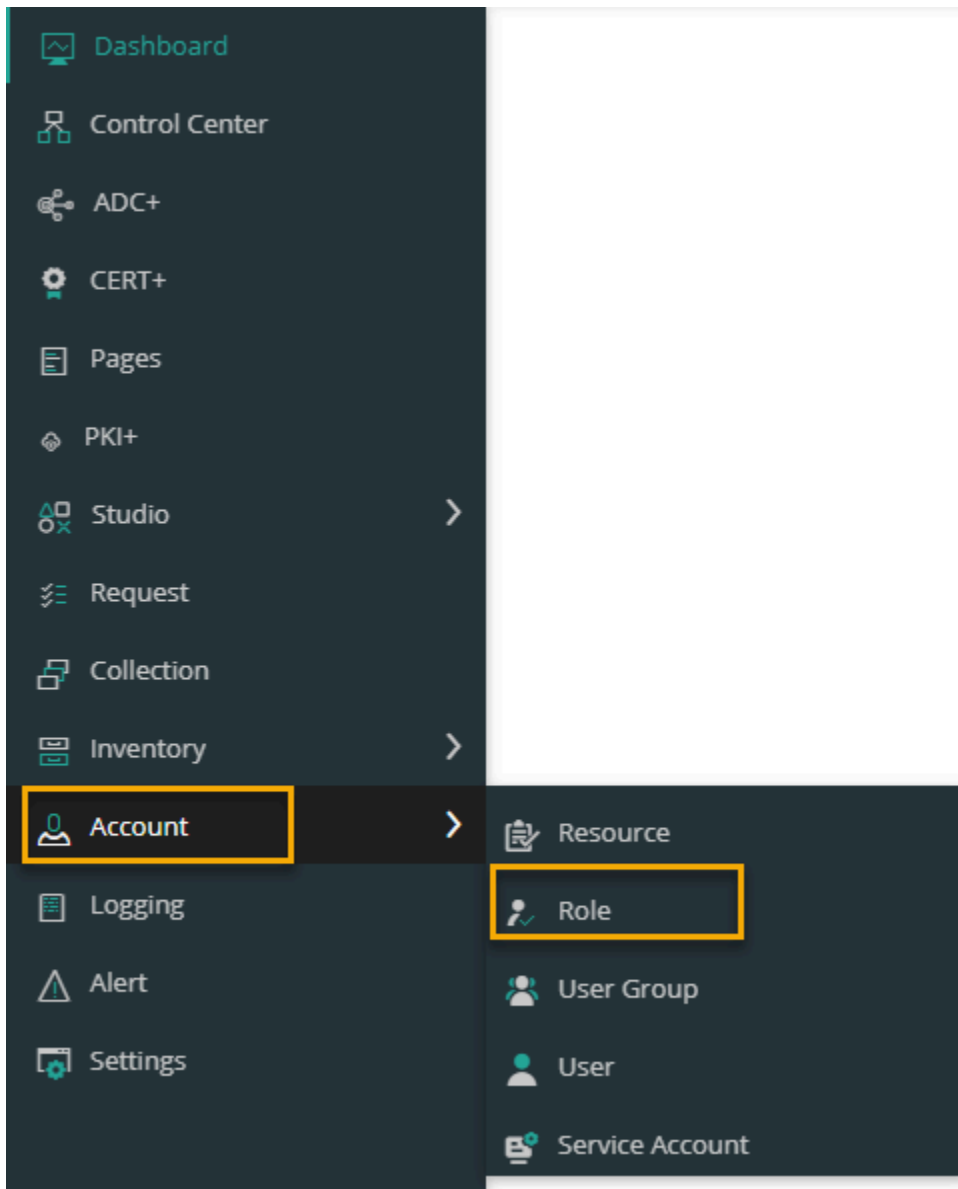
The pop-up message appears as Operation performed successfully.

Clone a Role

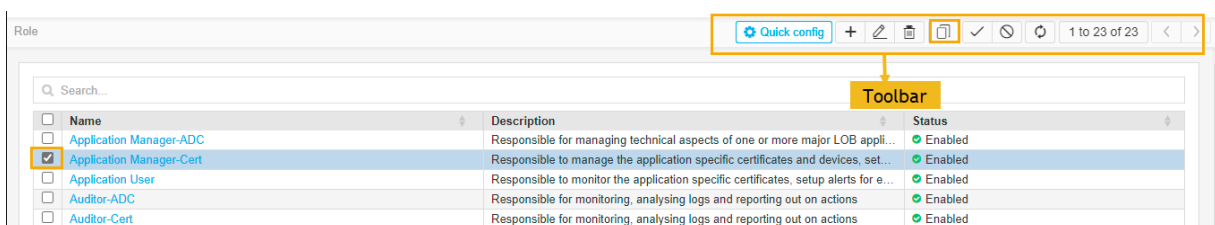
The Clone a role option allows you to create an exact copy of an existing role with a different name. The user can modify the permissions and tasks that can be performed while cloning a role.

To create a clone,

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. Navigate to **Account**, and then click **Role** from the list.



The **Role** page appears.



4. In the Roles list, select the check box beside the role you want to clone.



5. Click the **clone icon** in the command bar to clone the role.

The selected Cloning page appears.

Role > Cloning :: Techdoc2

Information Authorized functions

* Name Techdoc3

Description Techdoc test.

Save Cancel

The following table describes the options available on the Cloning page:

Field	Description
* Name	Enter the name of the resource.
Description	Enter a brief description of the resource and granular-level access associated with the role. Note: You can enter a maximum of 255 words in the field.
Note: The asterisk (*) symbol indicates a mandatory field.	

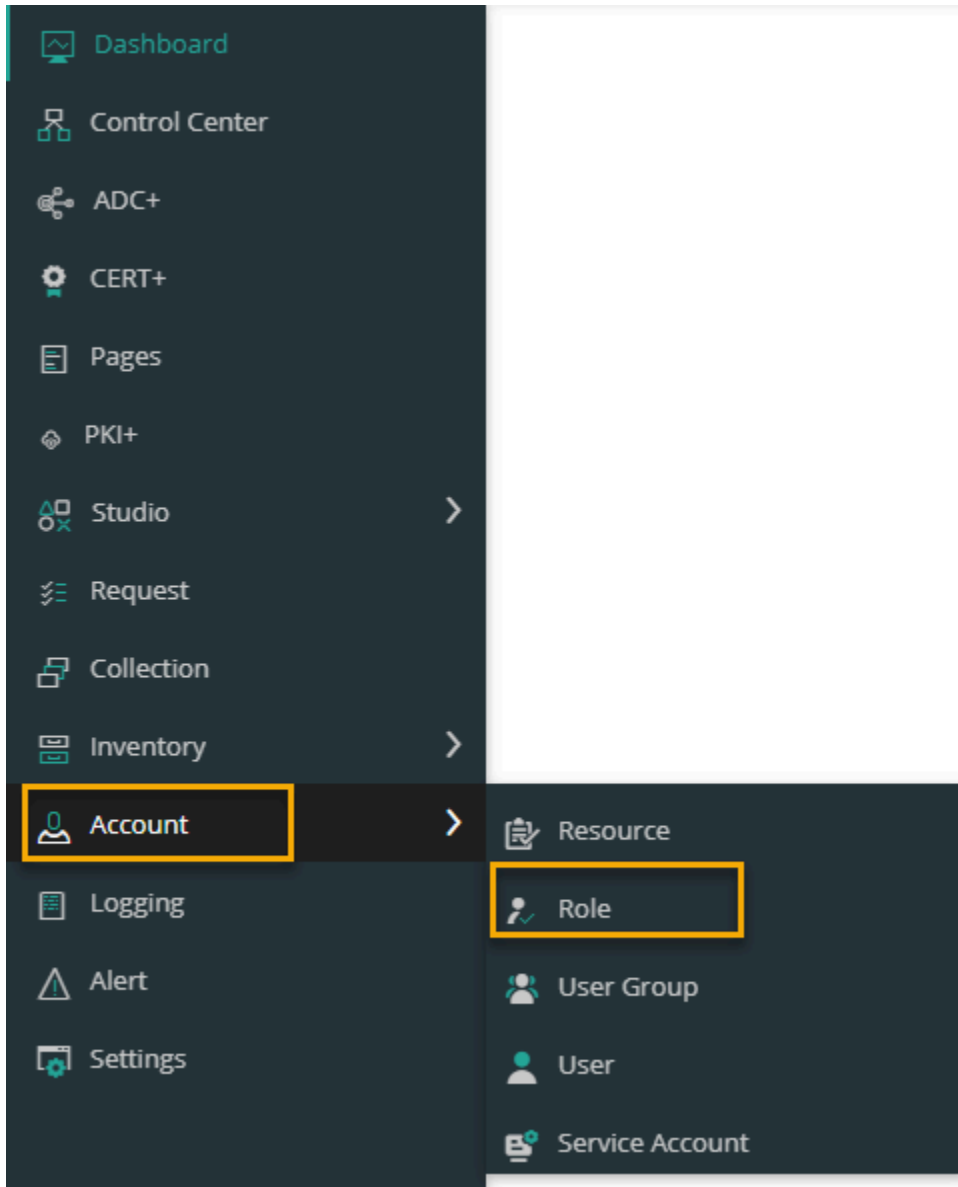
6. Click **Save**.

The role is cloned and a pop-up message displays as **Role has been cloned successfully**.

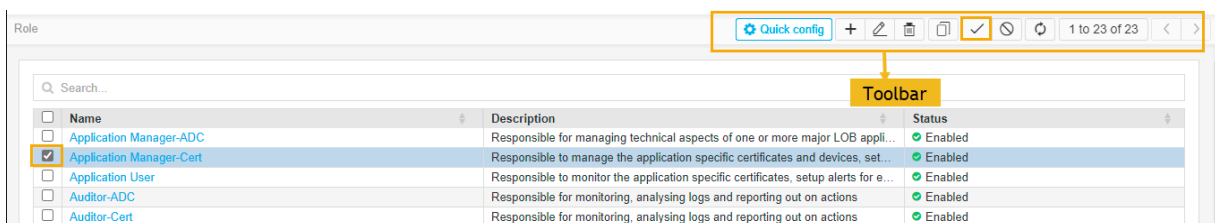
Enable a Role

To enable a role,

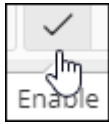
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **Account**, and then click **Role** from the list.

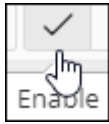


The **Role** page appears.

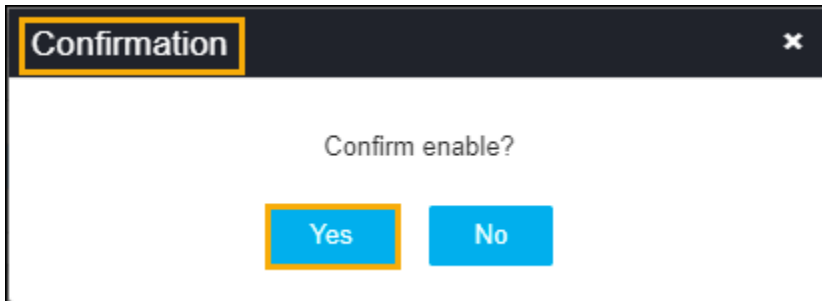


4. In the role inventory, select the check box against the role you want to enable.



5. Click the  icon in the command bar to enable the role.

6. A confirmation pop-up window, to confirm the operation.



7. Click **Yes**.

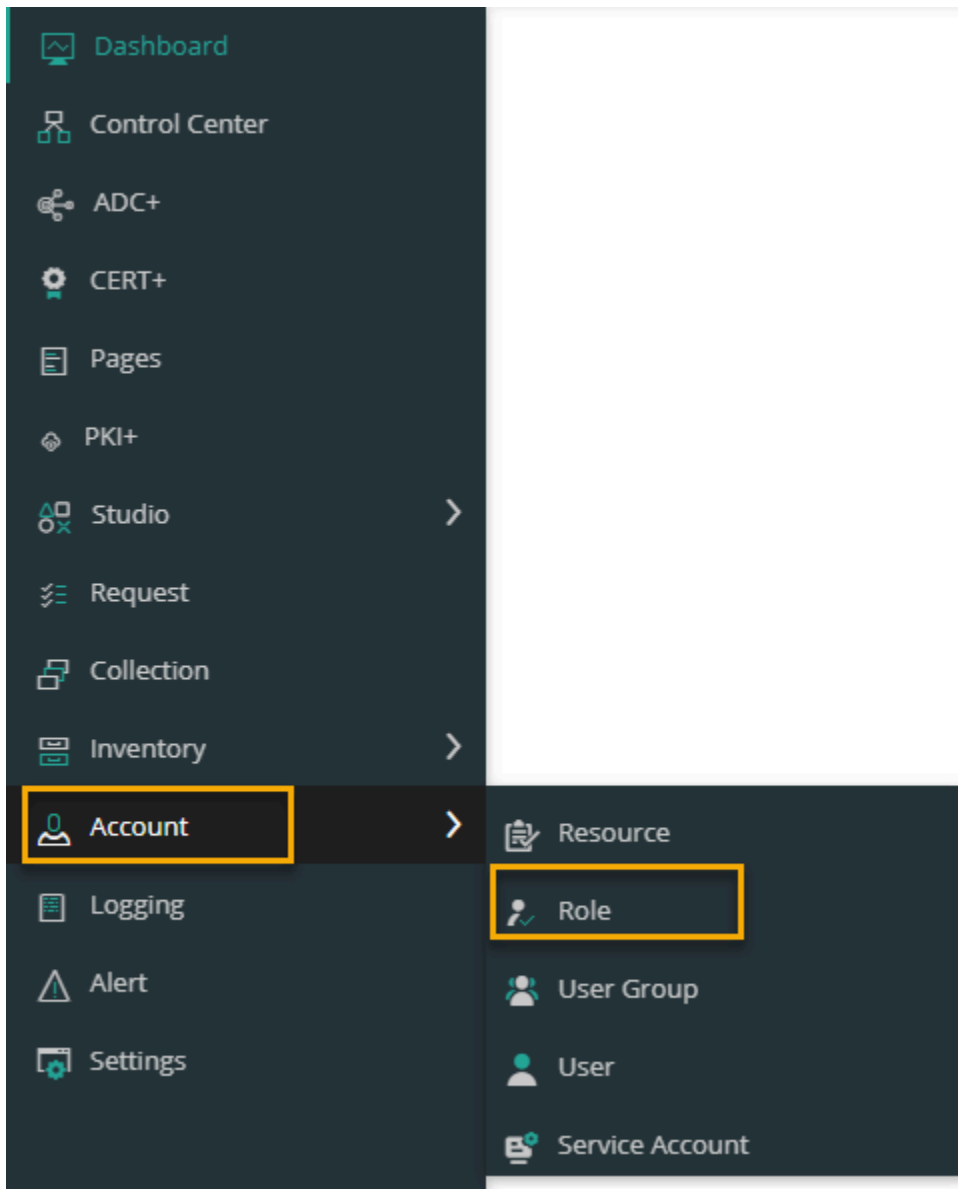
The role is enabled and a confirmation message displays as **Operation performed successfully**.

Disable a Role

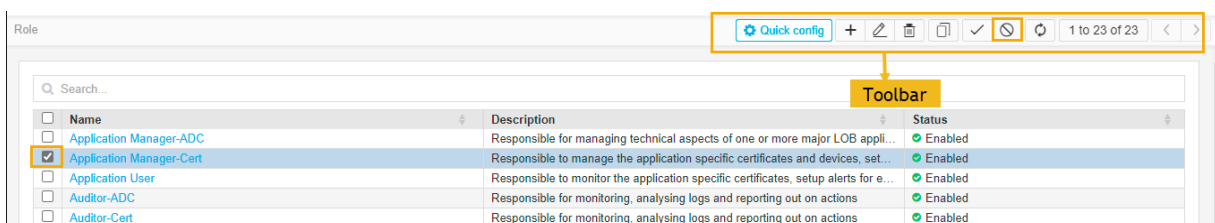
You cannot disable a role that has active users in it. The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role,

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. Navigate to **Account**, and then click **Role** from the list.



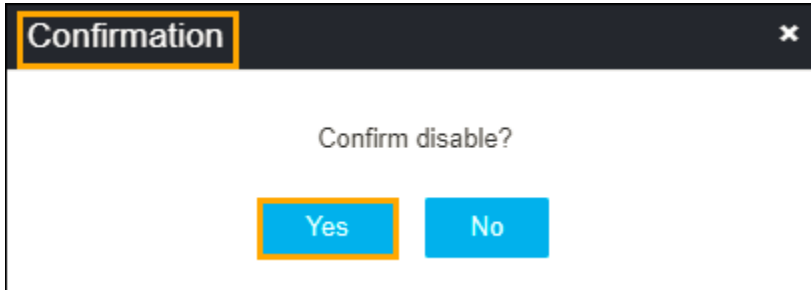
The **Role** page appears.



4. In the role inventory, select the check box against the role you want to disable.



5. Click the  icon in the command bar to disable the role.
6. A confirmation pop-up window, to confirm the operation.



7. Click **Yes**.

The role is enabled and a confirmation message displays as **Operation performed successfully**.

Birthright Role

When the Admin enables the Birthright role feature, all new users who log into the product will be provided with a pre-defined set of customizable functions.

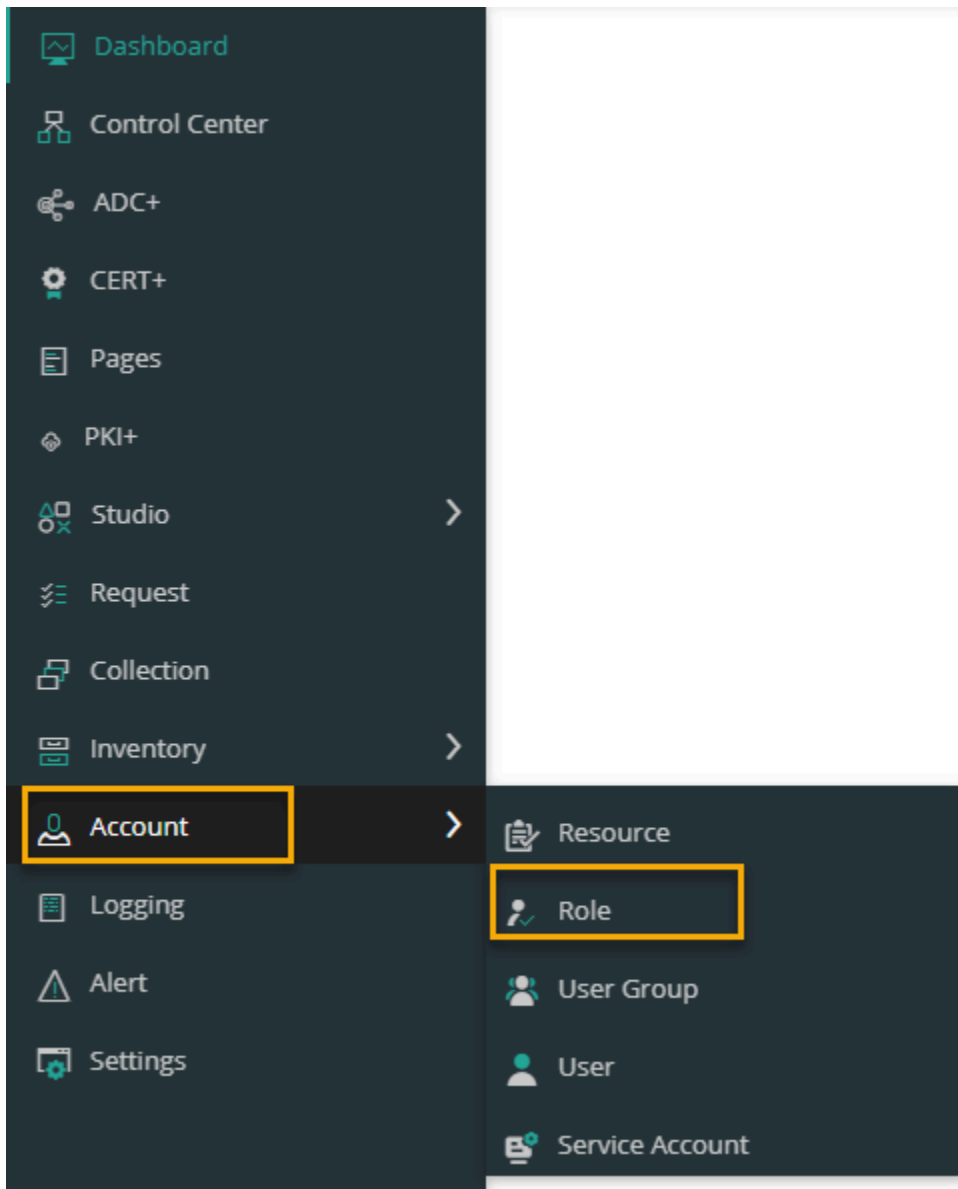
When this role is enabled, the admin can create and assign a dedicated user group with pre-defined roles and resources and set it as the Birthright role.

Whenever a new user logs in, the user will be mapped with roles and resources specified in that particular user group.

To configure the Birthright role,

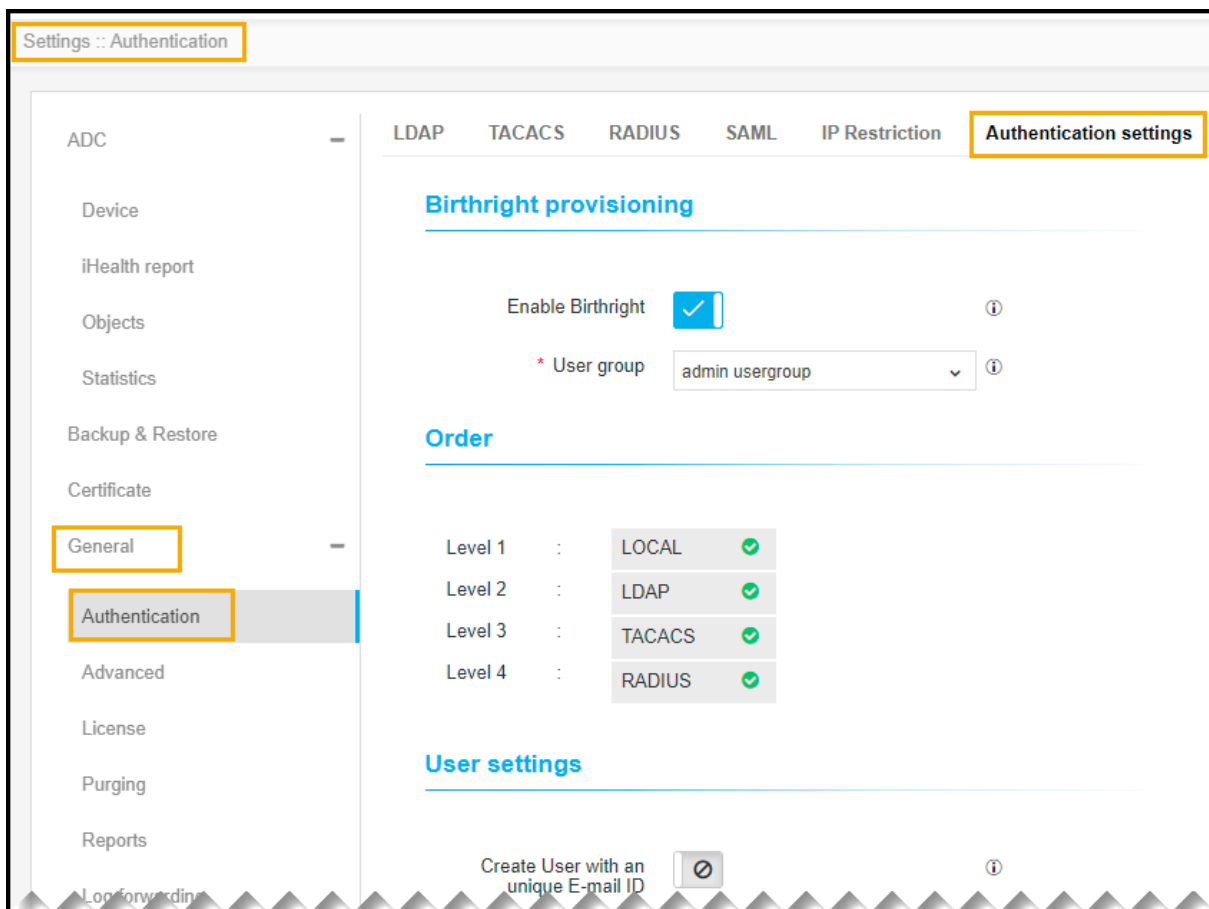
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.



3. Click **Settings**.
4. Navigate to **General**, and then select **Authentication**.
5. Click **Authentication Settings**.

Displays the available options on the page.



6. The following table describes the options available on the Authentication settings page:

Options	Description								
Birthright provisioning	- To enable birthright provisioning for new users who log into the system with a predefined set of permissions. * User group - Select the user group from the drop-down list.								
Order	By default, all the associated orders are selected.								
User settings	Enter/Enable the following settings: <table> <tr> <th>Options</th><th></th></tr> <tr> <td>Create a User with a unique E-mail ID</td><td>Enable the toggle key, to ensure that all the users</td></tr> <tr> <td>Create User on Authorization Failure</td><td>Enable the toggle key, to create a user even if auth</td></tr> <tr> <td>Session Timeout</td><td>Allows users to set the idle web session timeout lin</td></tr> </table>	Options		Create a User with a unique E-mail ID	Enable the toggle key, to ensure that all the users	Create User on Authorization Failure	Enable the toggle key, to create a user even if auth	Session Timeout	Allows users to set the idle web session timeout lin
Options									
Create a User with a unique E-mail ID	Enable the toggle key, to ensure that all the users								
Create User on Authorization Failure	Enable the toggle key, to create a user even if auth								
Session Timeout	Allows users to set the idle web session timeout lin								

Options	Description
	Options Note: The idle web session timeout is calculated in
Node settings	Enter the node password whenever AppViewX node password gets changed.  Note: The password entered in the Node Password field must be the same as the node password.
 Note: The asterisk (*) symbol indicates a mandatory field.	

7. Click **Save**.

User Group

- [Overview](#)
- [Create a User Group](#)
- [Modify a User Group](#)
- [Delete a User Group](#)
- [Clone a User Group](#)
- [Enable a User Group](#)
- [Disable a User Group](#)

Overview

A user group is a group of individuals that have access to the same roles and resources. When you associate a role and resource with a user group, the users within that user group are granted all of the role's and resource's corresponding privileges and permissions.

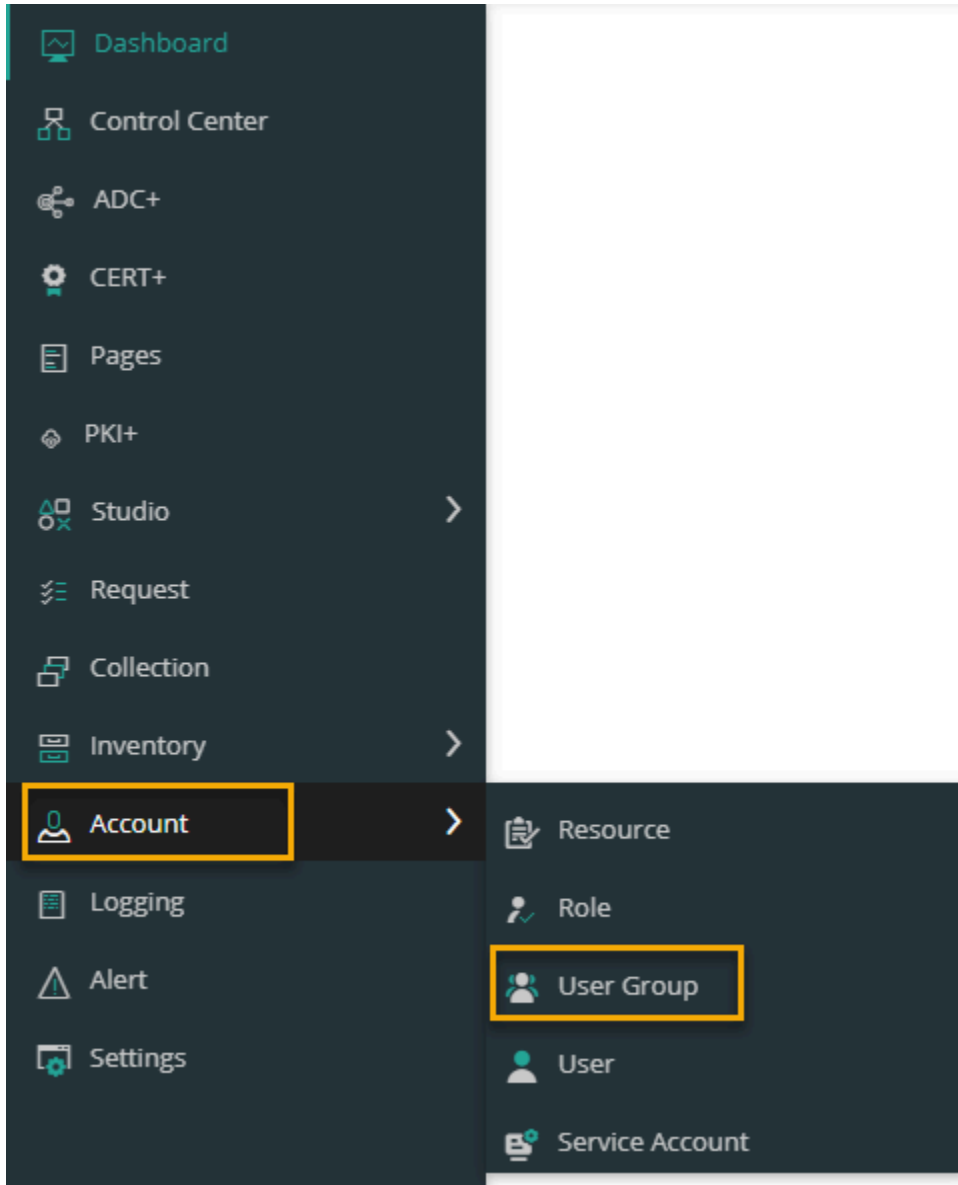


Note: You can associate the roles and resources only with the User groups.

Create a User Group

To create a user group,

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. Navigate to **Account**, and then click **User Group** from the list.



The **User Group** page appears.

User group		Quick config + ✎ 🗑 📄 ✓ 🔒 🔄 1 to 2 of 2				
Search...						
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin usergroup	Admin user group exi...	admin	super access	Default Rule	🟢 Enabled
☐	cert_acf_UnAssign_S...	sample	cert_acf_UnAssign_ServerCert_RenewC...	super access		🟢 Enabled



4. Click the  icon in the command bar to create a new user group.

The **Add** page appears.

User group > Add

Information

Roles

Resources

* Name

Techdoc

Description

Techdoc test.

242 remaining

Save

Cancel

The following table describes the options available on the User Group page:

Field	Description
* Name	Enter the name of the user group.
Description	Enter a brief description of the user group and granular-level access associated with the user group.  Note: You can enter a maximum of 255 words in the field.

 **Note:** The asterisk (*) symbol indicates a mandatory field.

5. Click **Save**.

The pop-up message appears as **the User group added successfully. Please associate the roles and resources to perform the concerned operations.**

6. Click the **Roles** tab.

Role name	Description	Status
☒ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Application User	Responsible to monitor the application specific certificates, setup alerts for expiry and acce...	Enabled
☒ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☒ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☒ Traffic Manager	Responsible to perform traffic management operations and Monitors specific app health wit...	Enabled
☒ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB applications,	Enabled
☒ admin	admin	Enabled
☒ Executive Director-Cert	AppViewX provides organizations with holistic, business-level visibility across cloud and on...	Enabled
☒ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☒ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Portal User	Responsible for Self-servicing and accessing automation flows via Catalogue	Enabled
☒ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☒ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☒ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☒ Security Manager	This role grants users complete access to all objects on the system	Enabled
☒ DevOps Manager	Responsible for managing a DevOp team; they may write applications, and responsible for...	Enabled
☒ Application Manager-Cert	Responsible to manage the application specific certificates and devices, setup alerts for ex...	Enabled
☒ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☒ USERS/Read-Only Admins	This role grants users complete access to all objects on the system.Cannot Create/Remov...	Enabled
☒ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☒ cert_and_UnAssign_Server/Cert_RenewCertificate	cert_and_UnAssign_Server/Cert_RenewCertificate	Enabled
☒ Techdoc	Techdoc test.	Enabled
☒ Techdoc2	Techdoc test.	Enabled

7. Select the checkbox against each role you want to assign to the new user group.

8. Click **Save**.

The pop-up message appears as **Operation performed successfully.**

9. Click the **Resources** tab.

Resource name	Description	Status
☒ super access	Super access will have the permissions to access all the resources in AppViewX.	Enabled
☐ Techdocs	Techdoc	Disabled
☐ Techdocs1	Techdoc	Disabled

10. Select the checkbox against each resource you want to assign to the new user group.



Note: A user can be assigned to more than one role and resource in the system. A user assigned to more than one role or resource has all of the permissions of all of the roles and resources to which the user is assigned. If one resource has only Read access to a component and another resource has Read/Write access to the same component, the higher-level access permissions (Read/Write) takes precedence and the user will have Read/Write access.

11. Click **Save**.

The pop-up message appears as **Operation performed successfully**.

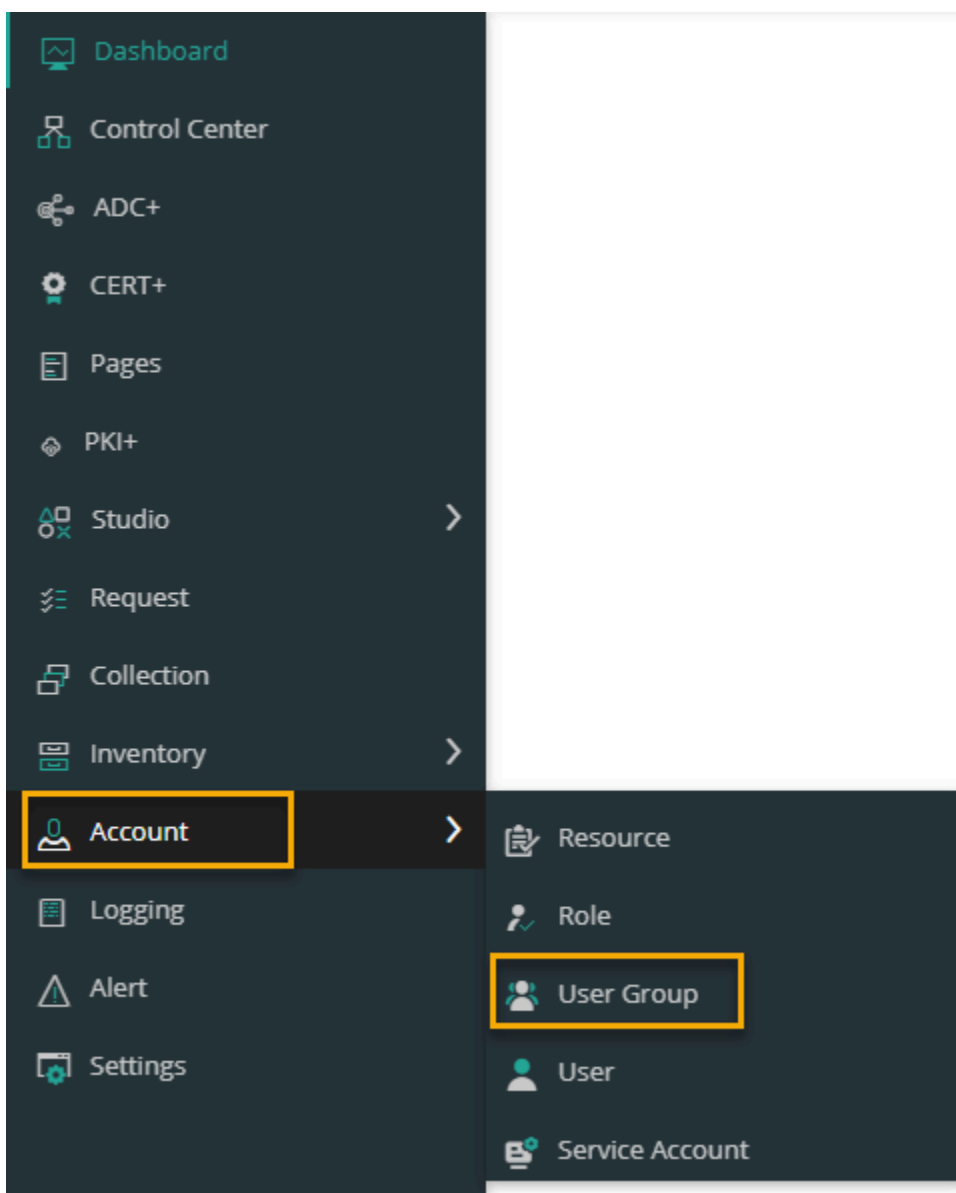
Modify a User Group

To modify a user group,

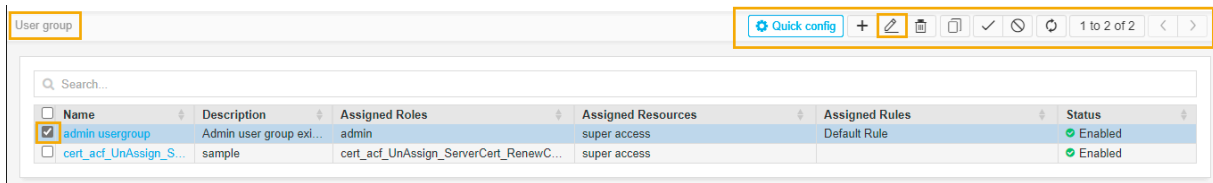
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Navigate to **Account**, and then click **User Group** from the list.



The **User Group** page appears.



4. Click the  icon in the command bar to modify a user group.

The **Modify** page appears.

The following table describes the options available on the User Group page:

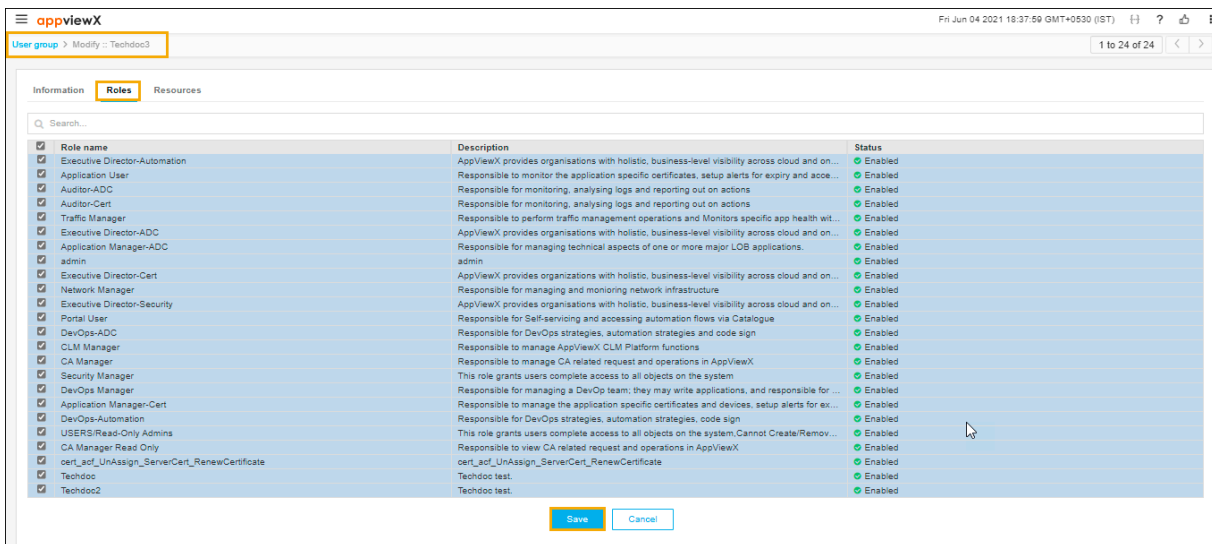
Field	Description
Name	Edit the name of the user group. Note: You cannot modify the name for the user group.
Description	Modify a brief description of the user group and granular-level access associated with the user group if required.  Note: You can enter a maximum of 255 words in the field.

Field	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

5. Click **Save**.

The pop-up message appears as **User group information updated successfully**.

6. Click the **Roles** tab.



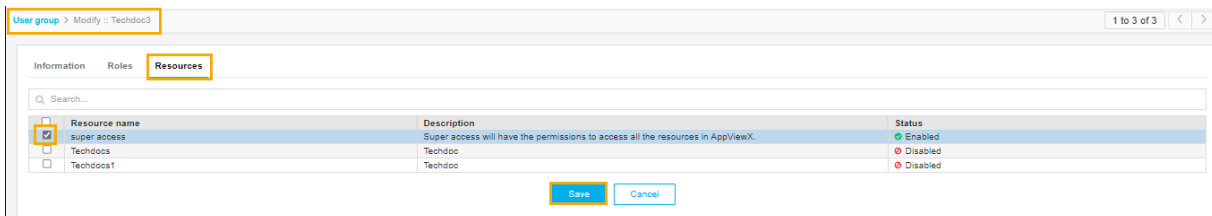
Role name	Description	Status
☒ Executive Director-Automation	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Application User	Responsible to monitor the application specific certificates, setup alerts for expiry and acce...	Enabled
☒ Auditor-ADC	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☒ Auditor-Cert	Responsible for monitoring, analysing logs and reporting out on actions	Enabled
☒ Traffic Manager	Responsible to perform traffic management operations and Monitors specific app health wit...	Enabled
☒ Executive Director-ADC	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Application Manager-ADC	Responsible for managing technical aspects of one or more major LOB applications.	Enabled
☒ admin	admin	Enabled
☒ Executive Director-Cert	AppViewX provides organizations with holistic, business-level visibility across cloud and on...	Enabled
☒ Network Manager	Responsible for managing and monitoring network infrastructure	Enabled
☒ Executive Director-Security	AppViewX provides organisations with holistic, business-level visibility across cloud and on...	Enabled
☒ Portal User	Responsible for Self-servicing and accessing automation flows via Catalogue	Enabled
☒ DevOps-ADC	Responsible for DevOps strategies, automation strategies and code sign	Enabled
☒ CLM Manager	Responsible to manage AppViewX CLM Platform functions	Enabled
☒ CA Manager	Responsible to manage CA related request and operations in AppViewX	Enabled
☒ Security Manager	This role grants users complete access to all objects on the system	Enabled
☒ DevOps Manager	Responsible for managing a DevOps team; they may write applications, and responsible for...	Enabled
☒ Application Manager-Cert	Responsible to manage the application specific certificates and devices, setup alerts for ex...	Enabled
☒ DevOps-Automation	Responsible for DevOps strategies, automation strategies, code sign	Enabled
☒ USERS/Read-Only Admins	This role grants users complete access to all objects on the system.Cannot Create/Remov...	Enabled
☒ CA Manager Read Only	Responsible to view CA related request and operations in AppViewX	Enabled
☒ cert_adf_UnAssign_ServerCert_RenewCertificate	cert_adf_UnAssign_ServerCert_RenewCertificate	Enabled
☒ Techdoc	Techdoc test.	Enabled
☒ Techdoc2	Techdoc test.	Enabled

7. Select additional roles or unselect existing roles for the User group.

8. Click **Save**.

The pop-up message appears as **Operation performed successfully**.

9. Click the **Resources** tab.



Resource name	Description	Status
☒ super access	Super access will have the permissions to access all the resources in AppViewX.	Enabled
☐ Techdocs	Techdoc	Disabled
☐ Techdocs1	Techdoc	Disabled

10. Select additional resources or unselect existing resources for the User group.

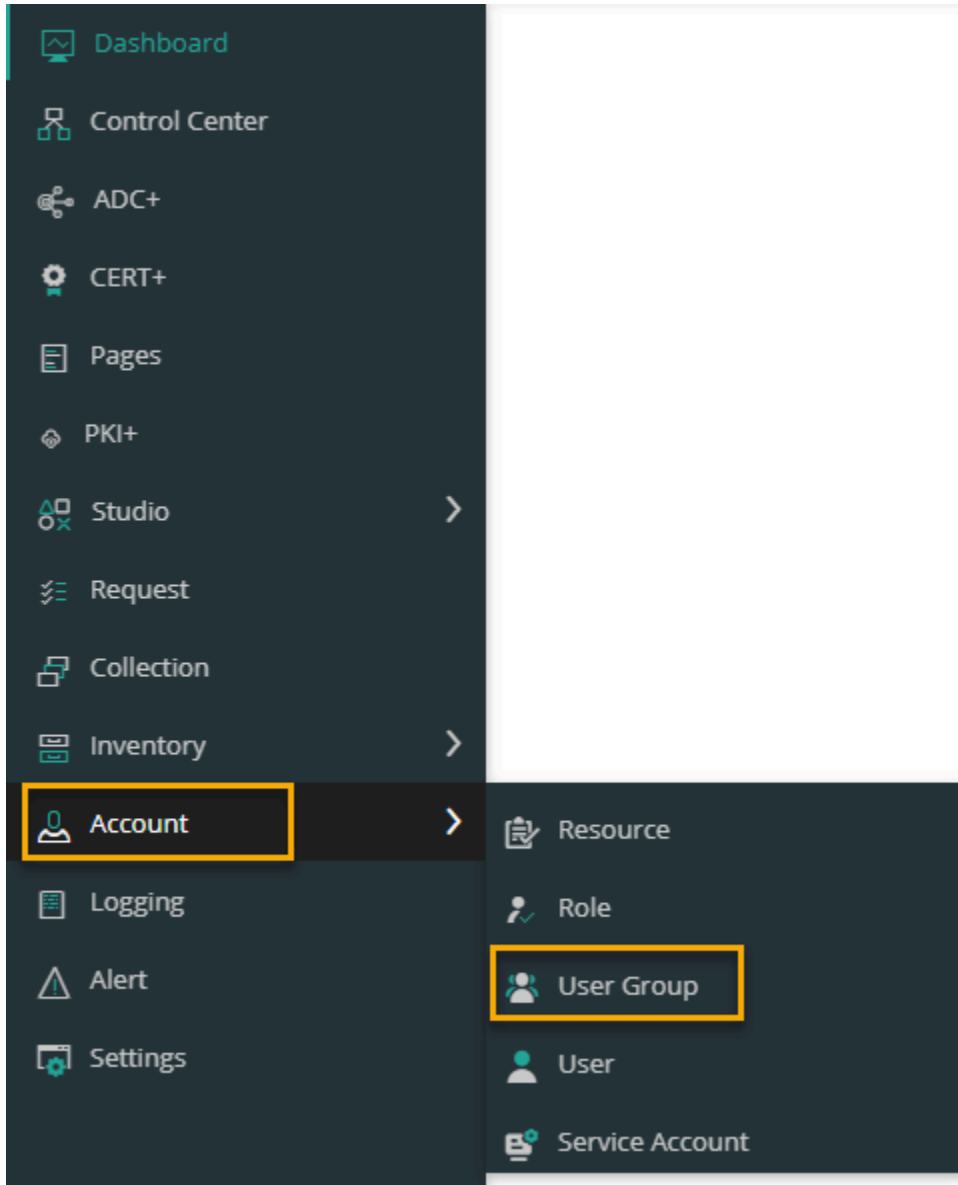
11. Click **Save**.

The pop-up message appears as **Operation performed successfully**.

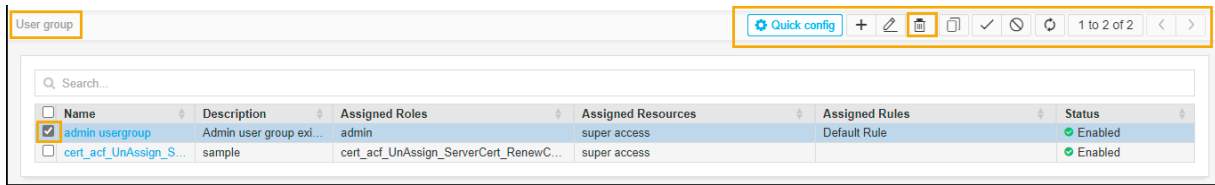
Delete a User Group

To delete a user group,

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. Navigate to **Account**, and then click **User Group** from the list.



The **User Group** page appears.



☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin_usergroup	Admin user group exi...	admin	super access	Default Rule	Enabled
☐	cert_acf_UnAssign_S...	sample	cert_acf_UnAssign_ServerCert_RenewC...	super access		Enabled

4. In the **User Group** list, select the check box beside the role you want to delete.



5. Click the  icon in the command bar to delete the User Group.

The confirmation pop-up window appears.

6. Click **Yes**.

The pop-up message appears as Operation performed successfully.

Clone a User Group

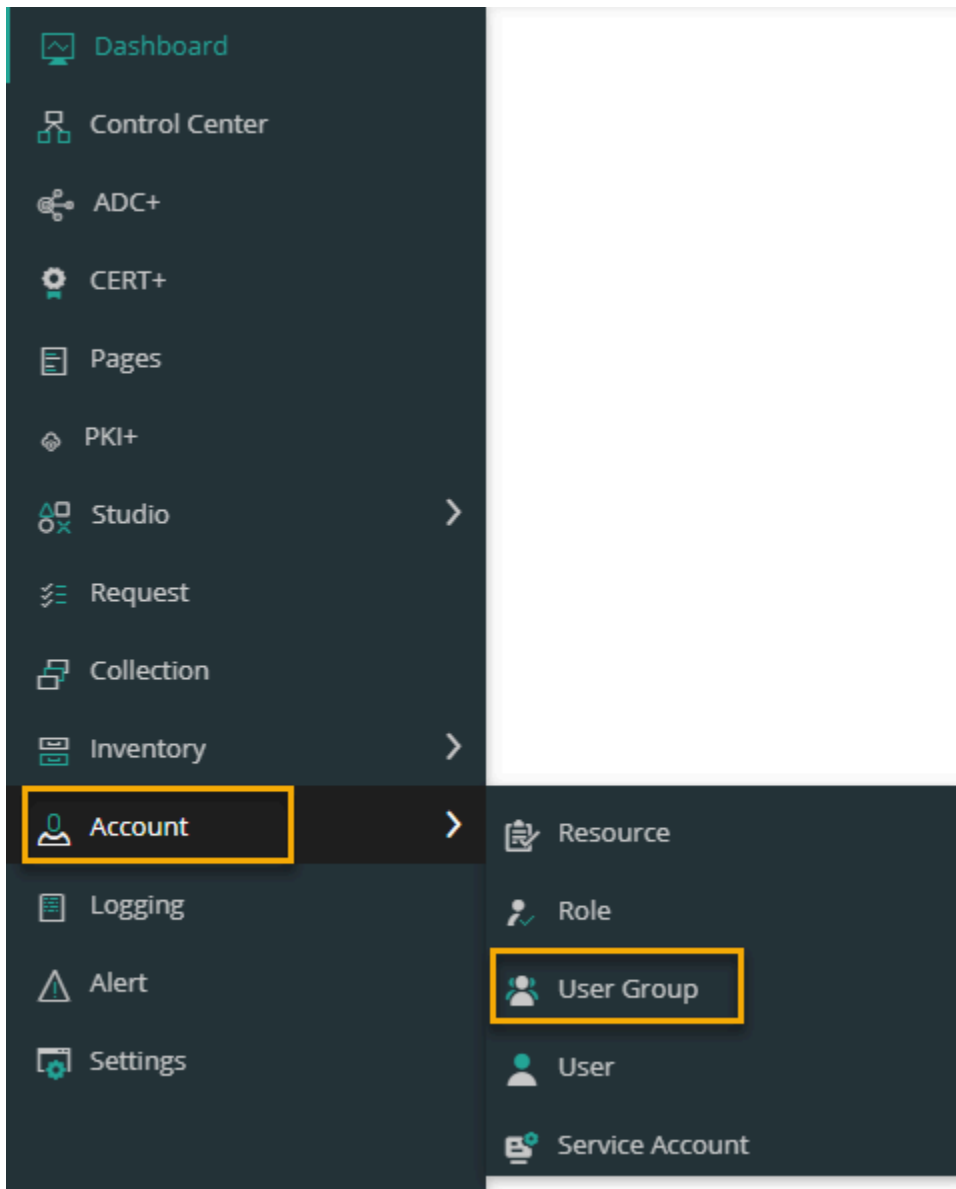
The Clone a user group option allows you to create an exact copy of an existing user group with a different name. You can modify the roles and resources association while cloning a role.

To create a clone,

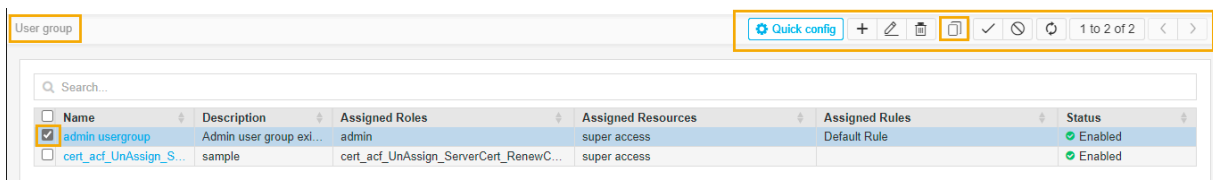
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Navigate to **Account**, and then click **User Group** from the list.



The **User Group** page appears.



4. In the user group inventory, select the check box against the user group you want to clone.



5. Click the **icon** in the command bar to clone the user group.

The selected Cloning page appears.

User group > Cloning :: Techdoc3

Information Roles Resources

* Name Techdocs

Description Techdocs test.

241 remaining

Save Cancel

The following table describes the options available on the Cloning page:

Field	Description
* Name	Enter the name of the user group.
Description	Enter a brief description of the user group and granular-level access associated with the resource.  Note: You can enter a maximum of 255 words in the field.
 Note: The asterisk (*) symbol indicates a mandatory field.	

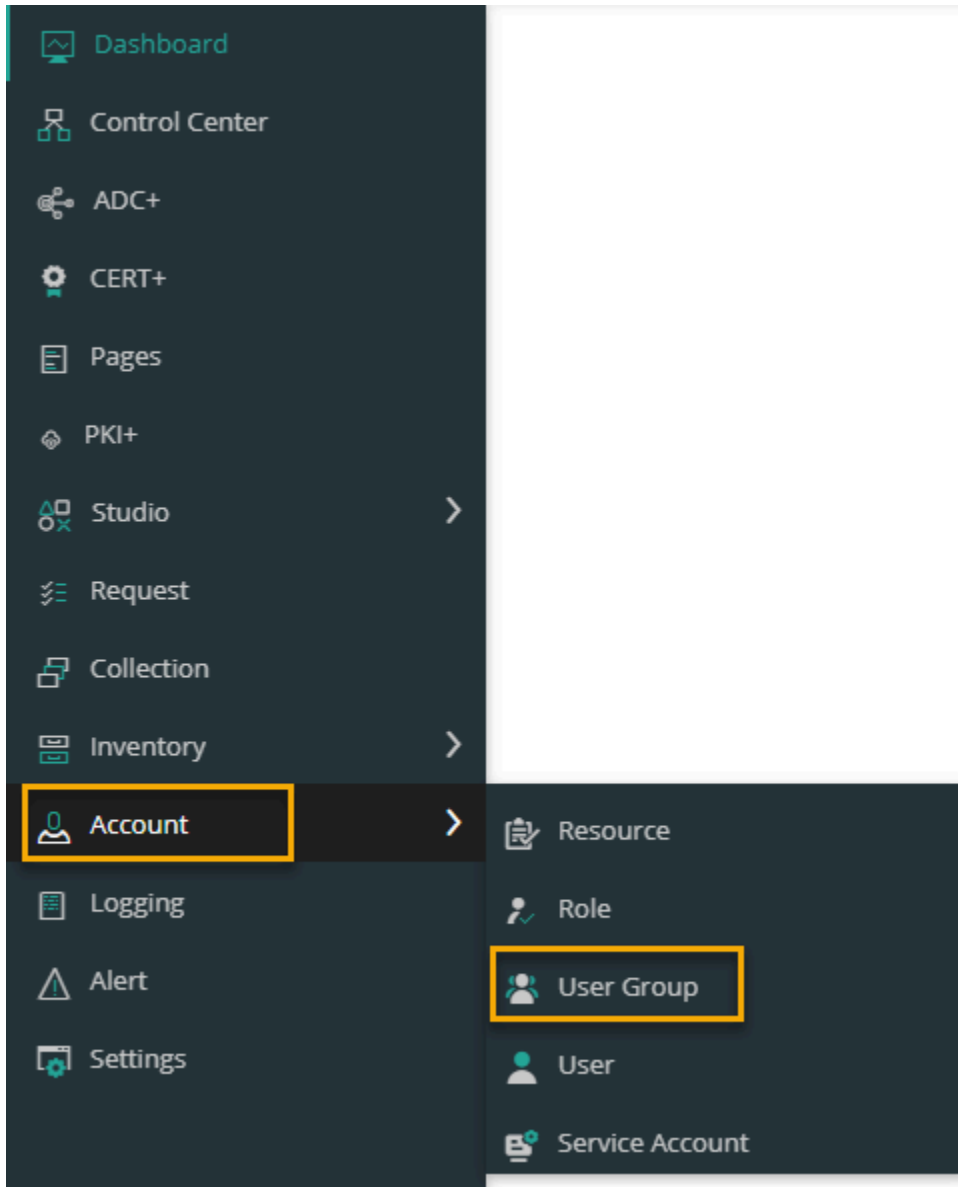
6. Click **Save**.

The user group is cloned and a pop-up message displays as **User group cloned successfully**.

Enable a User Group

To enable a user,

1. Log in to AppViewX application with valid credentials.
The left navigation pane appears.
2. Click the menu button located in the upper left corner of the screen.
3. Navigate to **Account**, and then click **User Group** from the list.

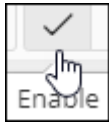


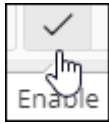
The **User Group** page appears.

The screenshot shows the 'User group' page in the AppViewX application. At the top, there is a 'User group' tab and a 'Quick config' button, both highlighted with yellow boxes. Below the tab, there is a search bar and a table listing user groups.

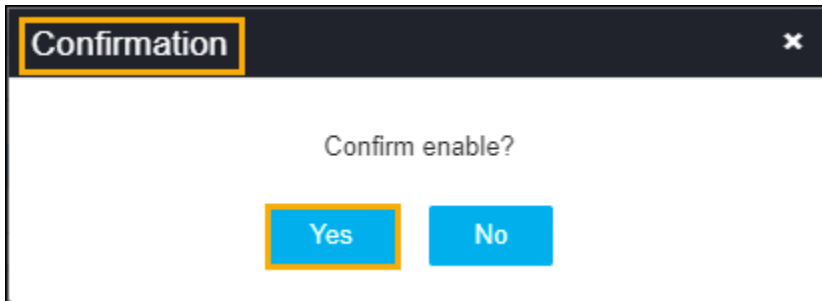
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin usergroup	Admin user group ext...	admin	super access	Default Rule	Enabled
☐	cert_acf_UnAssign_S...	sample	cert_acf_UnAssign_ServerCert_RenewC...	super access		Enabled

4. In the user group inventory, select the check box against the user group you want to enable.



5. Click the  icon in the command bar to enable the user group.

6. A confirmation pop-up window, to confirm the operation.



7. Click **Yes**.

The role is enabled and a confirmation message displays as **Operation performed successfully**.

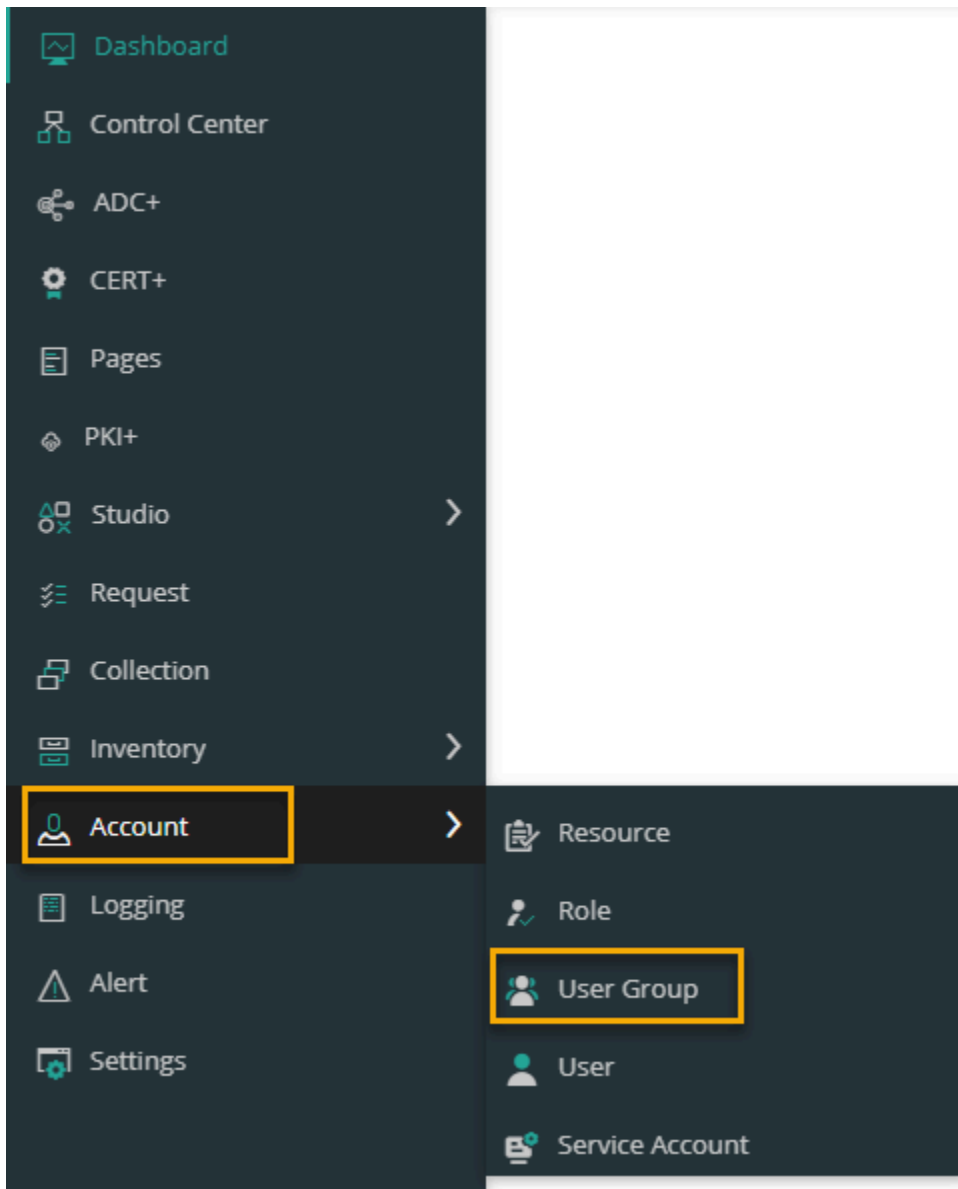
Disable a User Group

To disable a user,

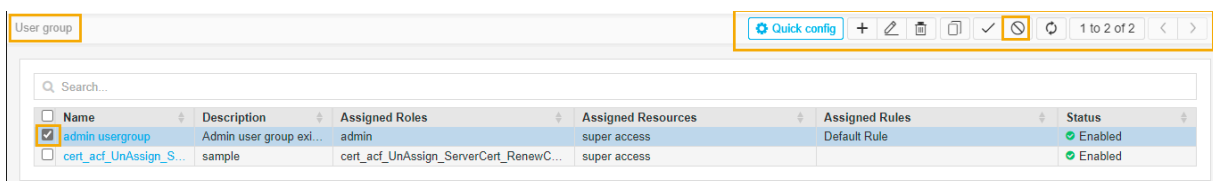
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Navigate to **Account**, and then click **User Group** from the list.



The **User Group** page appears.

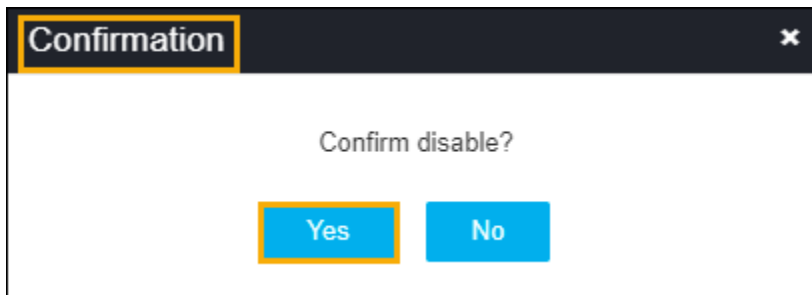


4. In the user group inventory, select the check box against the user group you want to disable.



5. Click the icon in the command bar to disable the user group.

6. A confirmation pop-up window, to confirm the operation.



7. Click **Yes**.

The role is disabled and a confirmation message displays as **Operation performed successfully**.

User

- [Overview](#)
- [Create a User](#)
- [Modify a User](#)
- [Delete a User](#)
- [Enable a User](#)
- [Disable a User](#)
- [Import Users](#)

Overview

A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directory (AD). A user account is used for authentication, access, accounting, security, logging, and resource management. To create user accounts, you must be assigned to either the Administrator or User Manager role.



Note: You must add a user to the user group as the roles and resources cannot be directly associated with the user.

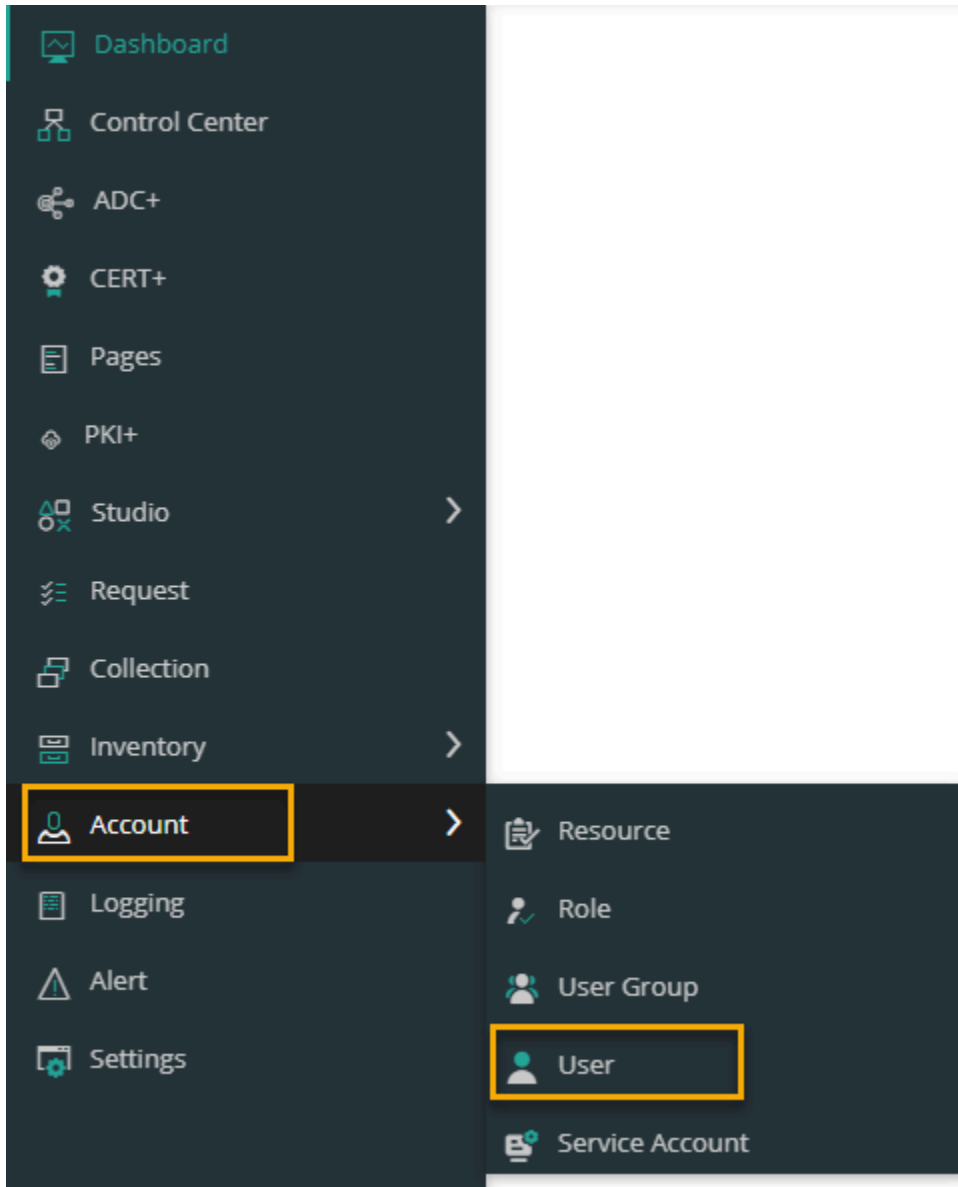
Create a User

To create a user,

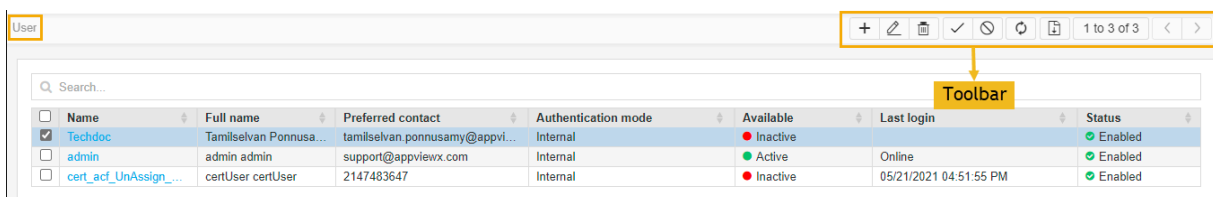
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Navigate to **Account**, and then click **User** from the list.



The **User** page appears.





4. Click the  icon in the command bar to create a new user.

The **User Add** page appears.

User > Add

Information User group

Account information

* User name

* Password ⓘ

* Confirm password

Authenticate externally ☐

First name

Last name

Description

242 remaining

5. Enter the required details in the Account Information and Contact Information sections.
6. The following table describes the options available on the Information tab:

Options	
Account Information	Enter the following account details as described below:

Options		
	Options	
	*User name	Enter the desired username.
	*Password	Enter the secured password, following the below criteria, • Have at least one uppercase and one lowercase character • Have at least one numeric character • Have at least one special character ~!@#\$%^*_-= (). • Must have 6 to 24 characters long • Not contain the user name • Not contain the same character more than three times in a row (f • Not contain blank spaces.
	*Confirm password	The password to confirm the entered Password field and match with
	(Optional) Authenticate externally	Select the Authenticate externally checkbox if you want authentication
	First name	Enter the first name of the user.
	Last name	Enter the last name of the user.
	Description	Enter a brief description of the user group and granular-level access  Note: You can enter a maximum of 255 words in the field.
Contact information	Enter the following account details as described below:	
	Options	
	Preferred mode of contact	Enter the mode of contact from the drop-down list. The • Email address • Phone number.
	*Email address	Enter the valid email address.
	Phone number	Enter the valid phone number.

Options		
	Options	
		 Note: If you select the mode of contact as Phone

 **Note:** The asterisk (*) symbol indicates a mandatory field.

7. Click **Save**.

The pop-up message appears as **User added successfully**.

8. Click the **User Group** tab to add the user to a group.

9. Select the check box beside each of the user groups that you want to add the user to.

 **Note:** A user can be assigned to more than one group in the system. A user assigned to more than one group inherits all of the permissions of all of the groups to which he or she is added.

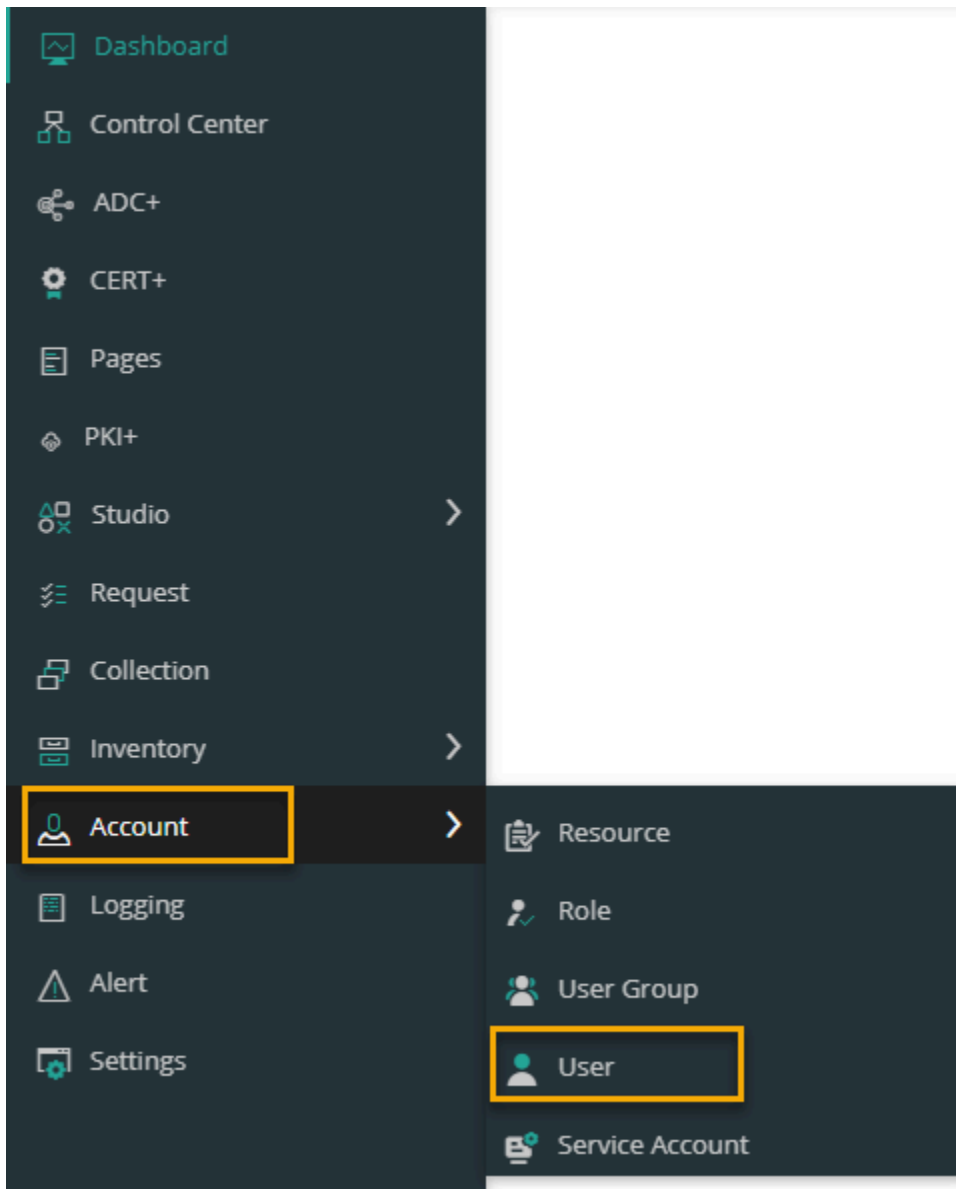
10. Click **Save**.

The pop-up message appears as **Updated successfully**.

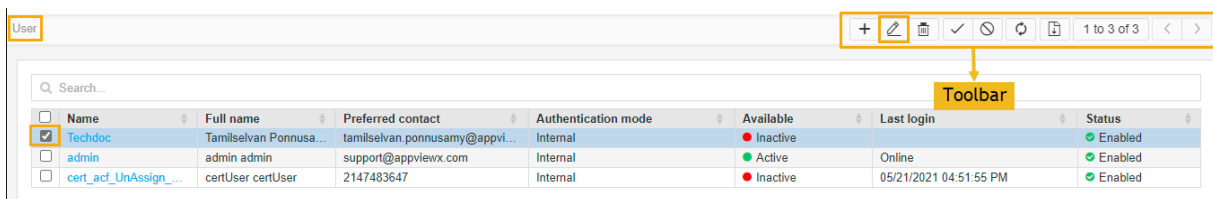
Modify a User

To modify a user,

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. Navigate to **Account**, and then click **User** from the list.



The **User** page appears.



- Click the  icon in the command bar to modify a user.

The **User Add** page appears.

User > Modify :: Techdoc

Information User group

Account information

* User name Techdoc

Password 

Reset password

Authenticate externally ☐

First name Tamilselvan

Last name Ponnusamy

Description Techdoc test.

Contact information

5. Enter the required details in the Account Information and Contact Information sections. The following table describes the options available on the Information tab:

Options		
Account Information	Enter the following account details as described below:	
	Options	
	*User name	You cannot modify the user name.

Options										
	Options									
	*Password	You cannot modify the user name.								
	Reset password	You can reset the password if required.								
	(Optional) Authenticate externally	Select the Authenticate externally checkbox if you want authentication.								
	First name	Enter the first name of the user.								
	Last name	Enter the last name of the user.								
	Description	Enter a brief description of the user group and granular-level access.  Note: You can enter a maximum of 255 words in the field.								
Contact information	Enter the following account details as described below: <table border="1"> <thead> <tr> <th>Options</th> <th></th> </tr> </thead> <tbody> <tr> <td>Preferred mode of contact</td> <td> Enter the mode of contact from the drop-down list. The available options are: • Email address • Phone number. </td> </tr> <tr> <td>*Email address</td> <td>Enter the valid email address.</td> </tr> <tr> <td>Phone number</td> <td> Enter the valid phone number.  Note: If you have the select mode of contact as Phone number, you must enter a valid phone number. </td> </tr> </tbody> </table>		Options		Preferred mode of contact	Enter the mode of contact from the drop-down list. The available options are: • Email address • Phone number.	*Email address	Enter the valid email address.	Phone number	Enter the valid phone number.  Note: If you have the select mode of contact as Phone number, you must enter a valid phone number.
Options										
Preferred mode of contact	Enter the mode of contact from the drop-down list. The available options are: • Email address • Phone number.									
*Email address	Enter the valid email address.									
Phone number	Enter the valid phone number.  Note: If you have the select mode of contact as Phone number, you must enter a valid phone number.									
 Note: The asterisk (*) symbol indicates a mandatory field.										

6. Click **Save**.

The pop-up message appears as **User information updated successfully**.

7. Click the **User Group** tab to add the user to a group.

8. Select or deselect the check box beside each of the user groups that you want to add the user to.



Note: A user can be assigned to more than one group in the system. A user assigned to more than one group inherits all of the permissions of all of the groups to which he or she is added.

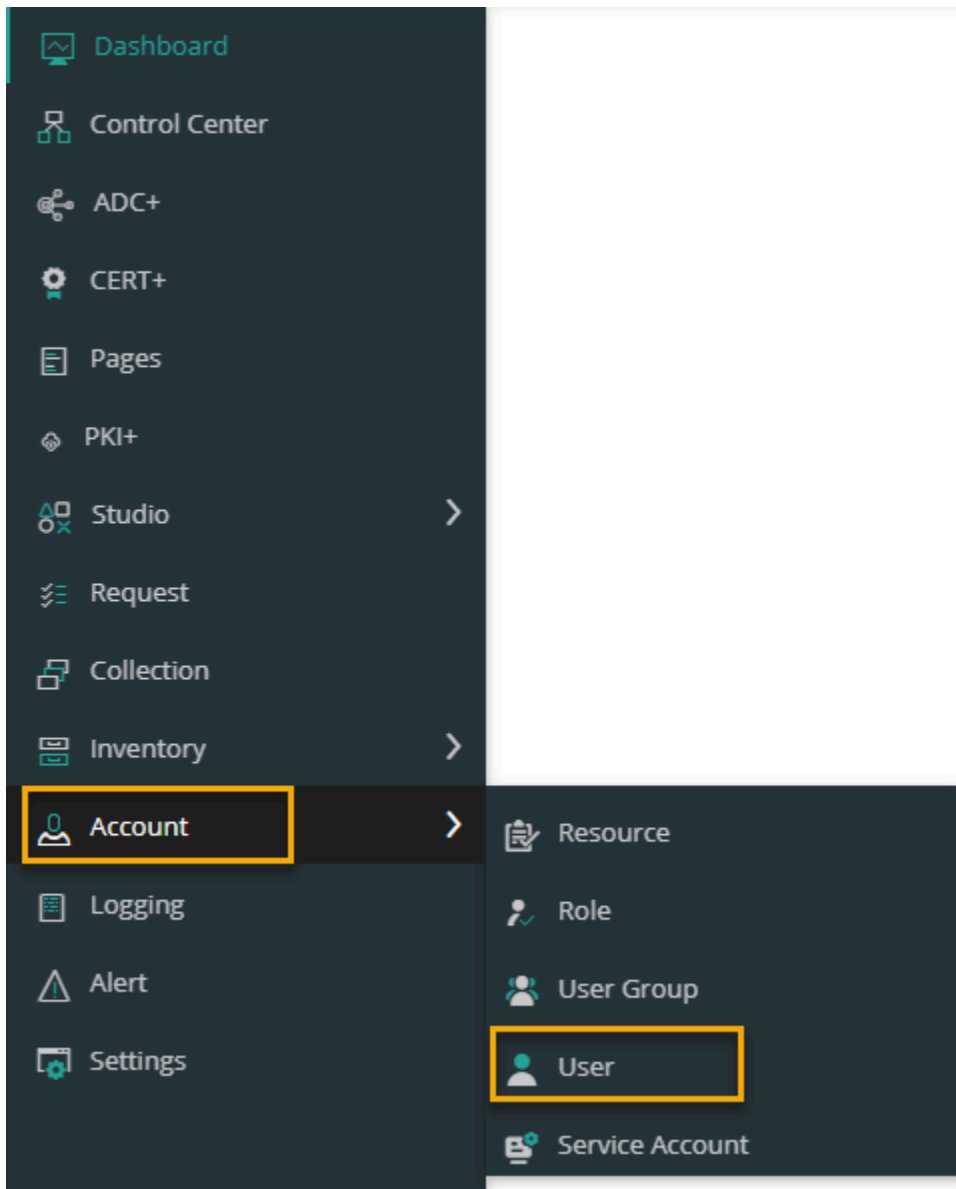
9. Click **Save**.

The pop-up message appears as **Updated successfully**.

Delete a User

To delete a user,

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. Navigate to **Account**, and then click **User** from the list.



The **User** page appears.

User							
+ ✎ 🗑️ ✓ 🔄 📄 1 to 3 of 3 < > Toolbar							
☐	Name	Full name	Preferred contact	Authentication mode	Available	Last login	Status
☒	Techdoc	Tamilselvan Ponnusa...	tamilselvan.ponnusamy@appvi...	Internal	Inactive		Enabled
☐	admin	admin admin	support@appviewx.com	Internal	Active	Online	Enabled
☐	cert_acf_UnAssign_...	certUser certUser	2147483647	Internal	Inactive	05/21/2021 04:51:55 PM	Enabled

- In the **User** list, select the check box beside the role you want to delete.
- Click the icon in the command bar to delete the User.

The confirmation pop-up window appears.

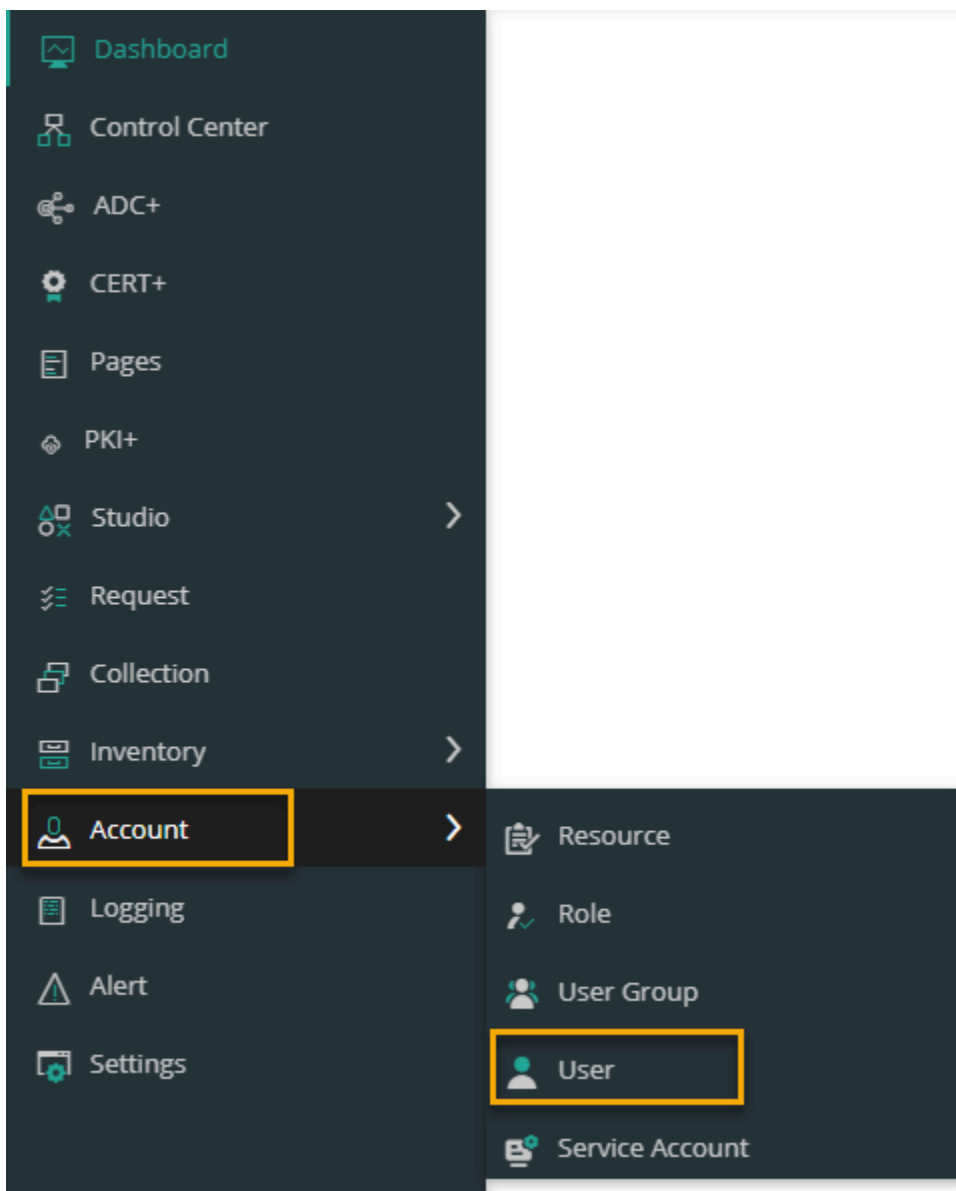
6. Click **Yes**.

The pop-up message appears as Operation performed successfully.

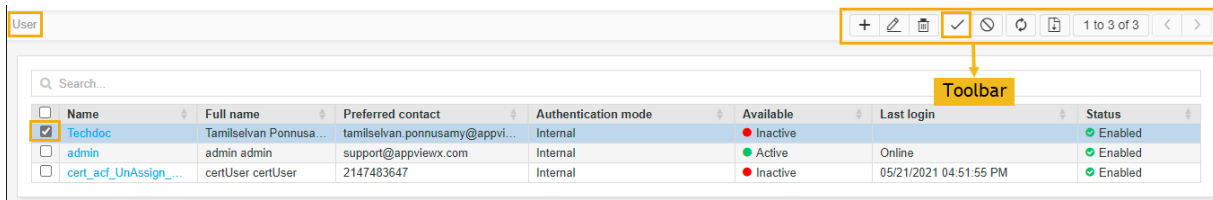
Enable a User

To enable a user,

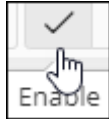
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **Account**, and then click **User** from the list.

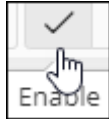


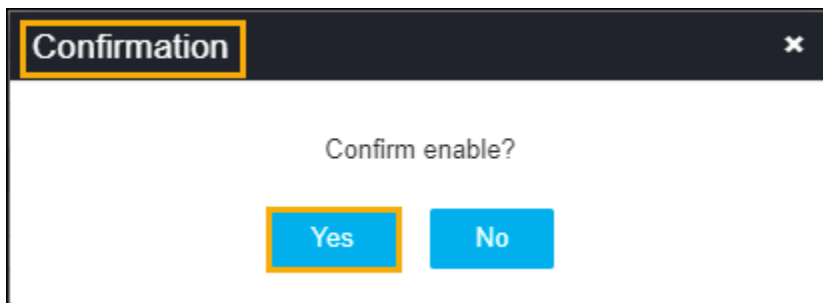
The **User** page appears.



- In the user group inventory, select the check box against the user you want to enable.



- Click the  icon in the command bar to enable the user.
- A confirmation pop-up window, to confirm the operation.

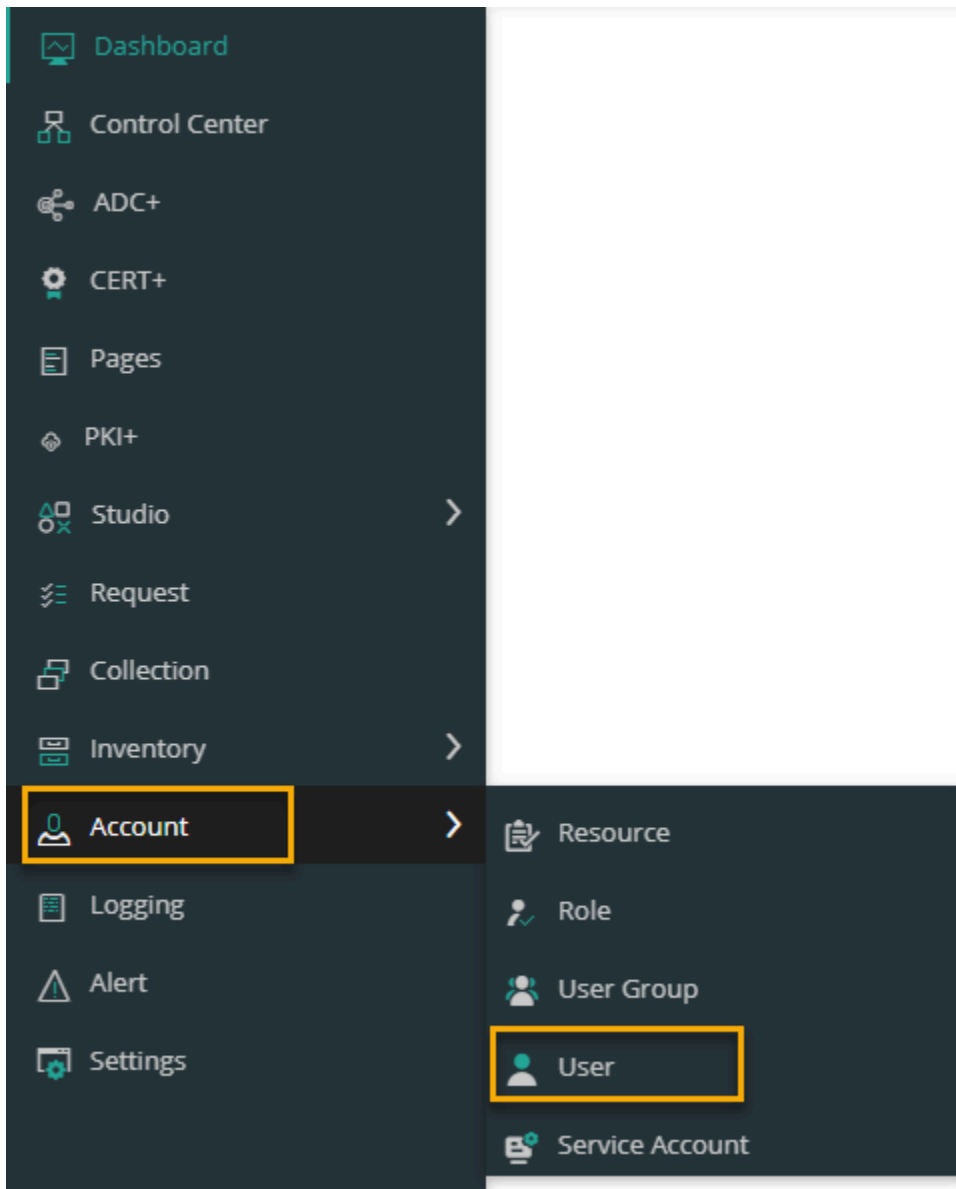


- Click **Yes**. The role is enabled and a confirmation message displays as **Operation performed successfully**.

Disable a User

To disable a user,

- Log in to AppViewX application with valid credentials.
- Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
- Navigate to **Account**, and then click **User** from the list.



The **User** page appears.

User group

Quick config

1 to 2 of 2

Search...

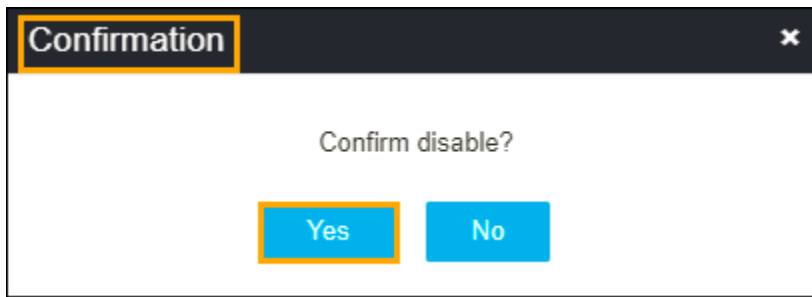
☐	Name	Description	Assigned Roles	Assigned Resources	Assigned Rules	Status
☒	admin usergroup	Admin user group exi...	admin	super access	Default Rule	Enabled
☐	cert_act_UnAssign_S...	sample	cert_act_UnAssign_ServerCert_RenewC...	super access		Enabled

4. In the user group inventory, select the check box against the user you want to disable.



5. Click the  icon in the command bar to disable the user.

6. A confirmation pop-up window, to confirm the operation.



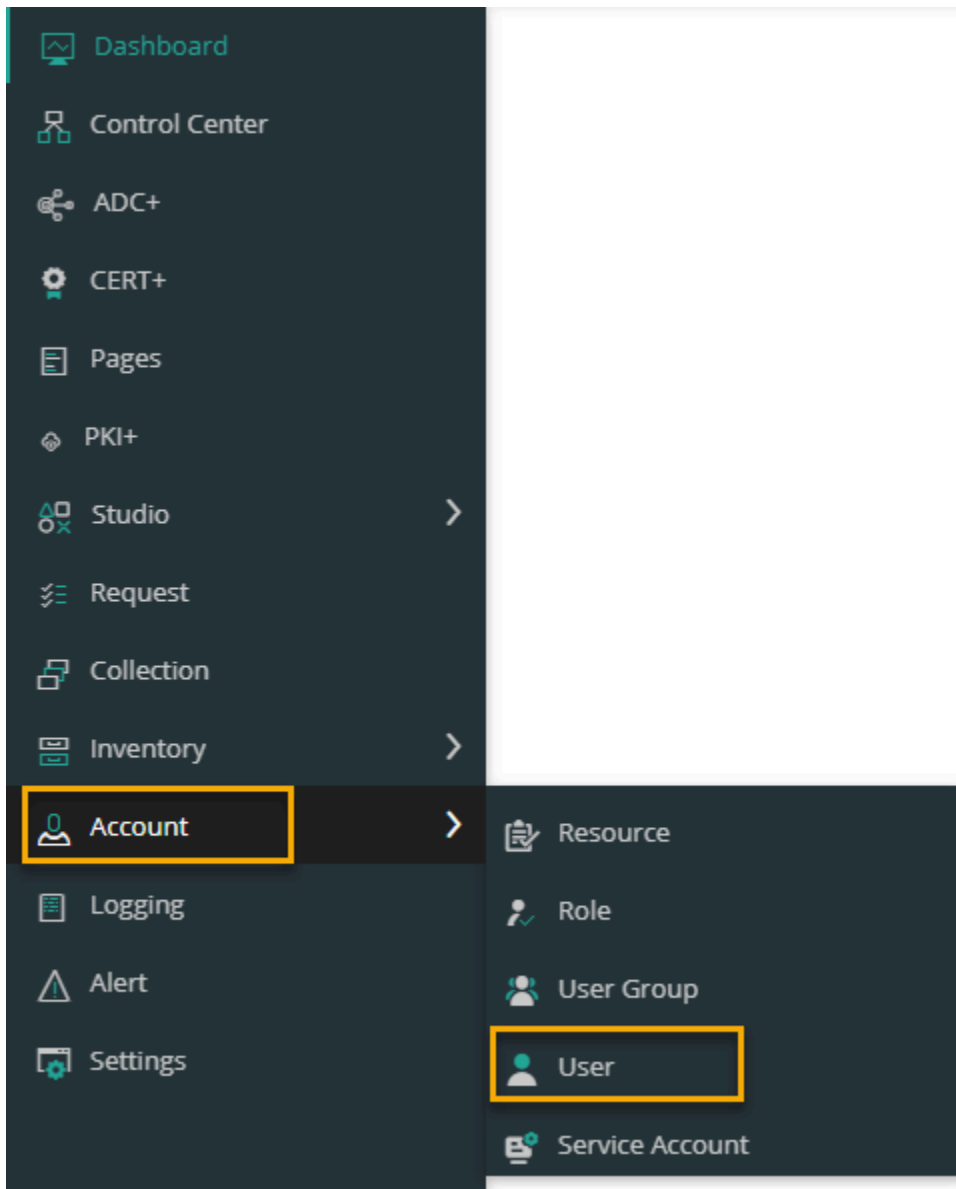
7. Click **Yes**.

The role is disabled and a confirmation message displays as **Operation performed successfully**.

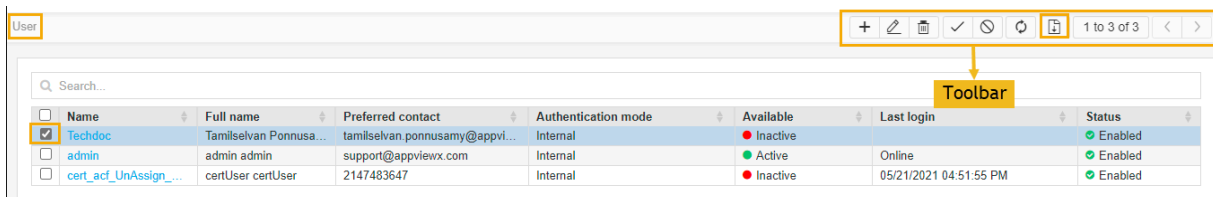
Import Users

To import users,

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. Navigate to **Account**, and then click **User** from the list.



The **User** page appears.



- Click the  icon in the command bar to import the file.

The import page appears.

- Click **Browse**, and select the user file.



Note: The file must be in <.csv> format. To download a sample template file, click the icon on the top right corner. **Tip:** The most efficient way to import user details is to download the sample import file that is available by clicking the **Sample file** button in the Command bar of the *Import* screen, modify the contents, save it, and then import it into the system. This reduces the chance that error messages appear during the import process.

6. Click **Upload** to review the user details.



Note: At this point, the user details are not imported. They are displayed for review.

7. Review the details for each user in the import file. If you do not want to import specific users, clear the check box against their names.

8. Click **Submit**.

RBAC Configuration

- [Overview](#)
- [Benefits of RBAC](#)
- [Simplified RBAC Configuration in AppViewX](#)

Overview

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.

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.

Accessing the Quick Config Option

- [Configuring RBAC using the Quick Config Option](#)
- [Ways to Access Quick Config Wizard Flow](#)

Configuring RBAC using the Quick Config Option

To configure RBAC using the Quick Config option,

- Click **Menu > Settings > General > Authentication > Quick Config** option.
- The Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of the wizard flow, user groups, roles, and resource stages are displayed at the top. Click on the respective stage for configuration.

Ways to Access Quick Config Wizard Flow

- Click **Menu > Account > User group > Quick Config** option.

(or)

- Click **Account > Role > Quick Config** option

(or)

- Click **Account > Resource > Quick Config** option.

The Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of the wizard flow, user groups, roles, and resource stages are displayed at the top. Click on the respective stage for configuration. For detailed instructions to perform the above-mentioned actions, refer **Platform User Guide**

Chapter 3: CERT+ Setup

- [Configuring CA Settings](#)
- [Certificate 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 MPKI](#)
- [GoDaddy CA](#)
- [Google CA](#)
- [InCommon CA](#)
- [Let's Encrypt CA](#)
- [Microsoft Enterprise CA](#)
- [Microsoft Standalone CA](#)
- [Symantec CA](#)
- [Trustwave CA](#)
- [GlobalSign MSSL](#)
- [GlobalSign SSL](#)
- [Nexus](#)

Amazon and Amazon Private CA

- [Before you Begin](#)
- [Configuring Amazon CA](#)
- [Configuring Amazon Private CA](#)
- [Validating Amazon](#)

Before you Begin

Following are the prerequisites for configuring Amazon CA or Amazon Private CA account in AppViewX

- Need to have 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. Check Proxy Setup for the steps to configure the proxy. <https://adminguide.appviewx.com/proxy-4>
- 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",

"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",
      "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": [
```

```
"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",

"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"

]

}

]

}

```

Configuring Amazon CA

To configure the Amazon CA,

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 **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Amazon**.

The **Amazon** home page is displayed.

6. To configure **Amazon** CA, click Amazon on the home page.
 - a. Click the **Configure Now** or **+Add** icon in the middle or top-right of the page respectively.

The **Amazon** configuration page appears.

The screenshot shows the Amazon Certificate Authority configuration page. The sidebar on the left lists various CA providers: CUSTOM, amazon, appviewX, SPECTIGO, digicert, EJBCA, Entrust, GlobalSign, GoDaddy, Certificate Authority Service, and InCommon. The 'amazon' provider is selected. The main content area is titled 'General Information' and contains the following fields:

- CA Account name:** Techdoc test
- Purpose/Usage:** Server, Client
- Proxy Required:** ☒
- Data Center (AppViewX's CA agent):** absecon

Below the 'General Information' section is the 'CA Configuration' section, which contains the following fields:

- Access Key ID:** 1234
- Secret Access Key:** ****
- Service Region:** US East (N. Virginia)

At the bottom of the page, there are two buttons: 'Save' and 'Cancel'.

Update the following details in the **General Information** section and **CA Configuration** section as described in the table:

Section	Field	Description
General Information	*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. 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.
	Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
CA Configuration	*Access Key ID	Enter the Amazon access key id to authenticate the request.
	*Secret Access Key	Enter the Amazon secret access key id to authenticate the request.
	Service Region	Select the service offered region from the drop-down list.
 Note: The asterisk (*) symbol indicates a mandatory field.		

b. Click **Save**.

Configuring Amazon Private CA

To configure the Amazon CA,

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 is displayed.

3. Click **CERT+**.

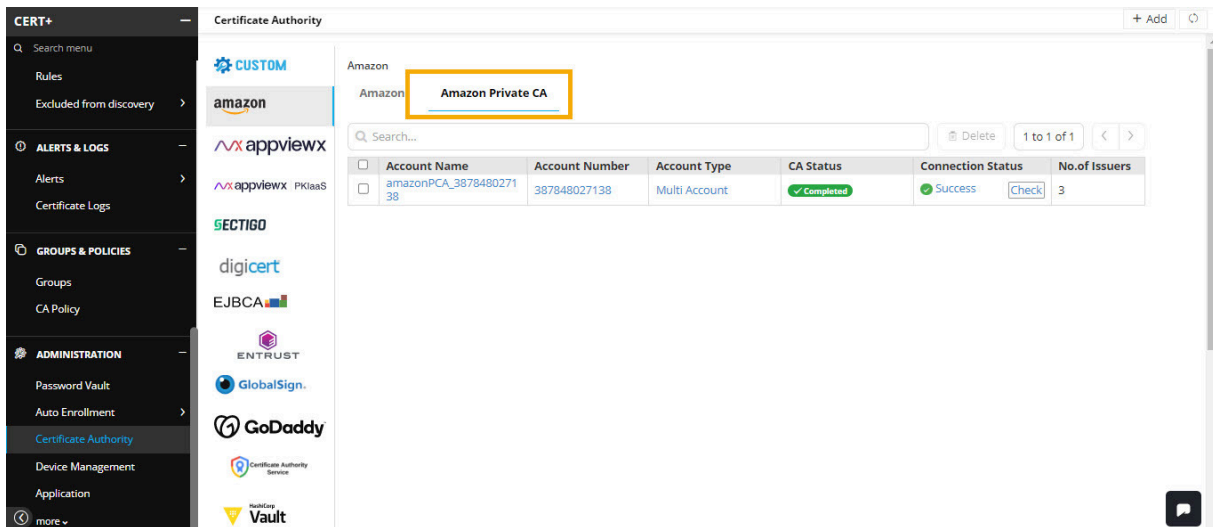
The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select **Amazon**.

The **Amazon** home page is displayed.

6. To configure the Amazon Private CA, click **Amazon PCA**.



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:

Field	Description
Search	Use the Search field to search for accounts, by entering the value of one of the details listed in the inventory grid.

Field	Description						
 Delete	To delete one or more accounts: a. From the inventory grid, select the checkbox corresponding to the account(s) you want to delete.  Delete b. Click  Tip: To delete all accounts listed in the inventory grid, select the checkbox in the grid header. Search... <table><tr><td>☐</td><td>Account Name</td><td>Account Number</td><td>Account Type</td><td>CA Status</td><td>Cor</td></tr></table>	☐	Account Name	Account Number	Account Type	CA Status	Cor
☐	Account Name	Account Number	Account Type	CA Status	Cor		
1 to 1 of 1	To set the number of records that should be displayed on one page: a. Click 1 to 1 of 1 b. From the Show menu displayed, select the required value. 1 to 1 of 1 Show : 25 Records 50 Records 75 Records 100 Records						
< >	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						

Field	Description
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 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.

7. To add an account, click **Configure Now** (if you are creating your first account) or click from the top-right corner of the screen.

 Add

The **Amazon** page is updated to display fields for entering the CA configuration-related information.

8. On this screen, enter the following **Basic Information**:

Field	Description
Account type*	From the dropdown list, from the following options, select the customer's AWS account type: • Stand-alone account sign-in: The user account and the resources are available in the same account. • Cross account sign-in: 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.

Field	Description
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)

9. Enter the following **Credentials**-related information:

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 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.

Field	Description
	 Note: This field is displayed only when Credential type is set to Credential List - CyberArk .

10. In the **Discover resources** section, enter the following details:

Field							
Role ARN for Resource Discovery*	 Note: 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 resource)						
	a. Click  .						
	b. Enter the following details:						
	<table border="1"> <thead> <tr> <th>Field</th> </tr> </thead> <tbody> <tr> <td> Role Session name </td> </tr> <tr> <td> Duration Seconds </td> </tr> <tr> <td> External Id </td> </tr> <tr> <td> Source Identity </td> </tr> <tr> <td> Session Tags </td> </tr> </tbody> </table>	Field	Role Session name	Duration Seconds	External Id	Source Identity	Session Tags
Field							
Role Session name							
Duration Seconds							
External Id							
Source Identity							
Session Tags							

Field	
	Field
Service Region*	Service regions are regions that are supported by the selected service. To select a service region: - To fetch the service regions for the account information provided, click Fetch Region.The retrieved service regions are displayed in the Select the Region(s) dropdown list. - From the Select the Region(s) dropdown list, select the required service region.
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the account. • ACM Private CA • AWS Certificate Manager (ACM)
S3 Bucket*	Note: This field is displayed only when the ACM Private CA operation mode is selected. Enter the S3 bucket name.
Role ARN for S3 Bucket	Note: This field is displayed only when the ACM Private CA operation mode is selected. - Click . The ARN Advanced Settings action pane is displayed. - In the ARN Advanced Settings action pane, enter the following details:

Field							
	<table border="1"> <thead> <tr> <th>Field</th> </tr> </thead> <tbody> <tr> <td>Role Session name*</td> </tr> <tr> <td>Duration Seconds</td> </tr> <tr> <td>External Id</td> </tr> <tr> <td>Source Identity</td> </tr> <tr> <td>Session Tags</td> </tr> </tbody> </table>	Field	Role Session name*	Duration Seconds	External Id	Source Identity	Session Tags
Field							
Role Session name*							
Duration Seconds							
External Id							
Source Identity							
Session Tags							
	c. Click Apply .						
Discover Certificate	To enable instant certificate discovery at the time of device addition, select this checkbox.						

Field	
CA 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 managed by AppViewX. • Monitored: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be monitored by AppViewX. • 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, to set the frequency of the schedule-based sync: - From the first dropdown list, select the interval between two schedule-based syncs. - From the second dropdown, 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

11. 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. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

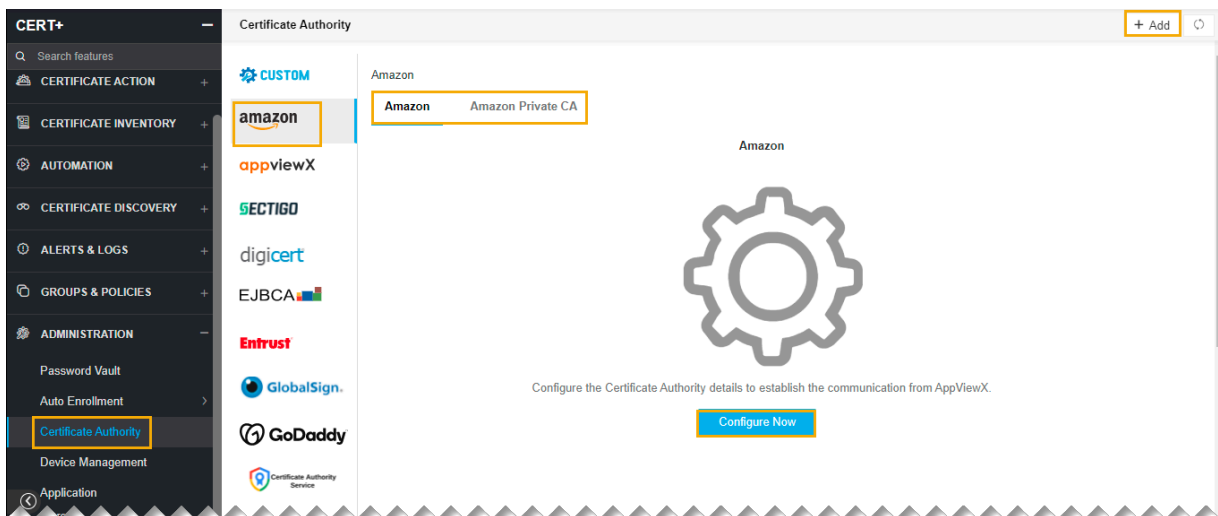
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

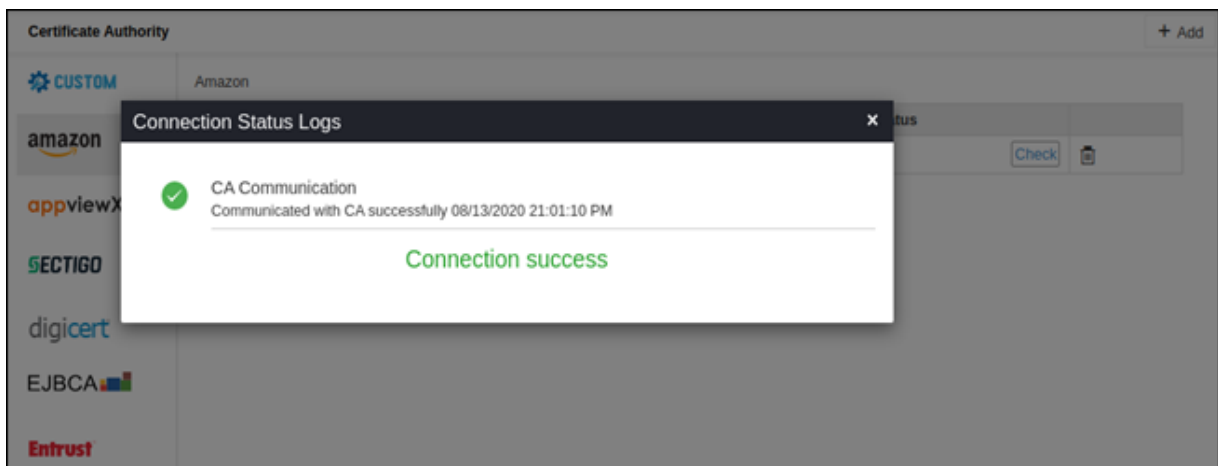
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Amazon**.

The **Certificate Authority** home page appears.



6. On the **Amazon** home page, select **Amazon** or **Amazon Private CA**.
7. 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

Following are the prerequisites for configuring Custom CA account in AppViewX:

- Need to have a Logo to use it for the custom CA.
- Optional CA certificate and key to use that as a root certificate.

Configuring Custom CA

To configure the custom CA,

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 **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Custom**.

The **Certificate Authority** home page appears.

The screenshot shows the 'Certificate Authority' page in the AppViewX application. On the left is a dark navigation pane with 'CERT+' at the top, followed by 'ADMINISTRATION' which is expanded to show 'Certificate Authority'. The main content area is titled 'Certificate Authority' and has a 'CUSTOM' tab selected. Below the tab is a 'Create Custom CA' button. The 'General Information' section contains a text box explaining that the custom CA will sign digital certificates for internal use. Below this are three required fields: 'Custom CA Name' (text input), 'Upload Custom CA Logo' (file upload, accepting .png, .jpg, or .jpeg), and 'Custom CA Certificate' (file upload, accepting .pfx or .p12). Each field has an 'Upload' button and an information icon. At the bottom are 'Save' and 'Cancel' buttons. A list of logos for various providers (amazon, appviewX, SECTIGO, ALL THINGS DECENTRAL, digicert, EJBICA, Entrust, GlobalSign, GoDaddy, InCommon) is visible on the left side of the main content area.

6. Update the following details in the **General Information** section as described in the table:

Name	Description
*Custom CA Name	A unique name to identify the CA name.

Name	Description
	 Note: 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.  Note: The <.pfx> and <.p12> are certificate types are supported.

 **Note:** The asterisk (*) symbol indicates a mandatory field.

Certificate Authority

CUSTOM

amazon

appviewX

SECTIGO

digicert

EJBCA

Entrust

GlobalSign

GoDaddy

< Create Custom CA

General Information

You can white label your organization's internal CA. Custom CA will sign digital certificates used for internal purposes.

* Custom CA Name

AppViewX Custom CA

* Upload Custom CA Logo

C:\fakepath\logo-blue-green.png

Upload

Custom CA Certificate

C:\fakepath\custom_ca_E4_02_B9_74_

Upload

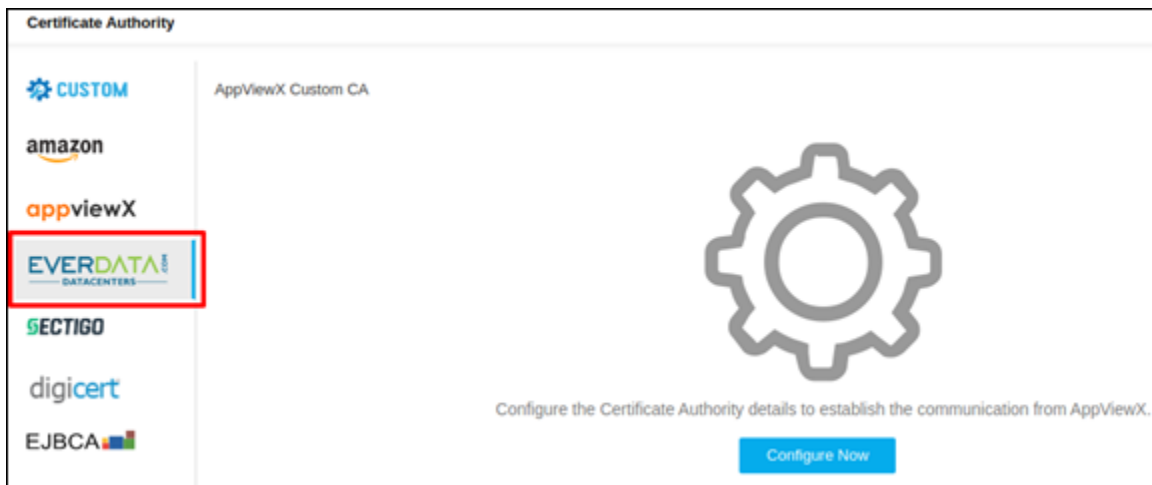
Preview



Save

Cancel

7. Once the logo and certificate are uploaded, the entered CA will appear in the CA list with the logo presented.



8. Once the logo is added, users can click **Configure Now** to input the CA details.
9. Update the following details in the **General Information** section as described in the table:

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. Update the following details in the **ROOT CSR parameters** section as described in the table:

Name	Description
Common Name	The common name of the root certificate.  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 (.)
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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

11. Update the following details in the **Validity** section as described in the table.

Root Validity

Start Date
09/30/2020 19:19:14

End Date
09/30/2025 19:19:14

Save
Cancel

Name	Description
*Start Date	Start date of the certificate issuance.
*End Date	End date of the certificate issuance.


Note: The asterisk (*) symbol indicates a mandatory field.

12. Click **Save**.

Once the setting is saved, the user will be directed to the root certificate submission holistic view as below.



13. Users can submit and fetch the root certificate.

14. On the CA setting page user can see the status of the created setting as shown below.

   	AppViewX Custom CA				
	Settings Name	CA Common Name	Immediate Parent Common Name	Purpose/Usage	Status
	AppViewX Custom CA Root CA	AppViewX Root CA		Server,Client,Code Signing	Not-generated

Digicert CA

- [Before you begin](#)
- [Configuring Digicert](#)
- [Validating Digicert Connection](#)

Before you begin

Following are the prerequisites for configuring Digicert CA account in AppViewX:

- Need to have Digicert CertCentral Account with **Administrator** role Access.
- **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. Check Proxy Setup for the steps to configure a proxy. <https://adminguide.appviewx.com/proxy-4>

Configuring Digicert

To configure the DigiCert CA,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

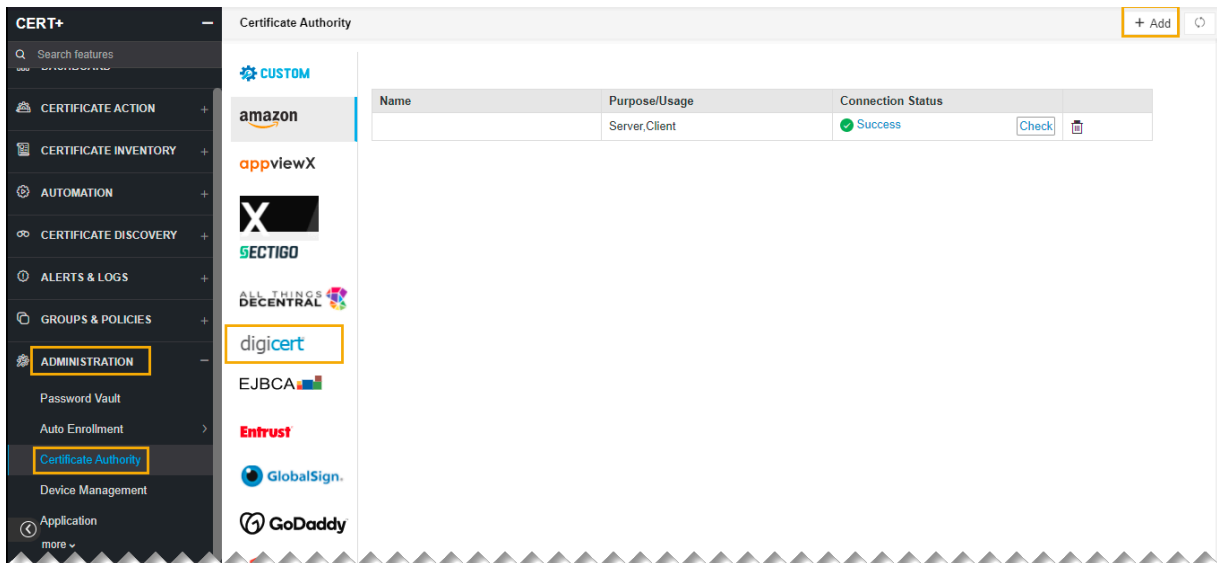
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **digicert**.

The **Certificate Authority** home page appears.



6. Click the **+Add** icon on the top right of the page.

The **DigiCert** configuration page appears.

Certificate Authority

< DigiCert

General Information

* CA Account name

* Purpose/Usage

Proxy Required

Data Center (AppViewX's CA agent)

CA Configuration

* Base URL

* Credential Type

Account ID

* API Key

Auto Approve

Fetch Divisions and Certificate Types

Save

Cancel

7. Update the following details in the **General Information** section as described in the table:

Name	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

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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:

Name	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.  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.

Name	Description
*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.
 Note: The asterisk (*) symbol indicates a mandatory field. Note: Auto approval checkbox is optional and features work only for one-step certificate requests configured in the Digicert Cert Central Account.	

9. Select **Fetch Divisions and Certificate Types**.

The Division and Certificate types available in the Digicert CA account will be fetched.

10. Click **Save**.

Validating Digicert Connection

Once the Digicert settings are added, the validation must be done to check whether the connection between AppViewX and Digicert is configured properly.

1. Log in to the **AppViewX** application with valid credentials.

2. Click on the menu button.

The left navigation pane appears.

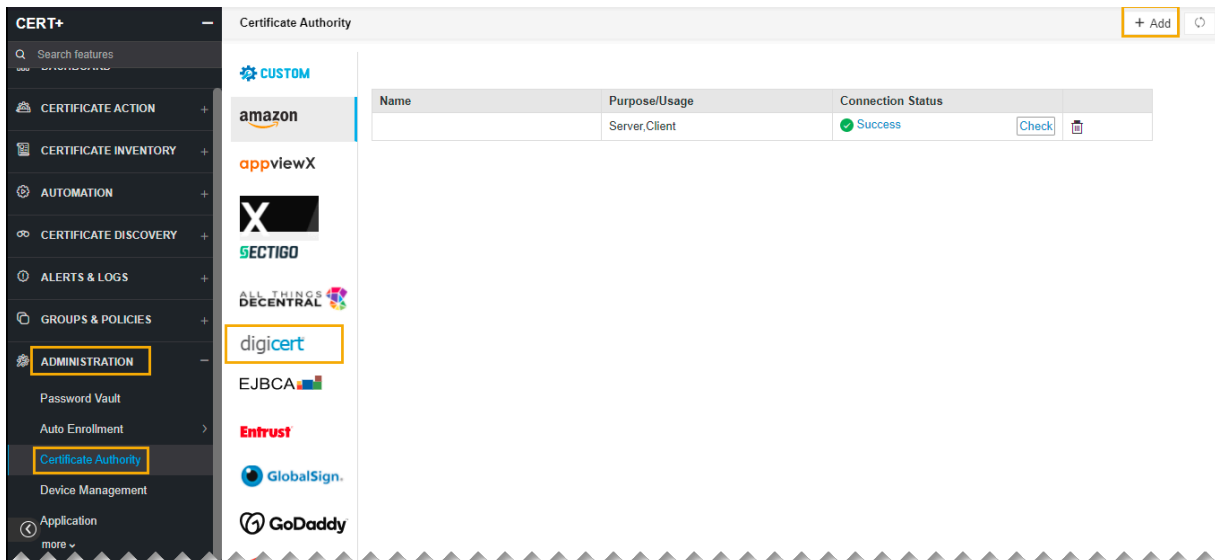
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

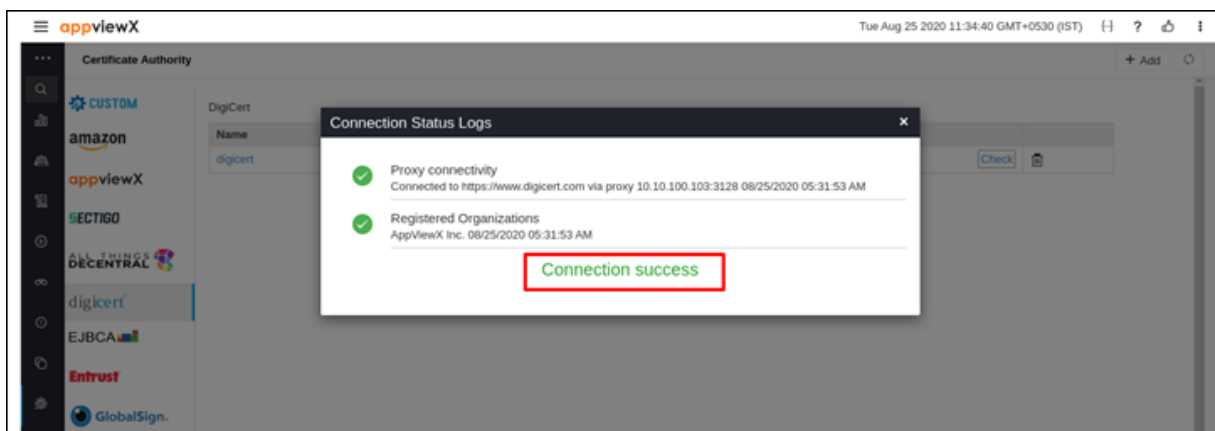
5. Click **Certificate Authority**, and then select **digicert**.

The **Certificate Authority** home page appears.



6. 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**.



Digicert MPKI

The following are the prerequisites for configuring a Digicert MPKI CA account in AppViewX:

- Need to have a Digicert MPKI Account with **Administrator** role Access.
- **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. Check Proxy Setup for the steps to configure the proxy. <https://adminguide.appviewx.com/proxy-4>

- Configuring DigiCert MPKI
- Validating DigiCert MPKI Connection

Configuring DigiCert MPKI

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

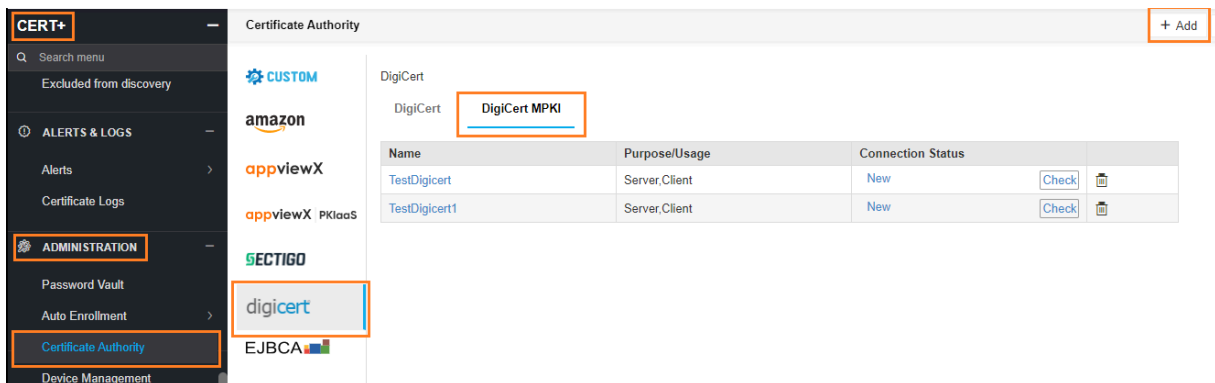
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **DigiCert**.

The **Certificate Authority** home page appears.



6. Choose the **DigiCert MPKI** tab and then click the **+Add** icon on the top right of the page.

The **DigiCert MPKI** configuration page appears.

CERT+

Search menu

Excluded from discovery

ALERTS & LOGS

Alerts

Certificate Logs

GROUPS & POLICIES

Groups

CA Policy

ADMINISTRATION

Password Vault

Auto Enrollment

Certificate Authority

Device Management

Application

more

Certificate Authority

CUSTOM

amazon

appviewX

appviewX PKIaaS

SECTIGO

digicert

EJBCA

Entrust

GlobalSign

GoDaddy

Certificate Authority

< DigiCert

General Information

* CA Account name: digicertmpki

* Purpose/Usage: Server, Client

Proxy Required: ☒

Data Center (AppViewX's CA agent): absecon

CA Configuration

* Base URL: https://pki-ws-rest.symauth.com/mpki/

* Seat ID: test@gmail.com

* API Key:

Fetch Profile

Save Cancel

7. Update the following details in the **General Information** section as described in the table.

Name	Description	Validation
*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	NA
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.	NA

Name	Description	Validation
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.	NA
 Note: The asterisk (*) symbol indicates a mandatory field.		

8. 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.

Name	Description	Validation
*Base URL	This URL will contain just the hostname of the Digicert CA instance. For example, <https://www.digicert.com>	vendorSpecificSettings.url - invalid URL
*Seat ID	Enter the unique seat id for discovering certificates.	NA.
*API Key	Enter the API key, which is generic across all CAs	NA.
 Note: - The asterisk (*) symbol indicates a mandatory field. - Auto approval checkbox is optional and features work only for one-step certificate requests configured in the Digicert Cert Central Account.		

9. 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.

	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	☒		☐	

10. Click **Save**.



Note: The 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. 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.

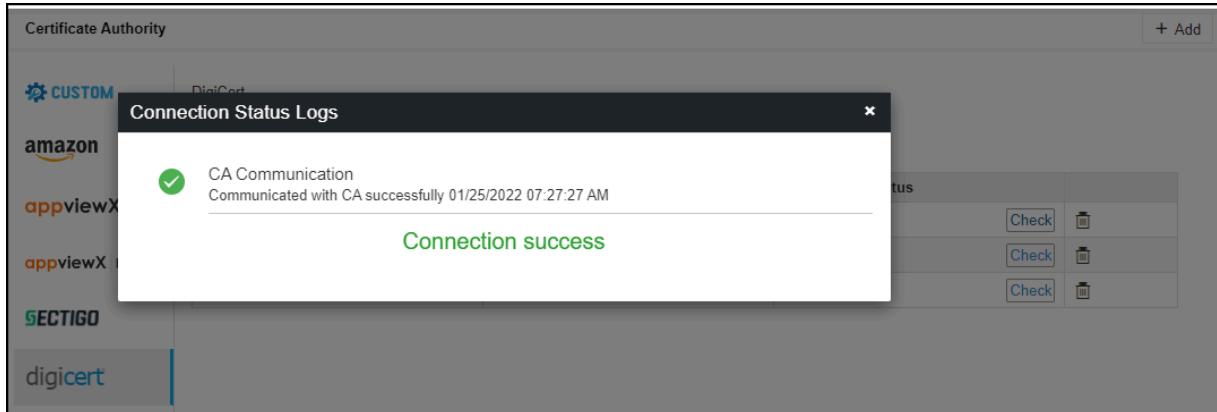
4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select **DigiCert**.

The **Certificate Authority** home page appears.

6. 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**.



EJBCA CA

- Before you begin
- Configuring EJBCA
- Validating EJBCA

Before you begin

Following are the prerequisites for configuring EJBCA account in AppViewX:

- Need to have 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. Check Proxy setup for the steps to configure the [proxy](#).

Configuring EJBCA

To configure the EJBCA CA,

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 **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **EJBCA**.

The **Certificate Authority** home page appears.

The screenshot shows the CERT+ interface. On the left, the 'ADMINISTRATION' menu is expanded, and 'Certificate Authority' is selected. The main area is titled 'Certificate Authority' and shows a list of EJBCA configurations. A table lists the configurations with columns for Name, Purpose/Usage, and Connection Status. Each row has a 'check' button and a trash icon.

Name	Purpose/Usage	Connection Status
ejbca	Server,Client,Code Signing	New
EJBCAMultipleSetting	Server,Client,Code Signing	New
MultipleEEP	Server,Client,Code Signing	New
EJBCA Deleted Profile	Server,Client,Code Signing	New
test	Server,Client,Code Signing	New
EJBCA With Custom Attributes	Server,Client,Code Signing	New

6. Click the +Add icon on the top right of the page.

The **Ejbca** configuration page appears.

Certificate Authority

CUSTOM

amazon

appviewX

X

SECTIGO

ALL THINGS DECENTRAL

digicert

EJBCA

Entrust

GlobalSign

GoDaddy

Certificate Authority Service

[< Ejbca](#)

General Information

* CA Account name ⓘ

* Purpose/Usage None Selected ⓘ

Proxy Required ☐ ⓘ

Please contact support/admin to restart the AppViewX CA agent when proxy required is enabled/disabled or proxy settings in Menu>> Certificate>> Administration >> General Settings Proxy is modified

Data Center (AppViewX's CA agent) absecon ⓘ

CA Configuration

* Client Authentication Upload ⓘ

* URL ⓘ

Please validate the credentials to fetch the end entity profile names from F.I.R.C.A account

Save Cancel

7. Update the following details in the **General Information** section as described in the table:

Options	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.

Options	Description
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Options	Description
*Client Authentication	Client authentication certificate for API communication. • Enter the valid password once the Authentication Details window appears. • Click OK. Note: 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.  Note: Must be a number.
End entity profile names	Required end entity profiles for CA setting.
Custom attributes	Required custom attributes for the specific end entity profile.  Note: Validation can be added by the user in the regex box.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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**.

10. Update the following details in the **Certificate Attributes** section as described in the table:

Options	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.
 Note: The asterisk (*) symbol indicates a mandatory field.Note: Custom attributes should be configured as exactly as it is available in the Ejbca portal.	

11. 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. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

The left navigation pane appears.

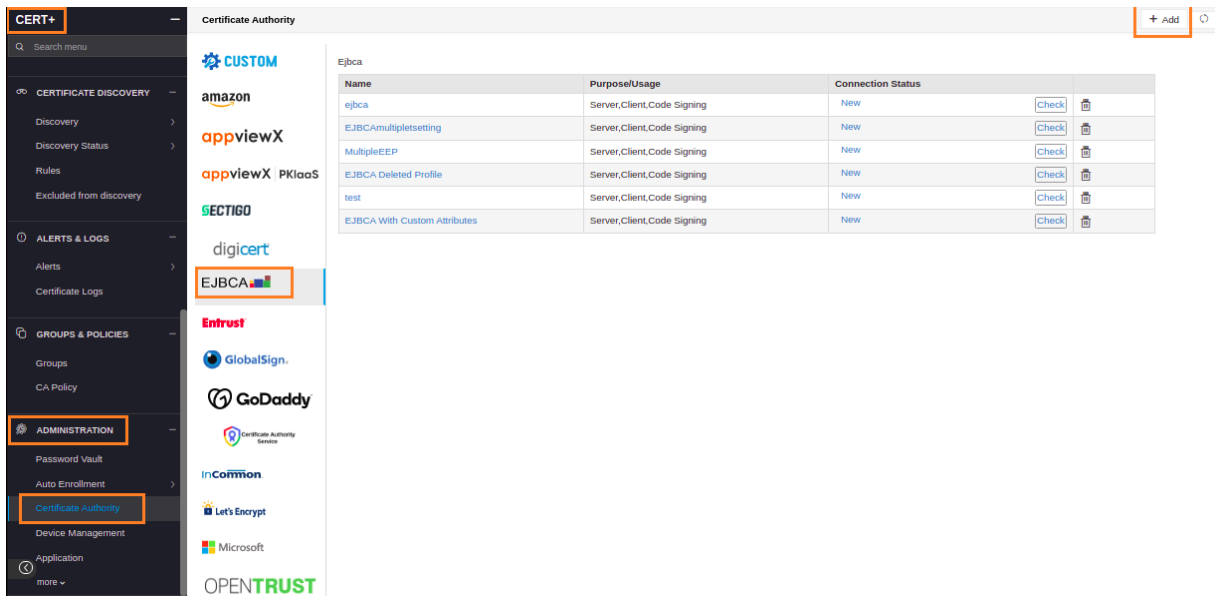
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

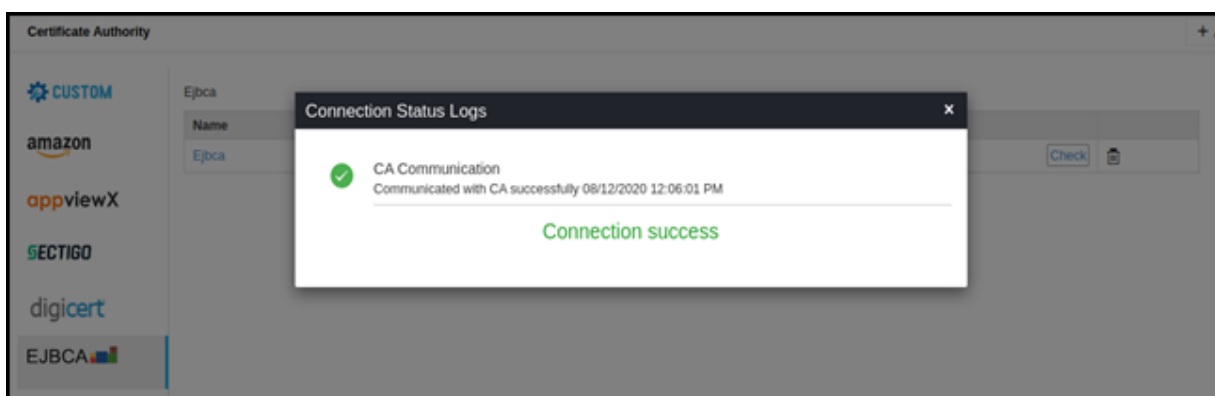
5. Click **Certificate Authority**, and then select **EJBCA**.

The **Certificate Authority** home page appears.



6. 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**.



Entrust MPKI

- Before you begin
- Configuring Entrust MPKI
- Validating Entrust MPKI Connection

Before you begin

Following are the prerequisites for configuring Entrust MPKI CA account in AppViewX:

- Need to have 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. Check [Proxy Setup](#) for the steps to configure the proxy.

Configuring Entrust MPKI

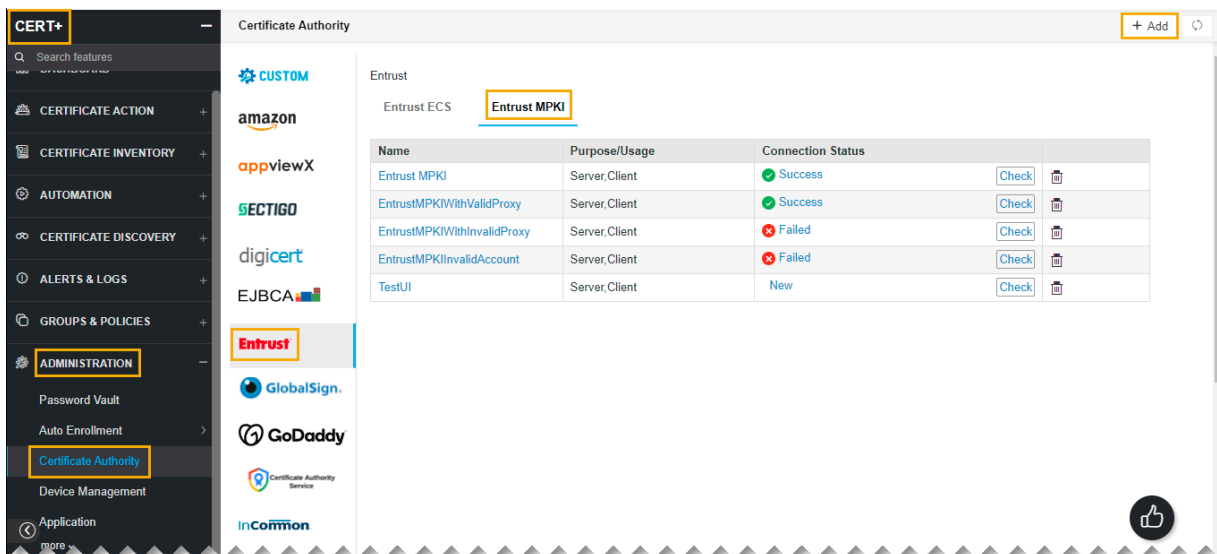
To configure the Entrust MPKI CA,

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+ > ADMINISTRATION > Certificate Authority**.

The **Certificate Authority** home page appears.



4. Click **Entrust** from the left pane of the page.

The Entrust CA home page appears.

5. Select the **Entrust MPKI** tab.

6. Click **+Add**.

The Entrust MPKI certificate page appears.

7. Update the following details in the **General Information** section as described in the table:

Name	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.
Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Name	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
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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.



Note: The pop-up message is displayed as **CA and profiles fetched**.

10. Click **Save**.

The created Entrust MPKI configuration settings will be added.



Note: The pop-up message is displayed as **<CA_name> Settings Added**.

Validating Entrust MPKI Connection

Once the Entrust settings are added, validation needs to be done to check whether the connection between AppViewX and Entrust is properly configured.

To validate the Entrust MPKI connection,

1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

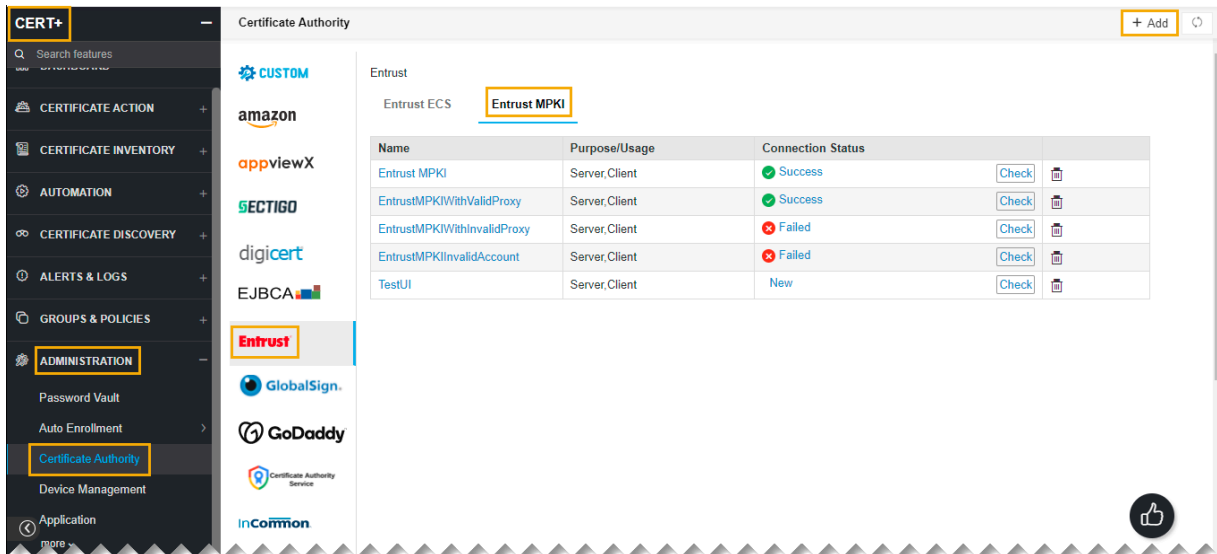
The left navigation pane appears.

3. Click **CERT+ > ADMINISTRATION > Certificate Authority**.

The **Certificate Authority** home page appears.

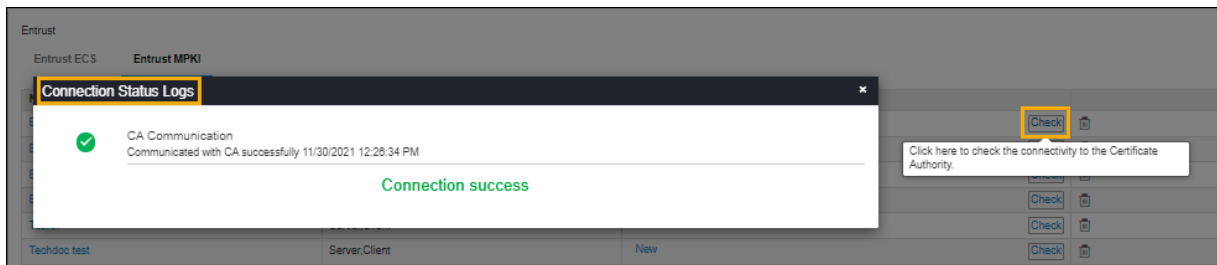
4. Click **Entrust MPKI** from the left pane of the page.

The **Entrust MPKI** CA home page appears.



5. 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**.



GoDaddy CA

- Before you begin
- Configuring GoDaddy
- Validating GoDaddy
- View GoDaddy product units

Before you begin

Following are the prerequisites for configuring a GoDaddy account in AppViewX:

- GoDaddy Customer Number, API key, and secret are required to make API Requests from AppViewX in order to perform CLM (Certificate Lifecycle Management) 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 the proxy. <https://adminguide.appviewx.com/proxy-4>
- Customer Number, API key, and secret configuration in GoDaddy Account:
 1. After logging into the GoDaddy portal with proper account credentials go to <https://developer.godaddy.com/keys>
 2. 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.
 3. This API key and secret will be used for further communication.
 4. Customer Number details are available on the Accounts page of the GoDaddy website
- Product units should be available in the customer's GoDaddy account to perform CLM operations.

Configuring GoDaddy

To configure the GoDaddy CA,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

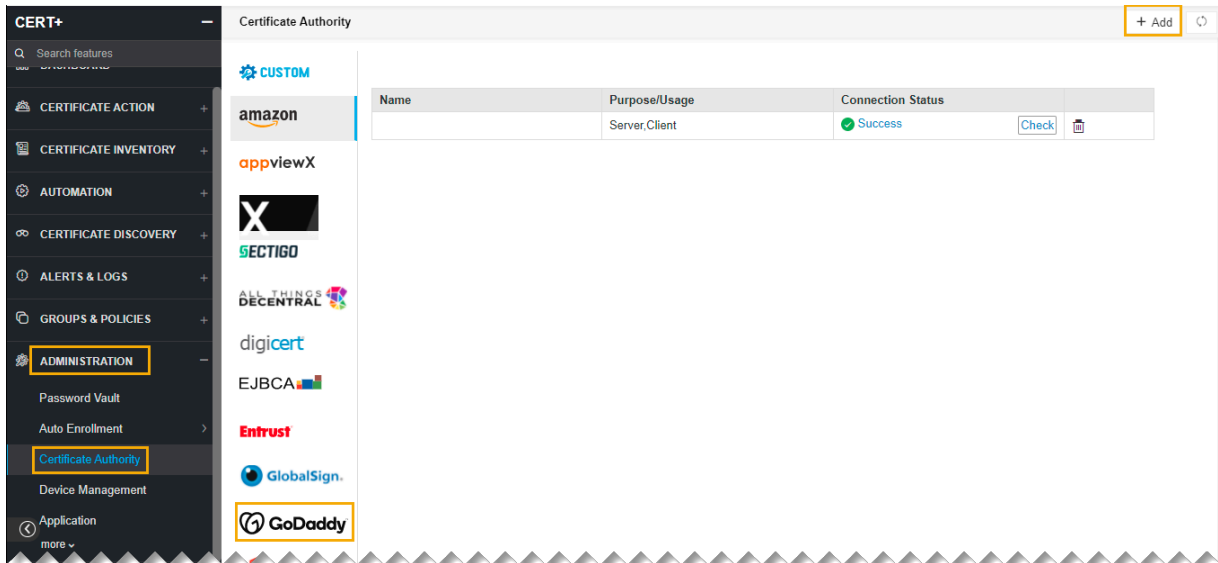
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **GoDaddy**.

The **Certificate Authority** home page appears.



6. Click the +Add icon on the top right of the page.

The GoDaddy configuration page appears.

Certificate Authority

< GoDaddy

General Information

* CA Account name

* Purpose/Usage

Proxy Required

Data Center (AppViewX's CA agent)

CA Configuration

* Base URL

* Customer Number

* API Key

* API Secret

First Name

Last Name

Save

Cancel

7. Update the following details in the **General Information** section as described in the table:

Name	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.

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Name	Description
*Base URL	This URL will contain the Base URL of the GoDaddy CA API instance. For example: https://api.godaddy.com
*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.

Name	Description
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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

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. To validate GoDaddy CA,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

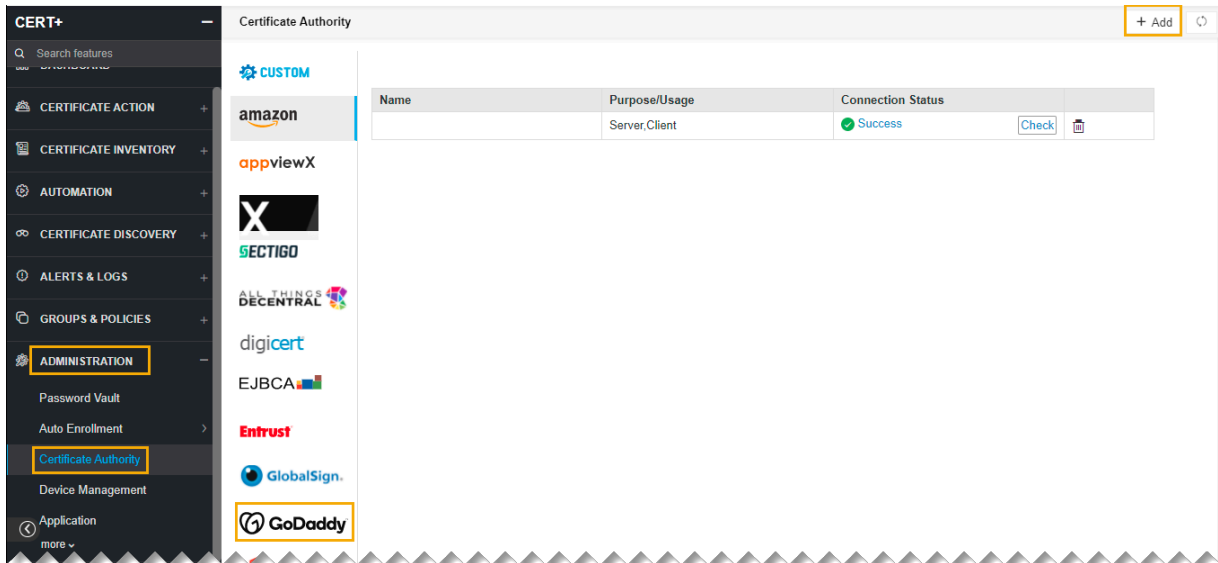
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

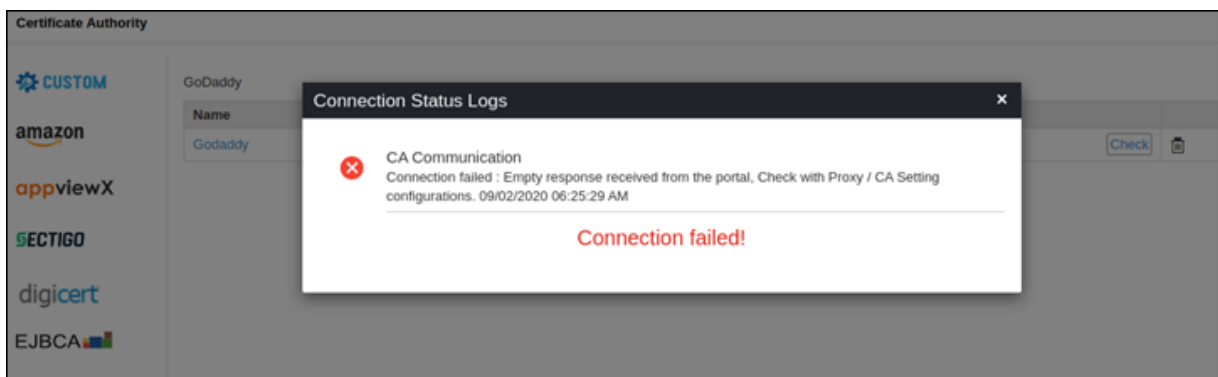
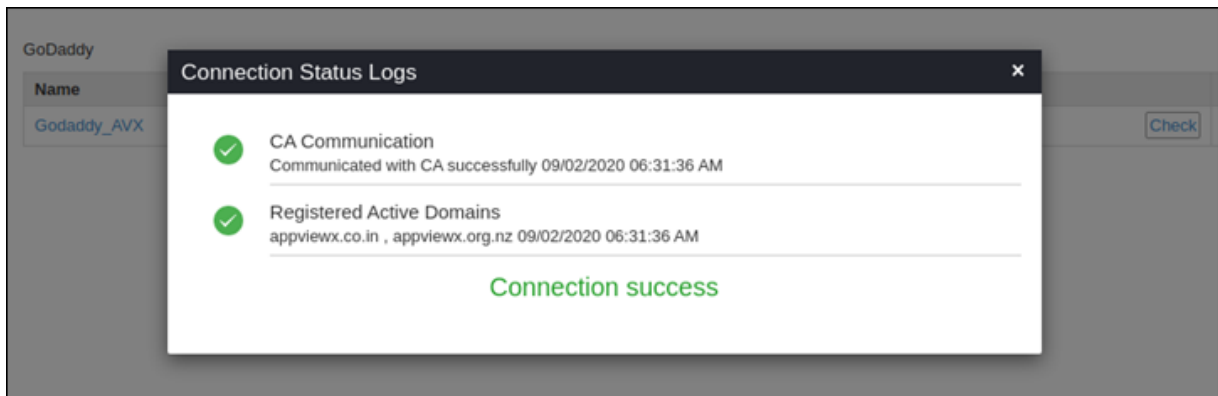
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **GoDaddy**.

The **Certificate Authority** home page appears.



6. 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 will have different types of SSL products and units, below said steps would allow users to know the availability of the products and their remaining units.

To view the GoDaddy product units,

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. Expand **ADMINISTRATION**.

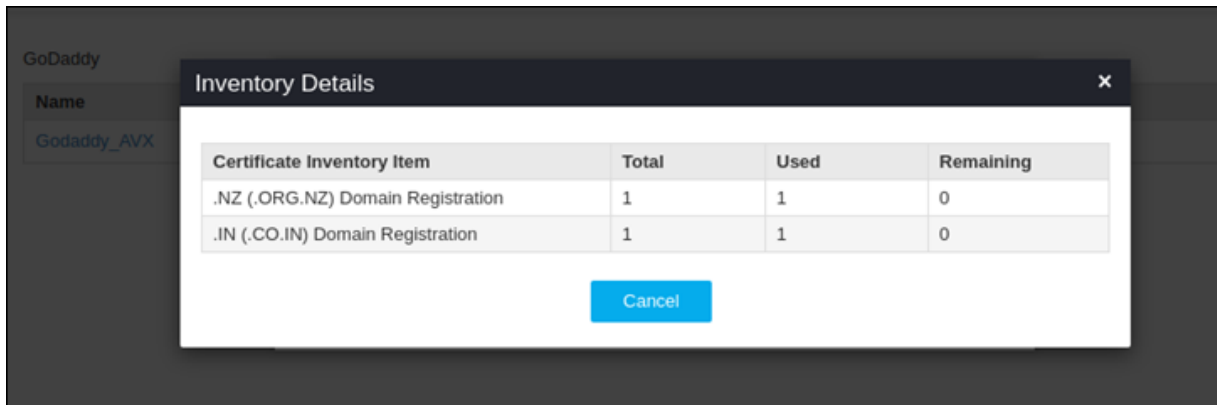
5. Click **Certificate Authority**, and then select **GoDaddy**.

The **Certificate Authority** home page appears.

The screenshot shows the CERT+ application interface. On the left is a dark navigation pane with the 'ADMINISTRATION' section expanded, and 'Certificate Authority' selected. The main content area is titled 'Certificate Authority' and features a '+ Add' button in the top right. Below the title bar is a list of certificate providers: amazon, appviewX, SECTIGO, ALL THINGS DECENTRAL, digicert, EJBCA, Entrust, GlobalSign, and GoDaddy. The 'GoDaddy' provider is highlighted. A table displays the certificates for the selected provider.

Name	Purpose/Usage	Connection Status	
	Server,Client	Success	Check

6. 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.



Google CA

- Before you begin
- Configuring Google
- Validating Google

Before you begin

Following are the prerequisites for configuring a Google CA account in AppViewX

- Need to have 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.
- From AppViewX, <https://www.googleapis.com> should be reachable.

Configuring Google

To configure the Google CA,

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.

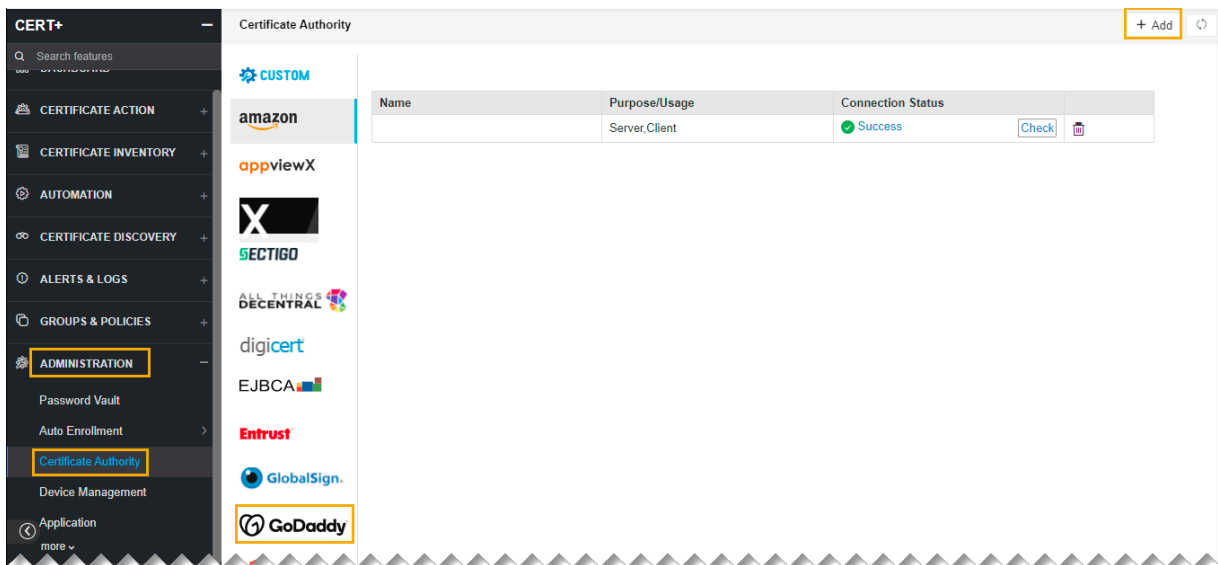
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select Google.

The **Certificate Authority** home page appears.



6. Click the +Add icon on the top right of the page.

The Google configuration page appears.

Certificate Authority

< Google

General Information

* Name

* Purpose/Usage

None Selected

Proxy Required

☐

Data Center (AppViewX's CA agent)

absecon

CA Configuration

* Configure With

☒ Certificate Upload
 ☐ JSON Upload

* Certificate and Key

filename.pkcs

Upload

* Email Address

* Project Id

Please validate the credentials to fetch CA names from Google account.

Save

Cancel

7. Update the following details in the **General Information** section as described in the table:

Name	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.

Name	Description
*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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. Configure it 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.

Options	Description
*Certificate and Key	Client authentication certificate for API communication.
*Email address	Email address of the user
*Project Id	Id of the project
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. Select the JSON Upload check box and configure a CA. Click the Upload button to upload the JSON file.
10. 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.

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	

11. 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. To validate the Google CA,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

The left navigation pane appears.

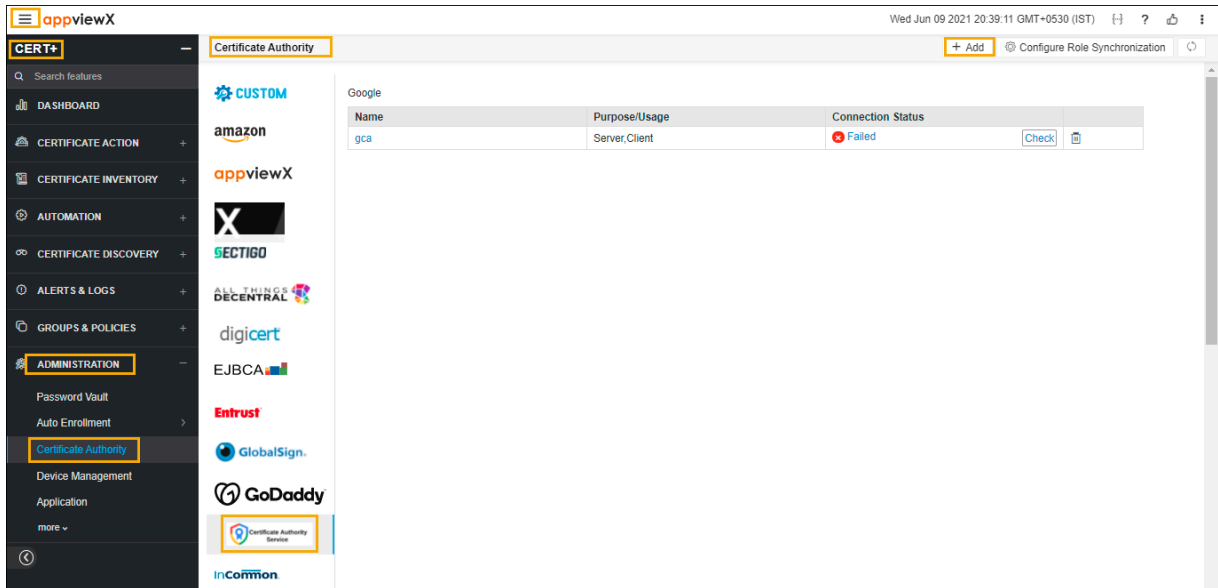
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

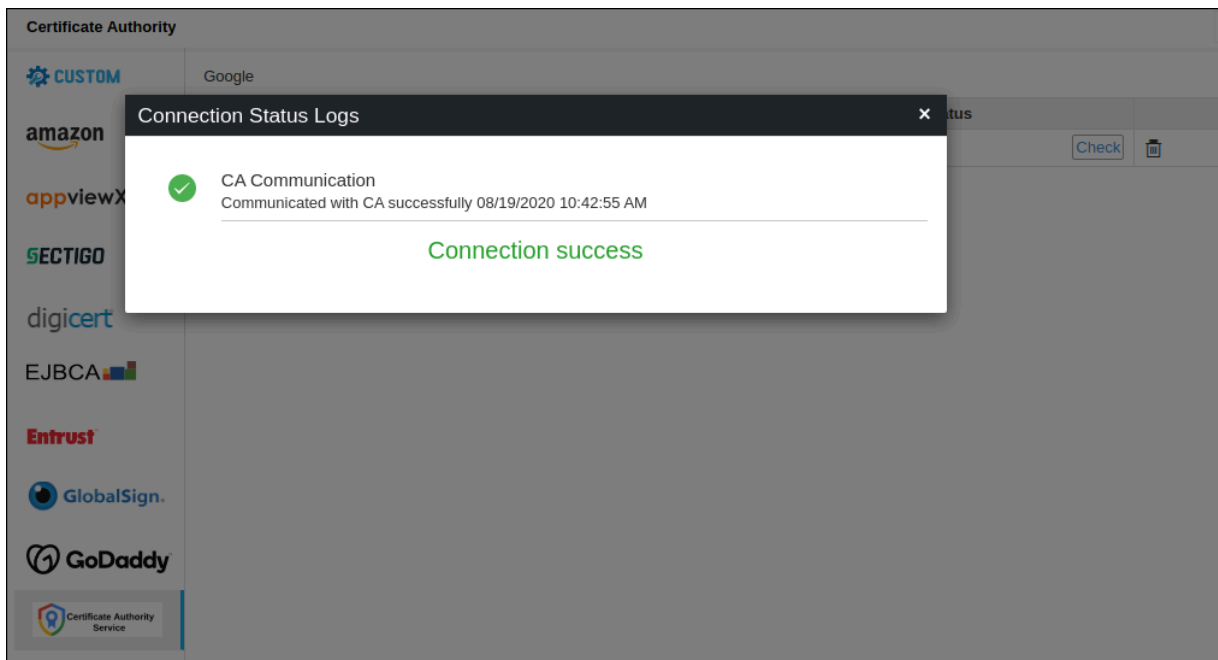
4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select Google.

The **Certificate Authority** home page appears.



6. Click Check to validate the CA setting that is created.
7. CA communication will be validated and the Connection Status will be shown as either Success or Failure.



InCommon CA

- [Before you begin](#)
- [Configuring InCommon CA](#)
- [Validating InCommon CA](#)

Before you begin

Following are the prerequisites for configuring InCommon CA account in AppViewX:

- Need to have 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.
- Need OrgID as provided by InCommon Certificate Manager.
- Need login URL and URI.

Configuring InCommon CA

To configure the InCommon CA,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

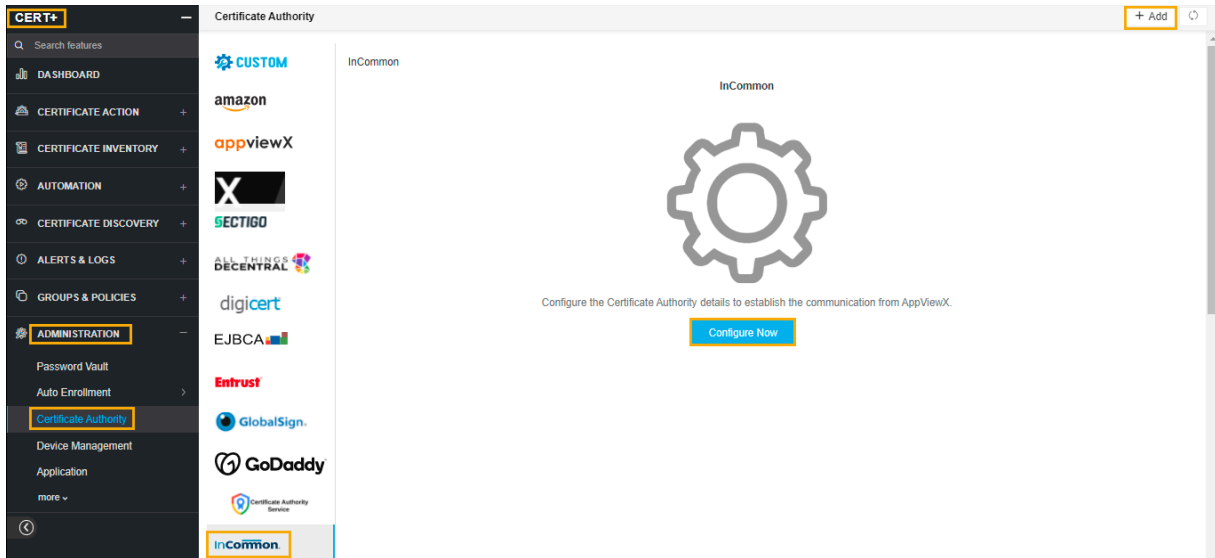
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **InCommon**.

The **Certificate Authority** home page appears.



6. Click the +Add or **Configure Now** icon on the top right of the page.

The **InCommon** configuration page appears.

Certificate Authority

< InCommon

General Information

* CA Account name

Techdoc

* Purpose/Usage

Server

Proxy Required

☒

Please contact support/admin to restart the AppViewX CA agent when proxy required is enabled/disabled or proxy settings in Menu>> Certificate>> Administration >> General Settings Proxy is modified

Data Center (AppViewX's CA agent)

absecon

CA Configuration

* Base URL

* Login URI

* User Name

* Password

Save

Cancel

Fetch Custom Attributes

7. Update the following details in the **General Information** section as described in the table:

Name	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.

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Name	Description
*Base URL	This URL will contain just the hostname of the InCommon CA instance. Eg - <a href="https://cert-manager.com/customer/<<customer_uri>>/ssl">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 <a href="https://cert-manager.com/customer/<<customer_uri>>/ssl">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.
Note:	

Name	Description
 Note: • The asterisk (*) symbol indicates a mandatory field. • 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.	

9. Select **Fetch Certificate Types**.

The Certificate types available for the CA account will be fetched from the Certificate Authority.

10. Click **Save**.

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. To validate the InCommon CA,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

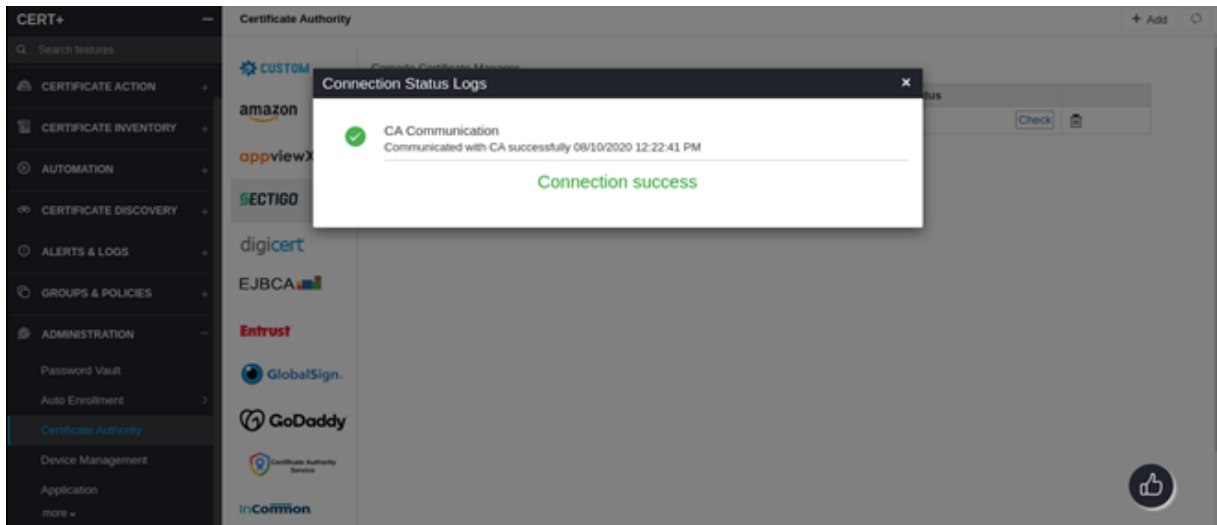
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **InCommon**.
6. 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

Following are the prerequisites for configuring Let's Encrypt CA account in AppViewX:

- 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>
- Need to provide any one of the following Let's Encrypt certificate enrolment URL as per requirement :
 1. <https://acme-staging-v02.api.letsencrypt.org> for **staging**.
 2. <https://acme-v02.api.letsencrypt.org> for **production**.

Configuring Let's Encrypt CA

To configure the Let's Encrypt CA,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

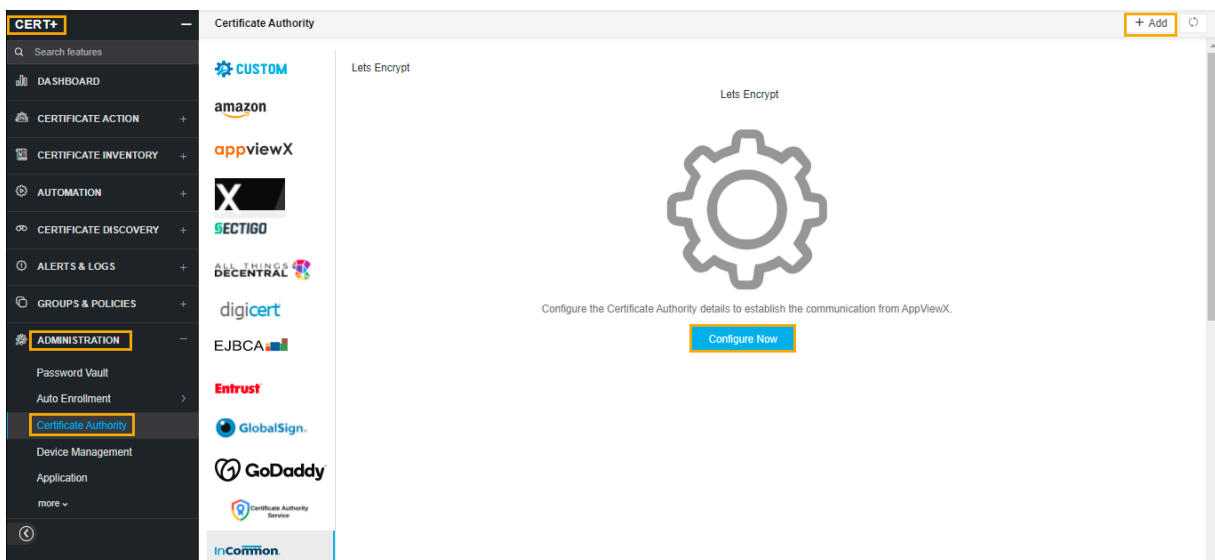
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Let's Encrypt**.

The **Certificate Authority** home page appears.



6. Click the +Add icon or **Configure Now** icon on the page.

The Let's Encrypt configuration page appears.

Certificate Authority

< Lets Encrypt

General Information

* CA Account name

* Purpose/Usage

None Selected

Proxy Required

☐

Please contact support/admin to restart the AppViewX CA agent when proxy required is enabled/disabled or proxy settings in Menu>> Certificate>> Administration >> General Settings Proxy is modified

Data Center (AppViewX's CA agent)

absecon

CA Configuration

* Base URL

https://acme-v02.api.letsencrypt.org

Email ID(s)

Save

Cancel

7. Update the following details in the **General Information** section as described in the table:

Name	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.

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Name	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 (,).
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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. To validate the Let's Encrypt CA,

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. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Let's Encrypt**.
6. 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

Following are the prerequisites for configuring Microsoft Enterprise CA in AppViewX

AppViewX Windows Gateway installer should be installed in a windows machine, running and reachable from AppViewX vendor plugin(s) **Communication Mode**

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account
	User permission		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

Communication mode	Category	Windows gateway machine	Microsoft CA
			certutil.exe command availability
	Ports		135 as the incoming port
POWERSHELL	User account type	Service account	Service account.
	User permission		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		5985
WMI	User account type	Service account	Service account
	User permission		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

Communication mode	Category	Windows gateway machine	Microsoft CA
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	NA.	135, 445 or 139

Configuring Microsoft Enterprise CA

To configure the Microsoft enterprise CA,

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 **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Microsoft**.

The **Certificate Authority** home page appears.

6. Select the **Enterprise** tab and click **Add** or **Configure Now**.
7. Update the following details in the **General Information** section as described in the table:

Name	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, Code Signing

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. Update the following details in the **CA Configuration** section as described in the table.

Name	Description
*Windows Gateway URL	Enter the URL where the AppViewX agent is running.
*Windows Gateway Type	The mode of communication types from Windows Gateway machine to CA machine. Available types are NATIVE API , POWERSHELL , WMI . Refer Communication Mode
Client Authentication Certificate	The client certificate used while installing Windows Gateway. Users can use the default client certificate (ClientCertificateGateway.pfx) or the custom certificate given by the Customer.
*Credential Type	Type of credential to be used. Either Manual Entry or Credential List .
Username	User name of the credentials.
Password	Password for the username.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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**.

10. Click on one specific CA and proceed.

GlobalSign
 GoDaddy
 Certificate Authority Service
 InCommon
 Let's Encrypt
 Microsoft
 Symantec
 Trustwave
 Programmable
 Known

*** Windows Gateway URL** ⓘ

Windows Gateway Type ☒ Native API ☐ POWERSHELL ⓘ
☐ WMI

Client Authentication Certificate Upload ⓘ

Fetch CA Names and Server Details.
Click to fetch the available Microsoft CAs in the domain.

Fetch CA Names

Select CA ▼

*** CA Machine Hostname** ⓘ

*** CA Name** ⓘ

CA Manager Approval ☐ ⓘ

*** Time Zone** ⓘ

Name	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.
*Time Zone	To perform scheduled and Optimized CA discovery, please provide time zone value.
Note: The asterisk (*) symbol indicates a mandatory field.	

Using Native API

Using Powershell and WMI

1. Configure the **Template Details**.

Once CA is selected from the **Select CA** list, the **Template** details should have auto-filled as shown below.

Template Name	OID	Action
testcreate	1.3.6.1.4.1.311.21.8.9988521.11120394.14369442.2024444.12371783.122.16647478.14904988	
ServerAndClientAuth	1.3.6.1.4.1.311.21.8.9988521.11120394.14369442.2024444.12371783.122.16389053.1742441	
AllEKUs	1.3.6.1.4.1.311.21.8.9988521.11120394.14369442.2024444.12371783.122.16750408.13078327	
CustomEku	1.3.6.1.4.1.311.21.8.9988521.11120394.14369442.2024444.12371783.122.2289813.6663087	
Web Server	1.3.6.1.4.1.311.21.8.9988521.11120394.14369442.2024444.12371783.122.11497616.5606298	



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.

2. In the Template Details section, select/enter the details as shown below.

Template Details

You can either manually enter template details or upload a file.

* MS Template Name ⓘ

OID ⓘ

[Add](#)

OR

Upload File [Upload](#)

Uploaded details will be added automatically. [Download Sample Template](#)

3. 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. To validate the Microsoft enterprise CA,

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.

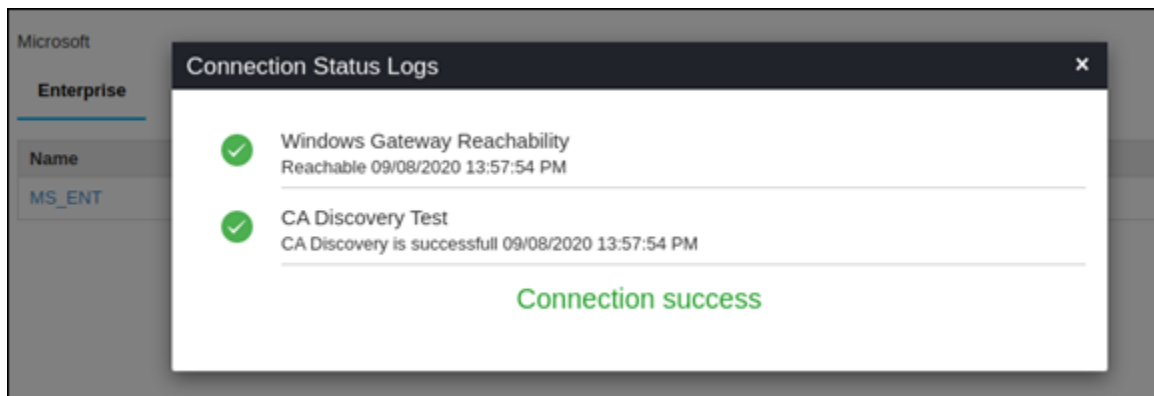
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

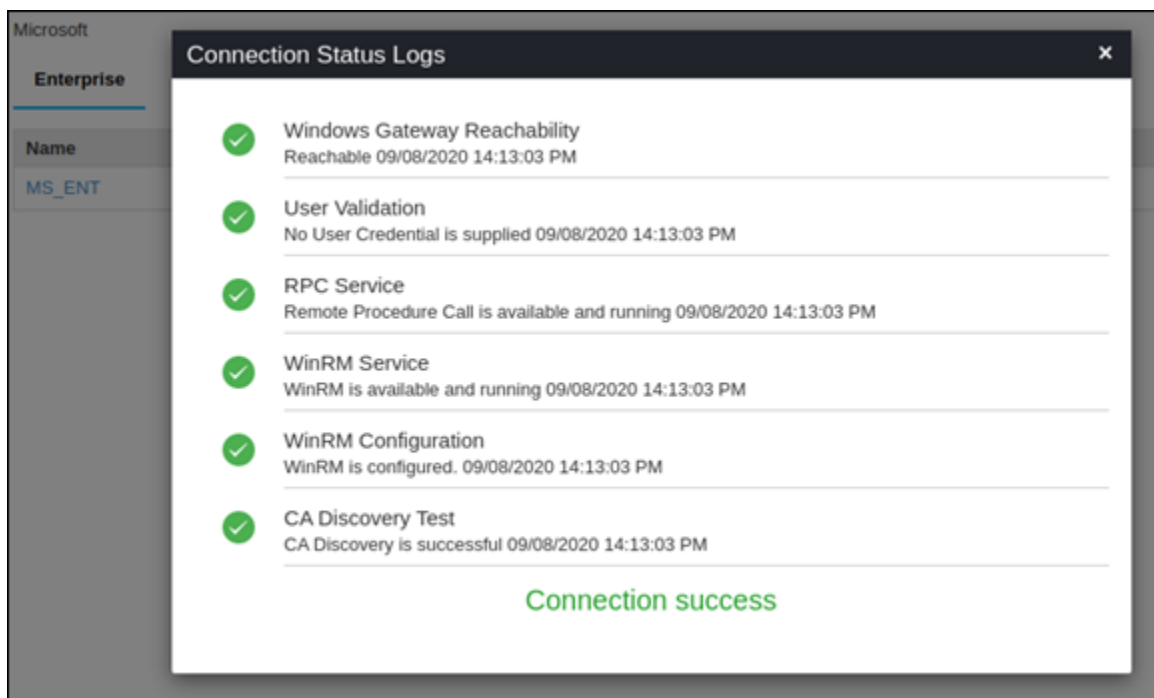
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Microsoft Enterprise**.
6. Click **Check** to validate the CA setting that has been created.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

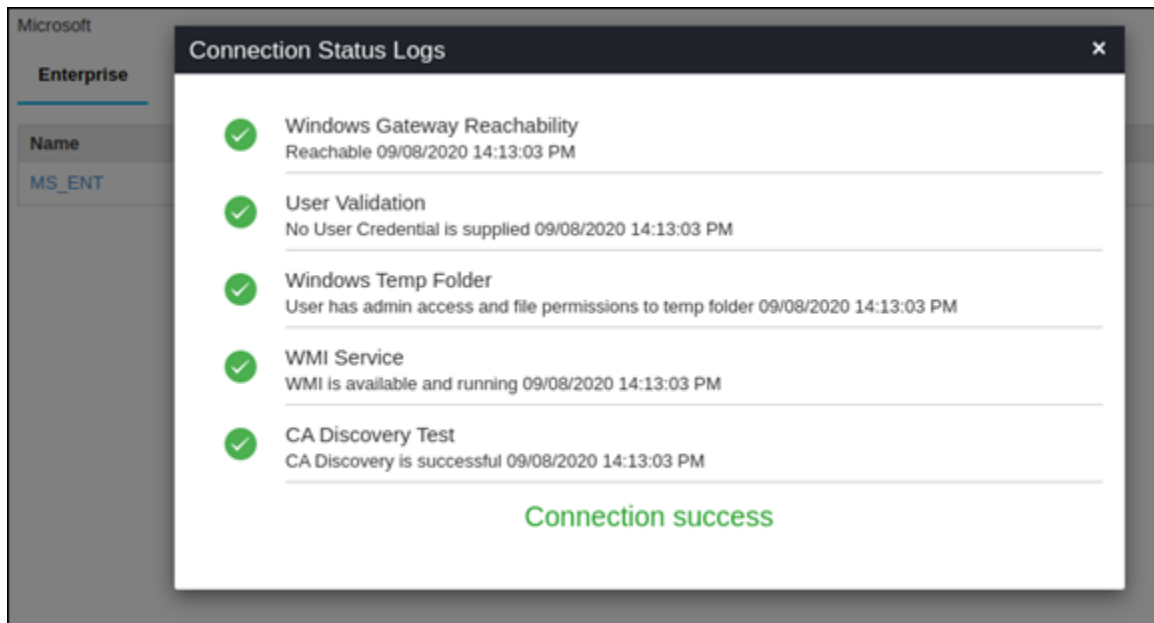
Success Message.



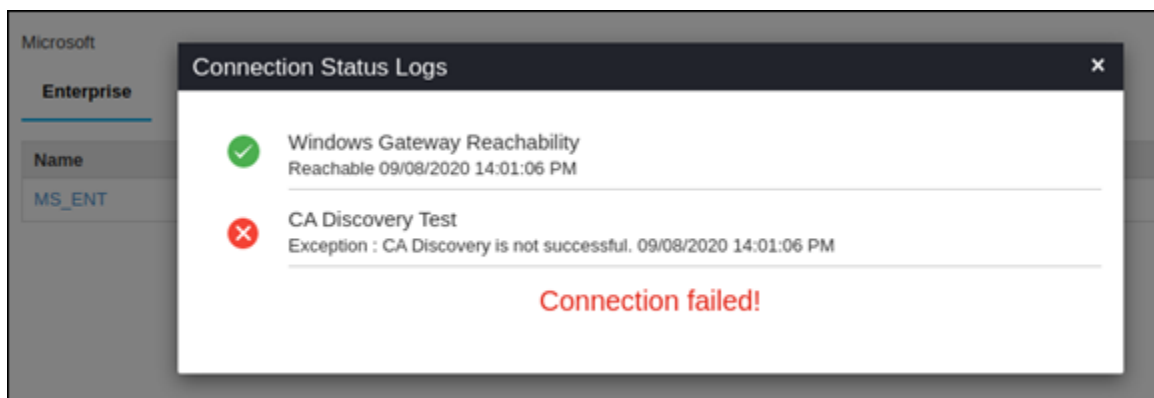
Success Scenario for Native API



Success Scenario for Powershell



Success scenario for WMI



Microsoft Standalone CA

- Before you begin
- Configuring Microsoft Standalone CA
- Validating Microsoft Standalone

Before you begin

Following are the prerequisites for configuring Microsoft Standalone CA in AppViewX:

- AppViewX Windows Gateway installer should be installed in a windows machine, running and reachable from AppViewX vendor plugin.

Communication Mode

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account
	User permission		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		135 as incoming port
POWERSHELL	User account type	Service account	Service account
	User permission		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

Communication mode	Category	Windows gateway machine	Microsoft CA
	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		5985
WMI	User account type	Service account	Service account
	User permission		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		135, 445 or 139

Configuring Microsoft Standalone CA

To configure the Microsoft standalone CA,

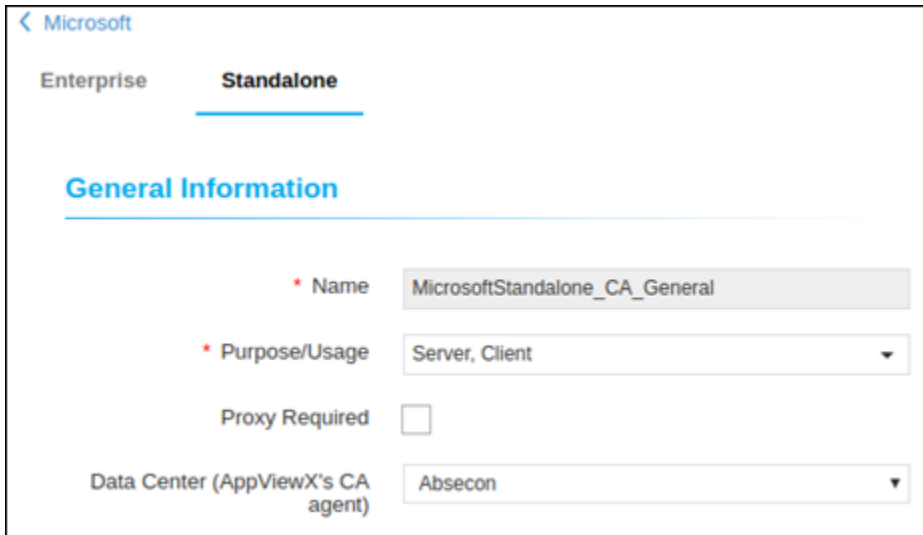
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Click **CERT+**.
The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select **Microsoft**.

The **Certificate Authority** home page appears.

6. Select the **Standalone** tab and click **Add** or **Configure Now**.

7. Update the following details in the **General Information** section as described in the table.



Microsoft

Enterprise **Standalone**

General Information

* Name MicrosoftStandalone_CA_General

* Purpose/Usage Server, Client

Proxy Required ☐

Data Center (AppViewX's CA agent) Absecon

Name	Description
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, 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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. Update the following details in the **CA Configuration** section as described in the table:

Name	Description
*Windows Gateway URL	Enter the URL where the AppViewX agent is running.
*Windows Gateway Type	The mode of communication types from Windows Gateway machine to CA machine. Available types are NATIVE API , POWERSHELL , WMI .
Client Authentication Certificate	The client certificate used while installing Windows Gateway. Users can use the default client certificate (Client Certificate Gateway.pfx) or the custom certificate given by the Customer.
*Credential Type	Type of credential to be used. Either Manual Entry or Credential List .
Username	User name of the credentials.
Password	Password for the username.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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**.

10. Click on one specific CA and proceed.

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

Using Native API

Certificate Authority

CA Configuration

GlobalSign.

GoDaddy

Certificate Authority Service

InCommon

Let's Encrypt

Microsoft

Symantec

Trustwave

Programmable

Known

* Windows Gateway URL ⓘ

Windows Gateway Type ☒ Native API ☐ POWERSHELL ⓘ
☐ WMI

Client Authentication Certificate ⓘ

Fetch CA Names and Server Details.
Click to fetch the available Microsoft CAs in the domain.

* CA Machine Hostname ⓘ

* CA Name ⓘ

CA Manager Approval ☐ ⓘ

Using Powershell and WMI

11. Click **Save**.

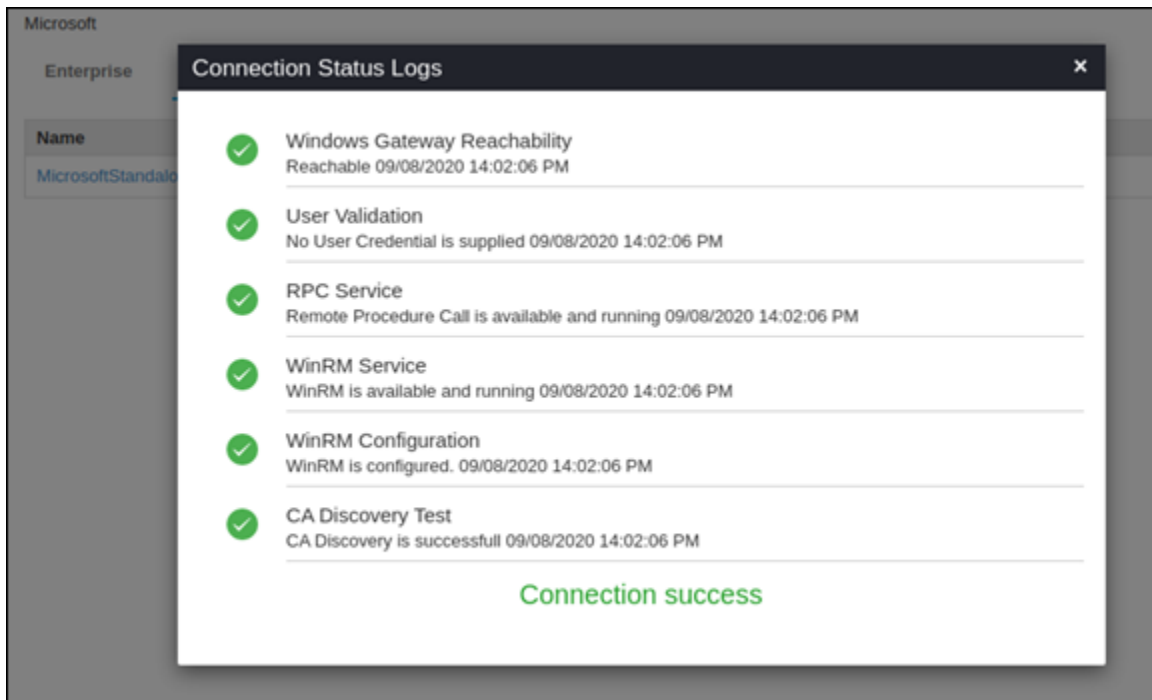
Validating Microsoft Standalone

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. To validate the Microsoft standalone CA,

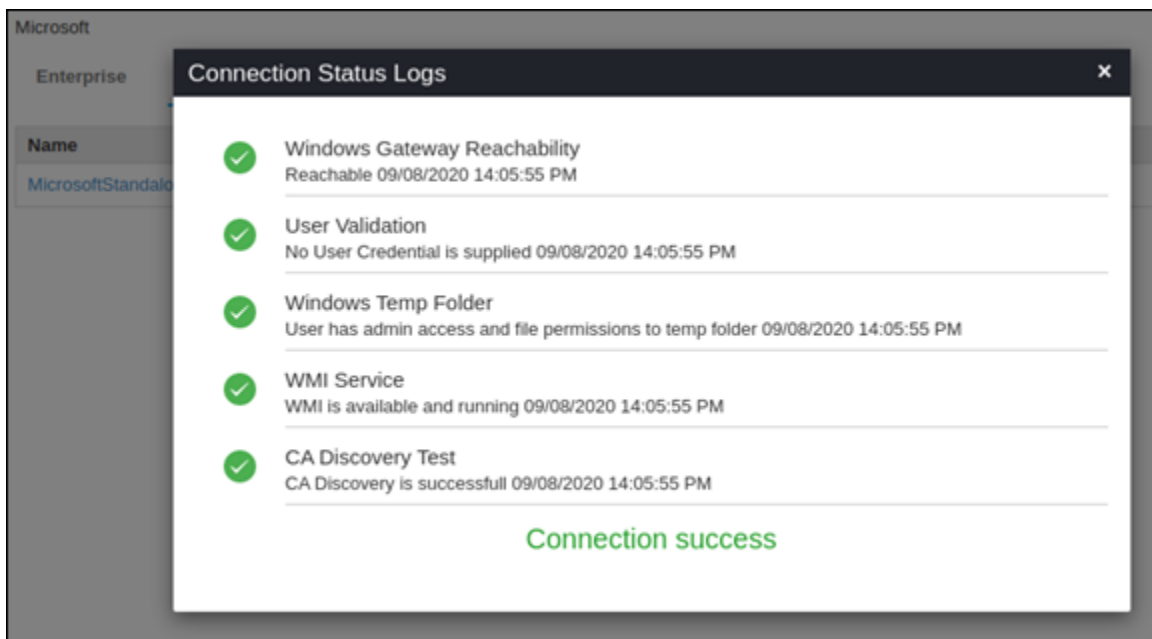
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Click **CERT+**.
The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Microsoft Standalone**.
6. 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 API Success scenario for Powershell Success scenario for WMI.

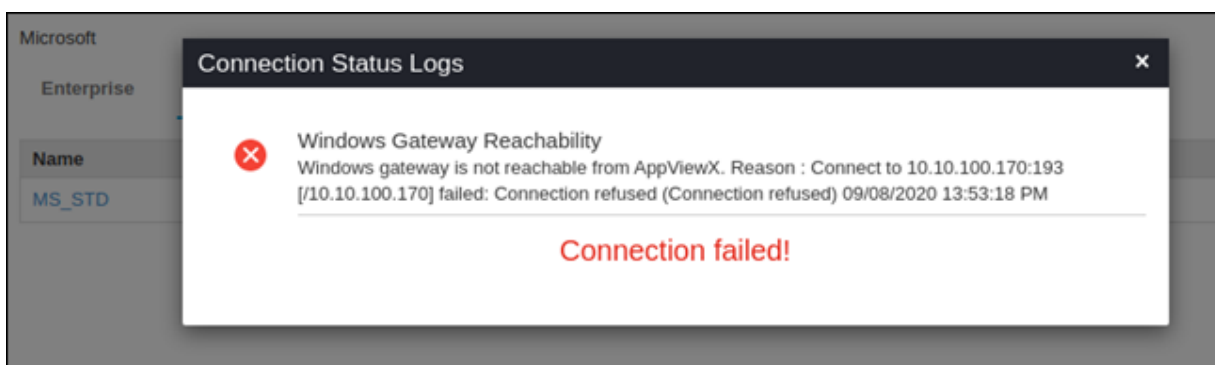
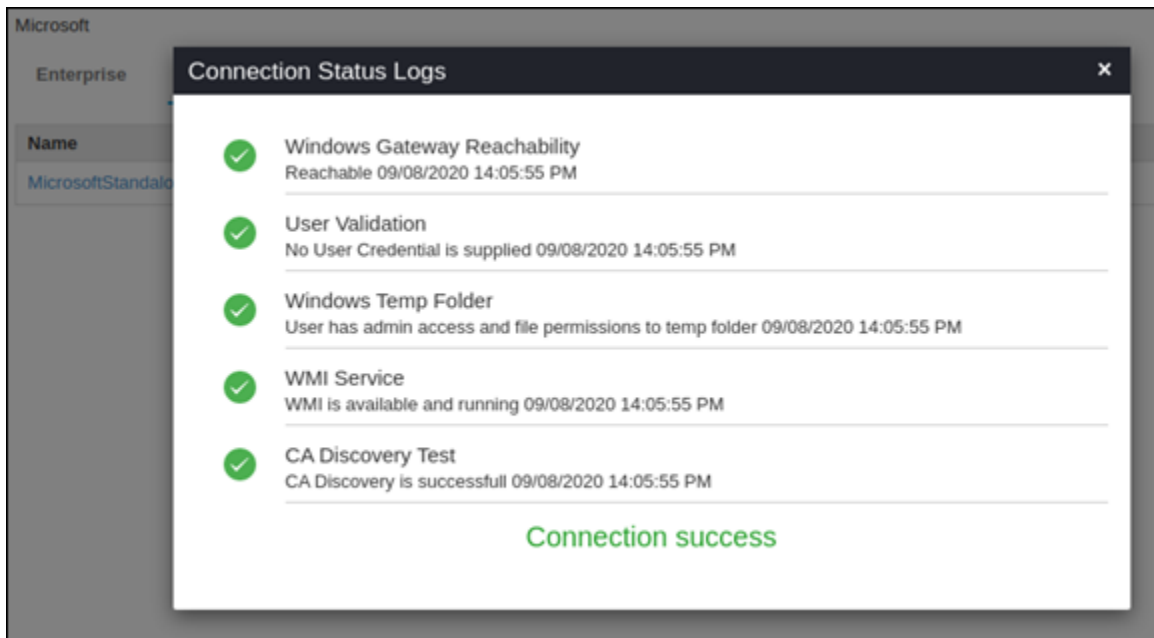
Success scenario for Native API



Success scenario for Powershell



Success scenario for WMI



Symantec CA

- [Before you begin](#)
- [Configuring Symantec CA](#)
- [Validating Symantec](#)

Before you begin

Following are the prerequisites for configuring a Symantec account in AppViewX:

- Need to have 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.
- Required certificate types should be enabled with the required values in the portal.
- Units value should be available for the required certificate type.

Configuring Symantec CA

To configure the Symantec CA,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

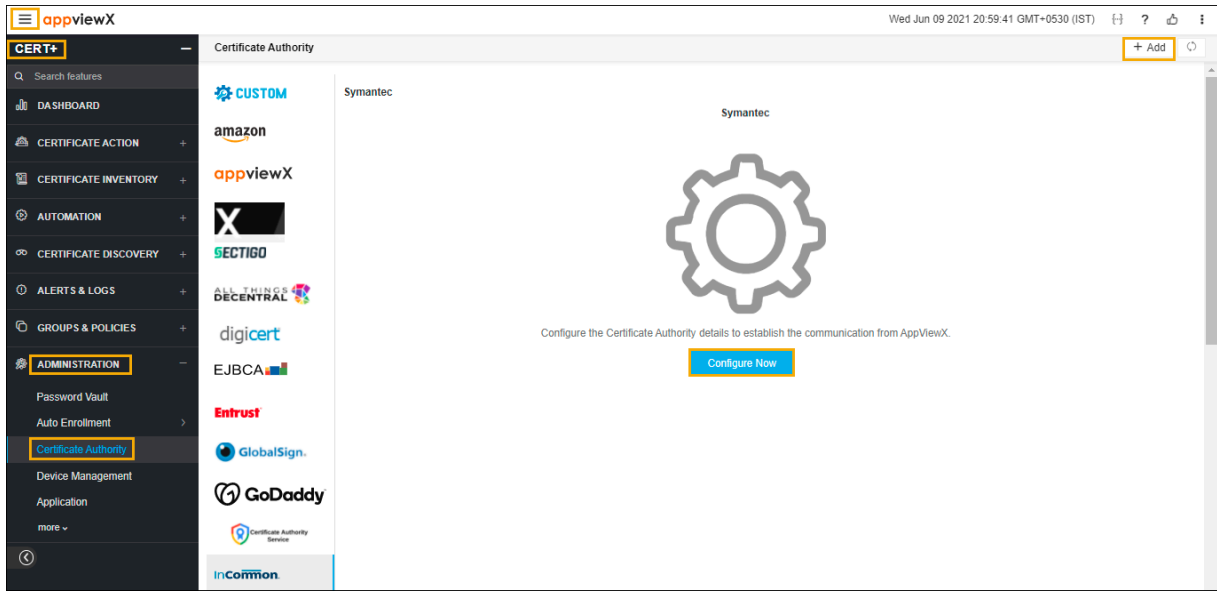
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Symantec**.

The **Certificate Authority** home page appears.



6. Click **Add** or **Configure Now**.

The **Symantec** configuration page appears.

Certificate Authority

< Symantec

General Information

* Name

* Purpose/Usage

None Selected

Proxy Required

☐

Data Center (AppViewX's CA agent)

absecon

CA Configuration

* Certificate and Key

filename.pkcs

Upload

* URL

* Jurisdiction Hash

* First Name

* Last Name

* Email Address

Save

Cancel

Fetch Custom Attributes

7. Update the following details in the **General Information** section as described in the table.

Name	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.

Name	Description
*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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. 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.

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. 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. To validate the Symantec CA,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

The left navigation pane appears.

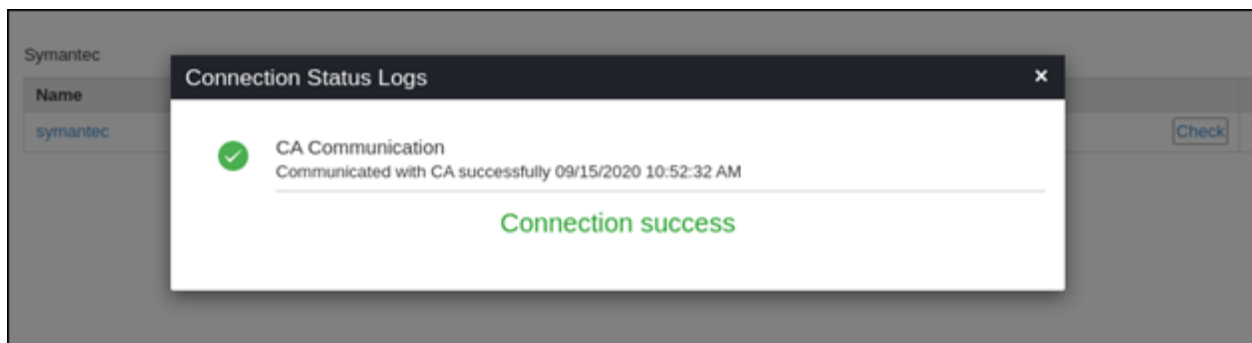
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

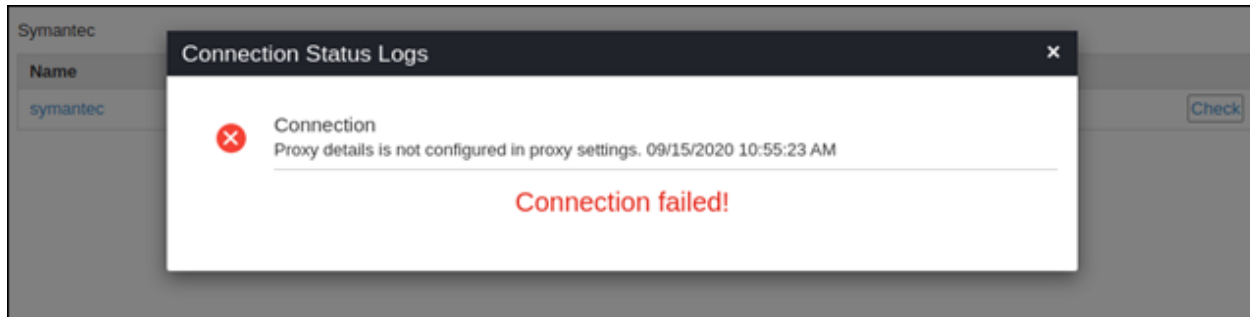
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Symantec**.
6. Click **Check** to validate the CA setting that has been created.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Success Scenario



Failed Scenario



Trustwave CA

- Before you Begin
- Configuring Trustwave CA
- Validating Trustwave

Before you Begin

Following are the prerequisites for configuring Trustwave CA in AppViewX:

- 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 in Trustwave 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. Check Proxy Setup for the steps to configure the proxy. <https://adminguide.appviewx.com/proxy-4>

Configuring Trustwave CA

To configure the Trustwave CA,

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.

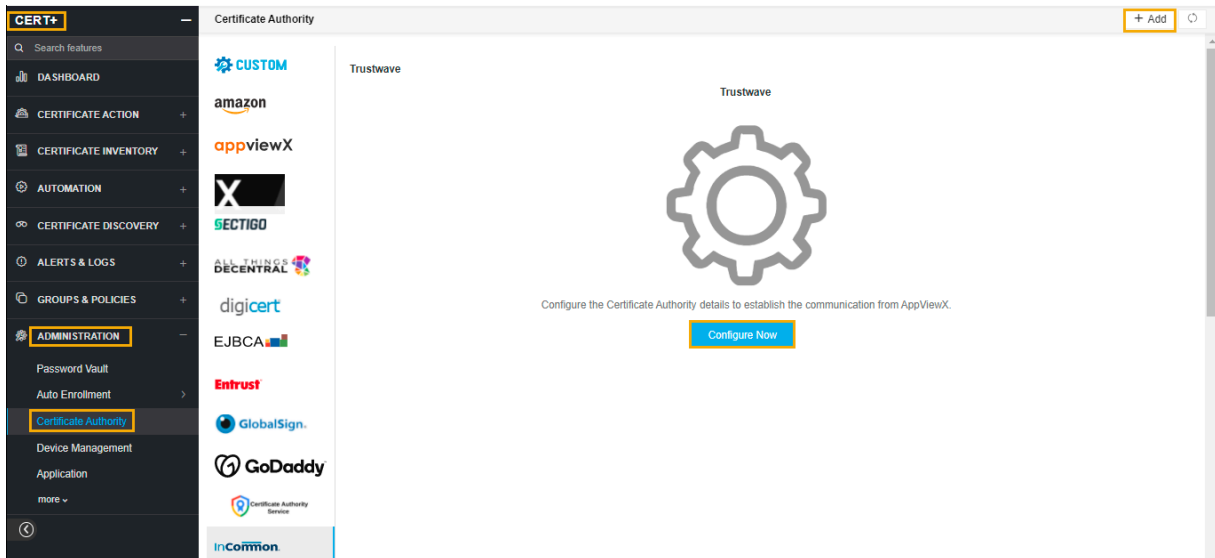
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

5. Click **Certificate Authority**, and then select **Trustwave**.

The **Certificate Authority** home page appears.



6. Select **Add** or **Configure Now**.

7. Configure the **General Information** details as follows:

- a. **CA Account name** - Provide an account name for the CA setting.
- b. **Purpose/Usage** - Choose the certificate categories that will be managed by this setting. Possible certificate categories could be:
 - i. Server
 - ii. Code Signing
- c. **Proxy Required** - Enable this field if the CA communication needs to happen via **Proxy**.

d. Choose the appropriate **Data Center**.

8. Configure the **CA Configuration** with information you want to configure:
 - a. **API URL**: The Trustwave API URL to communicate. Ex: <https://testapi.ssl.trustwave.com/3.0/>
 - b. **Username**: The username for API authentication.
 - c. **Password**: The password for API authentication.
 - d. **Reseller ID**: The Reseller Id for the account.
9. Configure the **Account Details** with information you want to configure:
 - a. **Name**: The Organization name given in the Trustwave account.
 - b. **Email Address**: The Administrator or organization email address given in the Trustwave account.
 - c. **Address**: The Organization Address given in the Trustwave account.
 - d. **City**: The city name given in the Trustwave account.
 - e. **State**: The state name given in the Trustwave account.
 - f. **Zip code**: The zip code given in the Trustwave account.
 - g. **Country**: The country code given in the Trustwave account. Ex: US.
 - h. **Phone number**: The phone number given in the Trustwave account.
10. 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. To validate the Trustwave CA,

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. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Trustwave**.
6. 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**.

GlobalSign MSSL

- [Configuring GlobalSign MSSL](#)
- [Validating GlobalSign MSSL](#)
- [Limitations](#)

Configuring GlobalSign MSSL

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

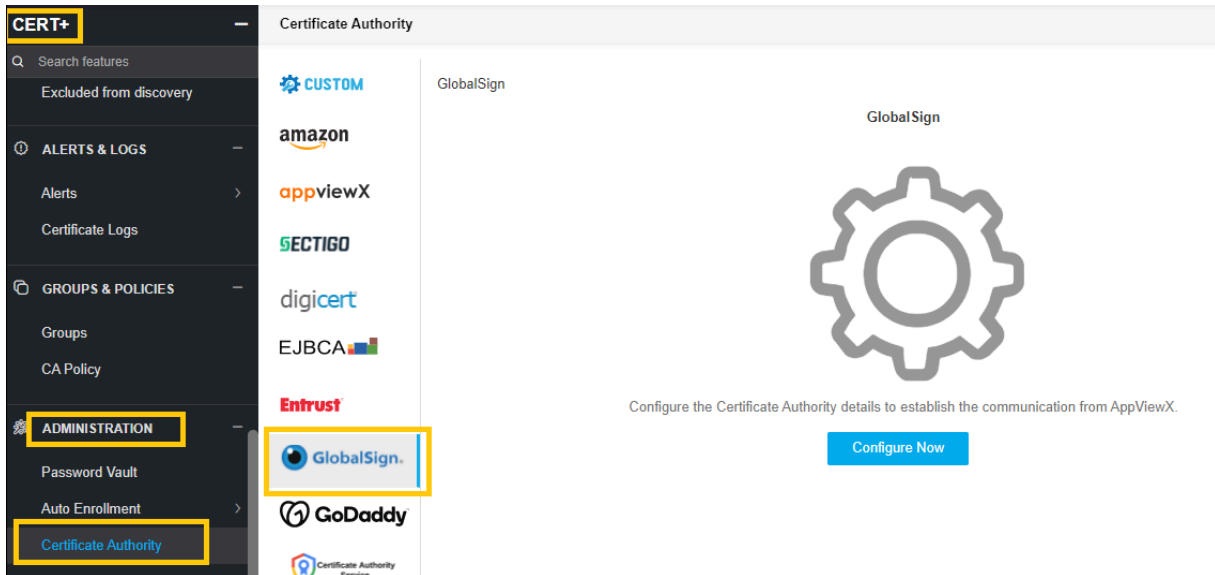
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

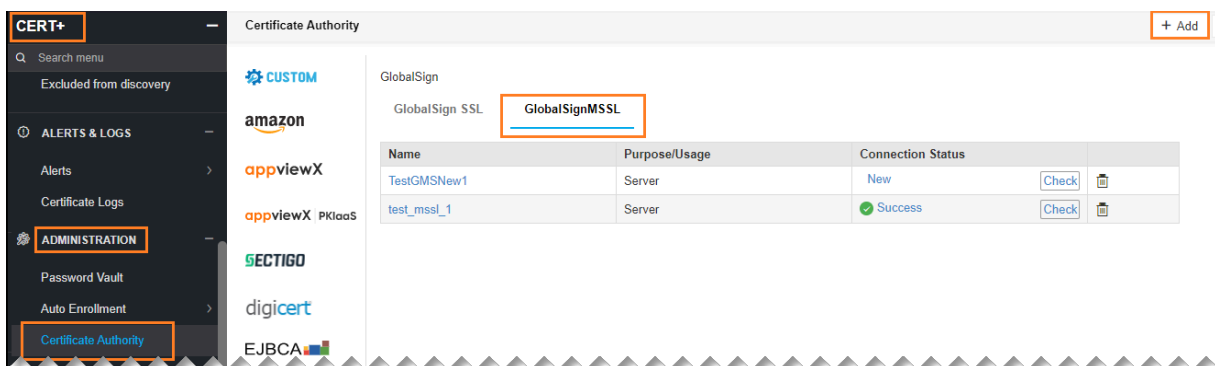
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select GlobalSign.

The **Certificate Authority** home page appears.



6. Click the **Configure Now** icon.

The GlobalSign configuration page appears.



7. Update the following details in the **General Information** section as described in the table.

< GlobalSign

General Information

* CA Account name ⓘ

* Purpose/Usage ⓘ

Proxy Required ☒ ⓘ

Please contact support/admin to restart the AppViewX CA agent when proxy required is enabled/disabled or proxy settings in Menu>> Certificate>> Administration >> General Settings Proxy is modified

Data Center (AppViewX's CA agent) ⓘ

Name	Description	Validation
*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	NA
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.	NA
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.	NA


Note: The asterisk (*) symbol indicates a mandatory field.

8. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration

* SSL URL

* User Name

* Password

Options	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.


Note: The asterisk (*) symbol indicates a mandatory field.

9. Once all the details are configured, click **Save**.

10. In GlobalSign MSSL, we can now fetch profiles and domains by clicking on the **Fetch Profiles and Domain** button.







CA Configuration

* SSL URL

* User Name

* Password

Domain name

Profile ID

No records found

Update

Cancel

Fetch Profile and Domains



Note: The supported CSR key types are RSA 2048-8192, ECC P-256, ECC P-384 .

Validating GlobalSign MSSL

Once the GlobalSign settings are added, validation needs to be done to check whether the connection between AppViewX and GlobalSign is properly configured.

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

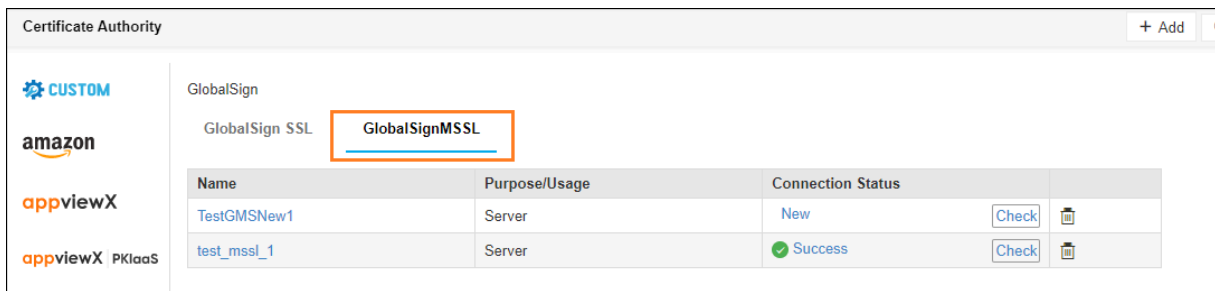
The left navigation pane appears.

3. Click **CERT+**.

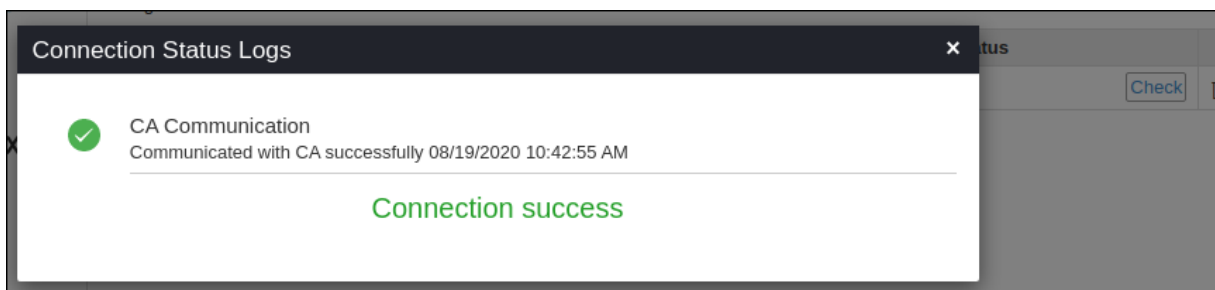
The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select GlobalSign.

The **Certificate Authority** home page appears.



6. Click **Check** to validate the CA setting that is created.
7. CA communication will be validated and the Connection Status will be shown as either Success or Failure.



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. Note: If the user clicks the Update button, MSSL domain/profile ID details will be removed from the associated policy. Steps to follow to update CA settings, 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.

GlobalSign SSL

- Configuring GlobalSign SSL
- Validating GlobalSign SSL

Configuring GlobalSign SSL

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

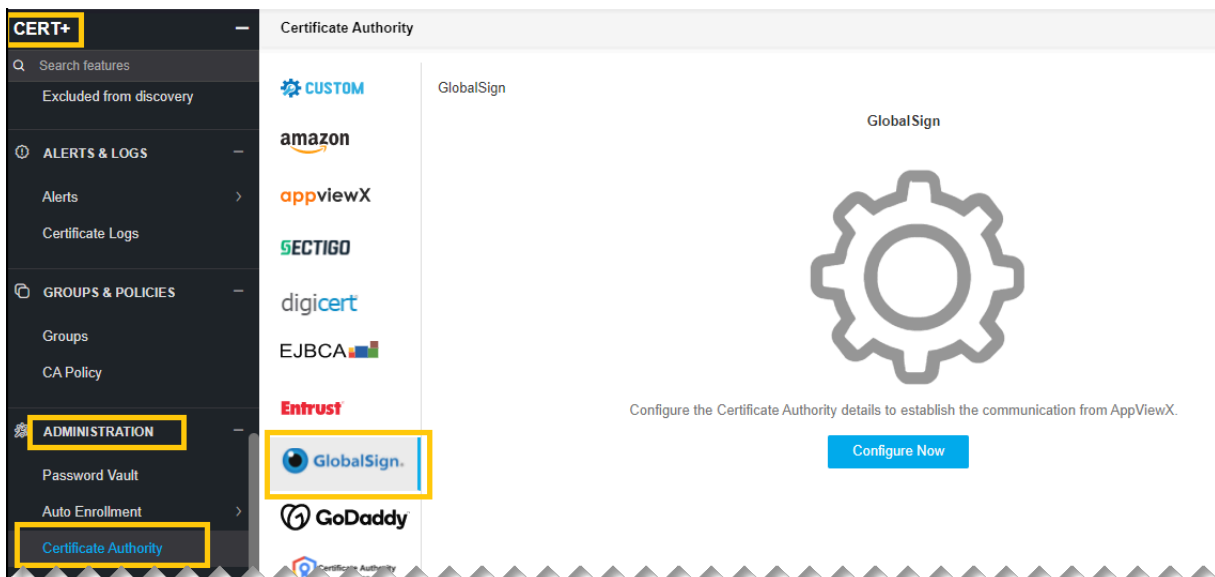
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select GlobalSign.

The **Certificate Authority** home page appears.



6. Click the **Configure Now** icon.

The GlobalSign configuration page appears.

7. Update the following details in the **General Information** section as described in the table.

[GlobalSign](#)

General Information

* CA Account name
i

* Purpose/Usage
i

Proxy Required
☒
i

Please contact support/admin to restart the AppViewX CA agent when proxy required is enabled/disabled or proxy settings in Menu>> Certificate>> Administration >> General Settings Proxy is modified

Data Center (AppViewX's CA agent)
i

Name	Description	Validation
*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.	NA
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.	NA
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.	NA

Name	Description	Validation
 Note: The asterisk (*) symbol indicates a mandatory field.		

8. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration

* SSL URL



* User Name



* Password



Options	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. Click **Save**.

Validating GlobalSign SSL

Once the GlobalSign settings are added validation needs to be done to check whether the connection between AppViewX and GlobalSign is properly configured.

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

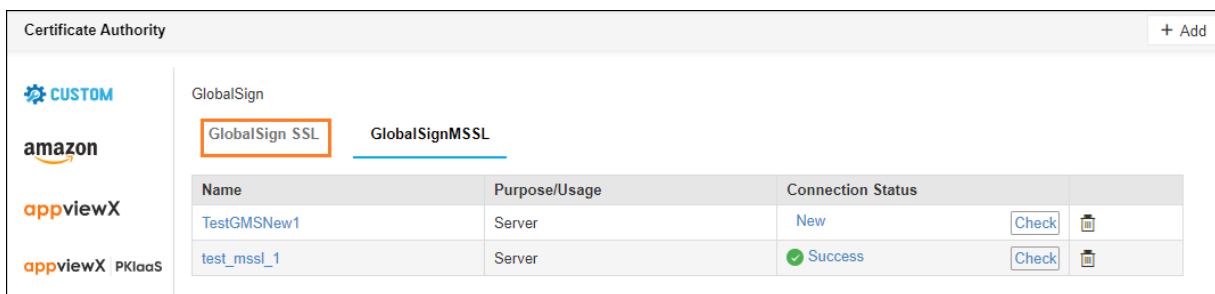
The left navigation pane appears.

3. Click **CERT+**.

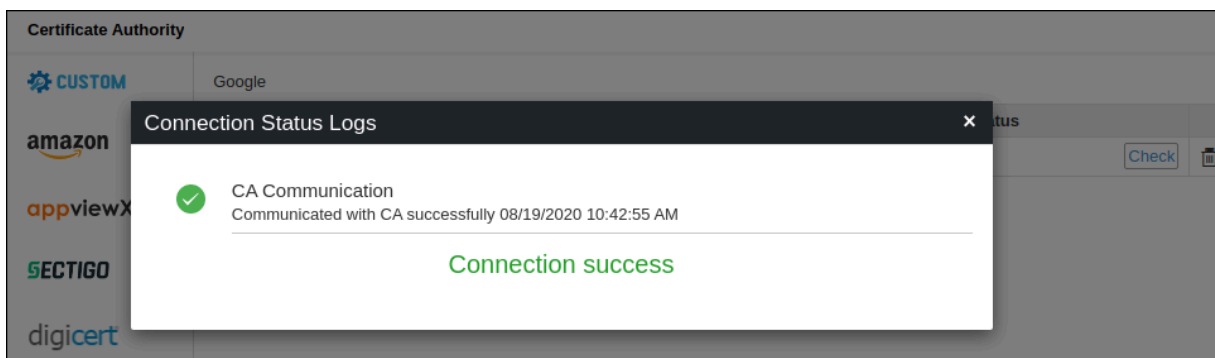
The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select GlobalSign.

The **Certificate Authority** home page appears.



6. Click **Check** to validate the CA setting that is created.
7. CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Nexus

- [Nexus](#)
- [Configuring Nexus](#)
- [Validating Nexus](#)

Nexus

The following are the prerequisites for configuring a Nexus CA account in AppViewX:

- Need to have a Nexus Account with Administrator role Access.
- Before discovery or enrollment, the customer has to upload the CA certificates manually.
- The 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.

Configuring Nexus

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

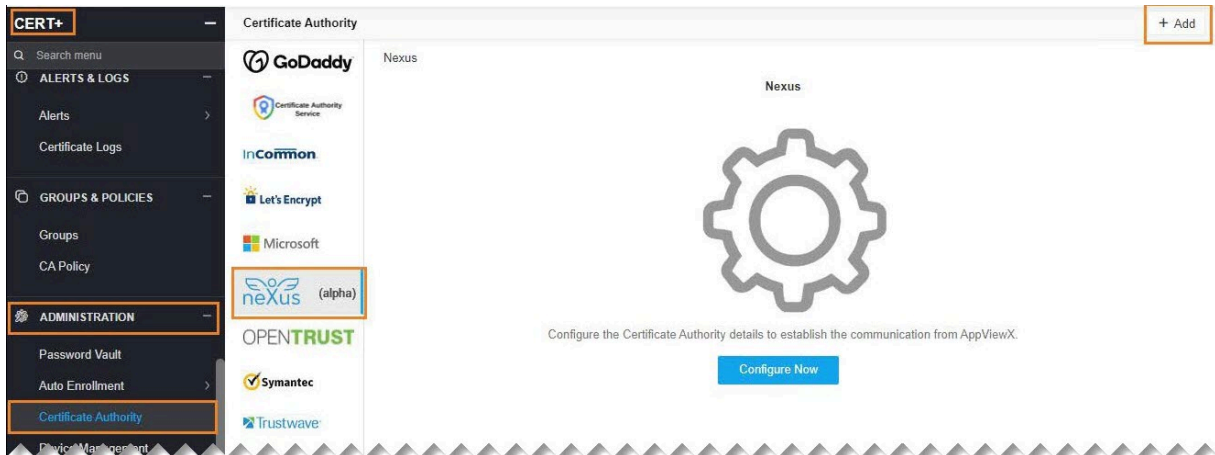
3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.

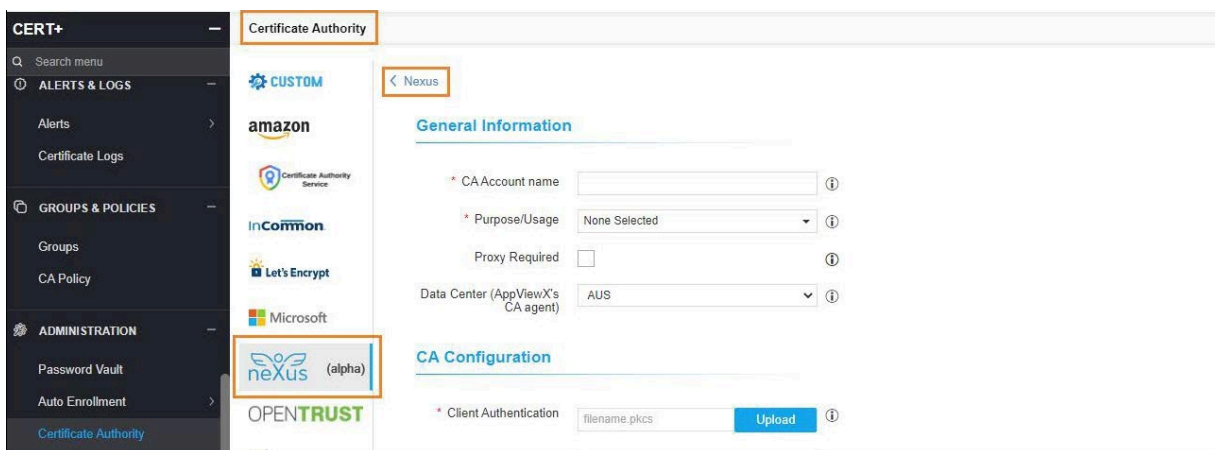
5. Click **Certificate Authority**, and then select **Nexus**.

The **Certificate Authority** home page appears.



6. Click the **Configure Now** icon.

The Nexus configuration page appears.



7. Update the following details in the **General Information** section as described in the table.

< Nexus

General Information

* CA Account name ⓘ

* Purpose/Usage ⓘ

Proxy Required ☐ ⓘ

Data Center (AppViewX's CA agent) ⓘ

Name	Description	Validation
*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	NA
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.	NA
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.	NA
 Note: The asterisk (*) symbol indicates a mandatory field.		

8. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration

* Client Authentication ⓘ

* Base URL ⓘ

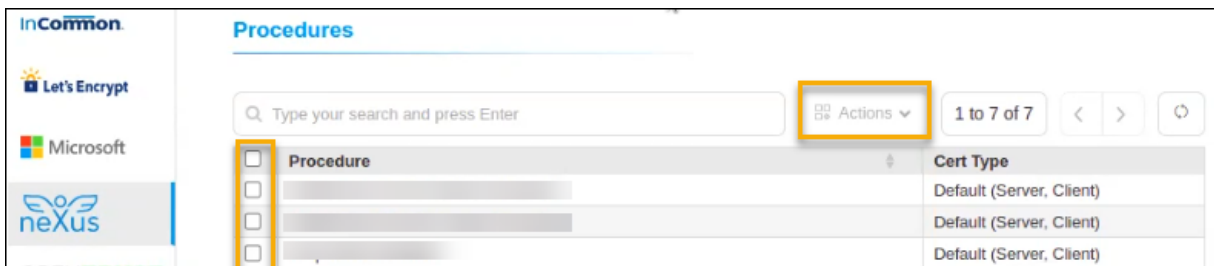
* Organization ID ⓘ

Options	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.


Note: The asterisk (*) symbol indicates a mandatory field.

9. Select **Fetch Procedures**.

The procedures available in the Nexus CA account will be fetched and listed for the specific user.



InCommon

Let's Encrypt

Microsoft

nexus

Procedures

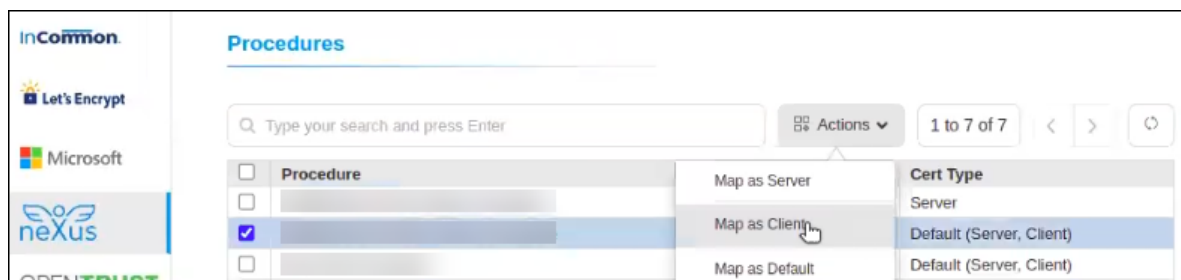
🔍 Type your search and press Enter

📄 Actions ▾ 1 to 7 of 7 < > ↺

	Procedure	Cert Type
☐		Default (Server, Client)
☐		Default (Server, Client)
☐		Default (Server, Client)

10. To map the fetched procedures, click on one or many and click the **Actions** dropdown

- a. **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**
- b. **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**
- c. **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**



11. 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. Log in to the 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+**.

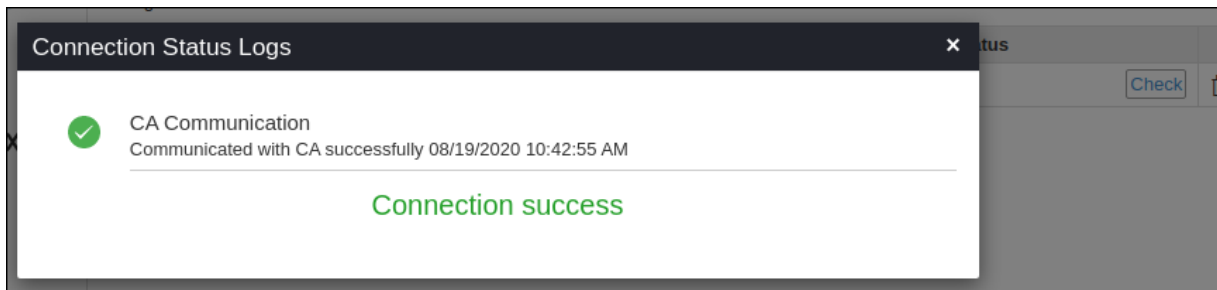
The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Nexus**.

The **Certificate Authority** home page appears.

6. Click **Check** to validate the CA setting that is created.

7. The CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Certificate Policy

- [Overview](#)
- [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 CA](#)
- [Configuring Policy for GoDaddy CA](#)
- [Configuring Policy for Google CA](#)
- [Configuring Policy for Let's Encrypt CA](#)
- [Configuring Policy for Microsoft Enterprise CA](#)
- [Configuring Policy for Microsoft Standalone CA](#)
- [Configuring Policy for OpenTrust CA](#)
- [Configuring Policy for Sectigo CA](#)
- [Configuring Policy for Symantec CA](#)
- [Configuring Policy for Trustwave CA](#)

- [Configuring Policy for GlobalSign MSSL CA](#)
- [Configuring Policy for Nexus CA](#)

Overview

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 compliant. If the certificate attribute deviates, it is marked as non-compliant and notified to users. Users can request for a new certificate (in-line to organization standards) to Certificate Authority.

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](#))

CERT > Policy > View Policy - To view the policy.

CERT > Policy > Add / Modify - To create/ modify the policy.

Configuring Policy Details

To configure policy:

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

The CA Policy home page appears.

CA Policy				+ Create	Delete
Search...				1 to 2 of 2	< > ↺
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Demo-AppViewX, Default	Strict		



Note: CERT+ is packaged with default policies they are Default and Certificate-Gateway.

6. Click + **Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description 1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval? ☒

When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key? ☒

When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user ☒

Enable certificate push-bind access for read-only user ☒

Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

The following table provides the field description in the **Policy Details** section:

Name	Description
*Policy name	Provide a unique name to identify the CA policy name.  Note: No special characters other than '.', '-', '_' are allowed. The name should not start with special characters.
Description	Provide a description of the policy.
*Policy Enforcement Type	Select Strict (or) Suggestive. By default, Strict is selected. Strict - This enforces the standards defined in the policy where a user cannot modify any parameters. Suggestive - This suggests users with policy parameters. A user can modify suggested values if required.
Certificate Requests Need Approval	When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.
Enable Access to Private Key	When enabled allows the user to download private keys from the holistic view.
Enable certificate push-bind access for a read-only user	Enabling the option might allow the user with the read-only user group to perform certificate push, bind, and rollback operations from the holistic view.
Validate issuer and root certificate for compliance	Enabling the option would validate if the Issuer and Root of the certificate are also compliant with the standard defined in the policy.
 Note: The asterisk (*) symbol indicates a mandatory field.	

7. You can configure the **Policy Details** section based on your organization's standards.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name



Description

You can tell us more about your rules and guidelines.

Policy Enforcement Type



Strict



Suggestive



Certificate Requests Need
Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

8. In the **Group selection**, select one or more groups to map to the policy.

Group selection

Search...				Add as Favorites	Favorites
☐	Select all	All	Selected	Unselected	Count: 14
☐	SopraGr				
☐	Networking				
☐	SopraGrp				
☐	CryptoOps				
☐	EndUserGroup				

No records found

Note: This policy applies to all certificates for the selected groups.

9. Under the **Compliance Check** section, you can enable the **Perform Compliance check** option to perform an immediate compliance check.

Compliance check

Perform Compliance Check



To check the compliance for the defined rules and certificates attributes of the discovered certificates.



Note: Scheduled Compliance check will run periodically based on the Job scheduler settings.

Configuring Policy for Amazon CA

To configure an Amazon CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

The CA Policy home page appears.

CA Policy				+ Create	Delete
Search...				1 to 2 of 2	Previous Next Refresh
☐ Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Demo-AppViewX, Default	Strict		

6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details** section
 - **Group Selection** section
 - **Compliance Check** section
8. To configure a policy with Amazon details, click **Amazon** in the **Certificate Authority** pane on the left side of the screen.

The following table provides the field description in the **CA Details** section:

Name	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **CA details** section, select **CA accounts** from the dropdown list.

* CAAccounts ⓘ

Add

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

CA Policy : Create ✓ Amazon - CA details table updated ✕

CA details

Define Certificate standards per Certificate Authority. Users can select the CAs configured with the policy while performing certificate operations.

Certificate Authority

☐ General

☒ Amazon

* CAAccounts ⓘ

Add

CA Accounts	Remove
AWS CA	
nhg-test-aws-prviateCA	

11. You can use the **Remove** option to delete the configuration.

CA Accounts	Remove
AWS CA	
nhg-test-aws-prviateCA	

12. In the CA details section, select the **Bit Length -Key Type(s)**, **ECDSA curve(s)**, and **Hash Function(s)**.

* Bit Length - Key Type 521 - EC 4096 - RSA 2048 - DSA ⓘ

* ECDSA curve secp521r1 / P-521 ⓘ

* Hash Function SHA512 SHA384 ⓘ

The following table provides the field description in the **CA Details** section:

Name	Description
*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 drop-down.  Note: 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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, and Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.  Note: The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.

Name	Description
	 Note: The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, and Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.	

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Common Name



Subject Alternative Name



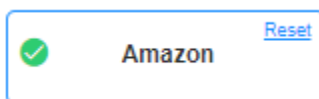
Save CA Details

The following table provides the field description **in the Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, Regenerate.

Name	Description
	 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. 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 the details are successfully stored.



15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.	+ Create	Delete
Q Search...		1 to 3 of 3		
Policy Name	Description	Group	Type	
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive	
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict	
☐ Presales		Demo-AppViewX	Strict	

Configuring Policy for Amazon Private CA

- 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.

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 **GROUPS & POLICIES**.

5. Click **CA Policy**.

Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Amazon Private CA details, click **Amazon Private CA** in the **Certificate Authority** pane on the left side of the page.

CA Policy : Create

CA details

Define Certificate standards per Certificate Authority. Users can select the CAs configured with the policy while performing certificate operations.

Certificate Authority

☐ General
 ☐ Amazon
 ☒ Amazon Private CA
 ☐ AppViewX
 ☐ Comodo Certificate Manager
 ☐ DigiCert
 ☐ Ejbca
 ☐ Entrust
 ☐ GlobalSign
 ☐ GoDaddy

* CA Accounts

Select...

* Issuer Region

Select...

* Issuer Name

Select...

* Validity

Type validity and press enter

Days

Type validity and press enter

Months

Type validity and press enter

Years

* Bit Length - Key Type

Select...

* Hash Function

Select...

* Signature Algorithm

Select...

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Create Policy Cancel

The following table provides the field description in the **CA Details** section:

Field	Description
*CA Account	Select the certificate authority account.
*Issuer Region	Select the issuer region from the dropdown list.
*Issuer Name	Select the issuer name from the dropdown list.
*Validity	Enter the 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.

Field	Description							
*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 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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate. The Amazon Private CA supports below Bit type and Length. <table> <tr> <th>Type</th><th>Length</th></tr> <tr> <td rowspan="2">RSA</td><td>2048</td></tr> <tr> <td>4096</td></tr> <tr> <td>EC</td><td>prime256v1 sec384r1</td></tr> </table>	Type	Length	RSA	2048	4096	EC	prime256v1 sec384r1
Type	Length							
RSA	2048							
	4096							
EC	prime256v1 sec384r1							
*Hash Function	Supported Hash Function(s) are listed. You can select one or more than one Hash Function from the dropdown list. The supported hash functions are: • SHA256 • SHA384 • SHA512.							
*Signature Algorithm	Select the SignAlgorithm from the dropdown list. The available options are: • SHA256WITHECDSA • SHA384WITHECDSA • SHA512WITHECDSA • SHA256WITHRSA							

Field	Description
	• SHA384WITHRSA • SHA512WITHRSA.  Note: The Issuer will print the issuer algorithm that the users selected in the Signature Algorithm field.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Certificate parameters** section, enter/select the following details.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name ⓘ

Organization ⓘ

Organization Unit ⓘ

Locality ⓘ

State ⓘ

Country code ⓘ ✕

Email ⓘ ✕

Subject Alternative Name

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description **in the certificate parameters** section:

Field	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, 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.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 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.

Field	Description
	The discovered certificate's Country code will be compared against the country code provided in the policy to identify if they are complaints. 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 complaints. 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

- 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 the details are successfully stored.
- Click the **Create Policy** button to create a new policy.

The policy is created and a confirmation message displays.

CA Policy		Policy created.		+ Create	Delete
Q Search...		1 to 3 of 3		<	>
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict		
☐ Presales		Demo-AppViewX	Strict		

Configuring Policy for Digicert CA

To configure a Digicert CA policy,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

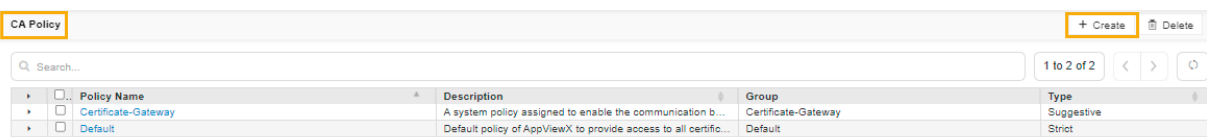
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **GROUPS & POLICIES**.

5. Click **CA Policy**.



Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Digicert details, click Digicert in the **Certificate Authority** pane on the left side of the page.

CA details

Define Certificate standards per Certificate Authority. Users can select the CAs configured with the policy while performing certificate operations.

CA Accounts	Division	Certificate Type	view details	Edit	Remove
Digicert	AppViewX Inc.	SSL Plus	view	edit	remove

The following table provides the field description in the **CA Details** section:

Field	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	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 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.

Field	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Vendor Specific Details section**, select/enter the details as listed in the table

Field	Description
* Server Type	Select the server type from the dropdown list.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use the **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

CA Accounts	Division	Certificate Type	validity	Edit	Remove
Digicert	private-only	Private SSL Plus	view		
Digicert	public-only	SSL Plus	view		
Digicert	AppViewX Inc.	Private SSL Multi Domain	view		

12. In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type

× 521 - EC
 × 4096 - RSA
 × 2048 - DSA
 Clear
ⓘ

* ECDSA curve

× secp521r1 / P-521
 Clear
ⓘ

* Hash Function

× SHA512
 × SHA384
 Clear
ⓘ

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description under the **Certificate parameters** section:

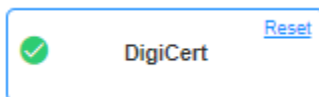
Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, and Regenerate. Note: Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Organization	You can provide the organization's name.

Name	Description
	The discovered certificate's SubjectOrganization 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. 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 complaints. Mail address is

Name	Description
	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 (@)

 **Note:** The asterisk (*) symbol indicates a mandatory field.

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Digicert** option to indicate the details are successfully stored.



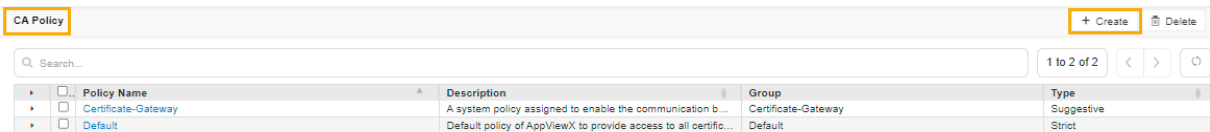
15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.		+ Create	Delete
Search...		1 to 8 of 8		<	>
Policy Name	Description	Group	Type		
☐ Banking-app		Banking-app	Suggestive		
☐ Certificate-Gateway	A system policy assigned to enable the communi...	Certificate-Gateway	Strict		
☐ Default	Default policy of AppViewX to provide access to ...	SopraGr, Networking, SopraGrp, CryptoOps, En...	Suggestive		
☐ Demo-Policy		DEV	Strict		
☐ MSG-CA-Policy		MSG	Suggestive		
☐ TestPolicy		test	Suggestive		
☐ aut-mobile		Auto-mobile	Suggestive		
☐ healthcare-app		health-care	Suggestive		

Configuring Policy for EJBCA CA

To configure an EJBCA CA policy,

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 **GROUPS & POLICIES**.



5. Click **CA Policy**.
The CA Policy home page appears.
6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure the policy with EJBCA details, click **Ejbca** in the **Certificate Authority** pane on the left side of the page.

The screenshot shows the 'Certificate Authority' section on the left with a list of providers: General, Amazon, AppViewX, Comodo Certificate Manager, DigiCert, Ejbca (highlighted), and Entrust. The 'Vendor Specific Details' section on the right includes a dropdown for 'CA Accounts' set to 'EJBCA'. Below this are fields for 'End entity user name' (AppViewXUser), 'End Entity Profile Name' (APPVIEWX PROFILE), 'Issuer Common Name' (EJBCA INTERMEDIATE CA), and 'Certificate Profile Name' (CLIENT PROFILE). An 'Add' button is present. At the bottom, there's a table for 'CA Accounts' with columns 'View', 'Edit', and 'Remove'. The 'View' column shows 'view' for 'EJBCA'. Below the table are buttons for 'Bit Length - Key Type' with options: 1024 - RSA, 2048 - RSA, 3072 - RSA, and a 'Clear' button. A thumbs up icon is in the bottom right corner.

The following table provides the field description **in the CA Details** section.

Field	Description
*CA Accounts	The EJBCA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

Field	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.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use the **Remove** option to delete the configuration.

CA Accounts	Remove
EJBCA	
MSG-EJBCA-SAAS-CA	

12. In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type 521 - EC 4096 - RSA 2048 - DSA ⓘ

* ECDSA curve secp521r1 / P-521 ⓘ

* Hash Function SHA512 SHA384 ⓘ

The following table provides the description of other fields in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate.

Name	Description	Purpose
		We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.


Note: The asterisk (*) symbol indicates a mandatory field.

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name ⓘ

Organization ⓘ

Organization Unit ⓘ

Locality ⓘ

State ⓘ

Country code ⓘ ✕

Email ⓘ ✕

Subject Alternative Name

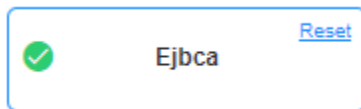
CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description under the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.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.

Name	Description
	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. 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 complaints. Mail address is enforced while performing any certificate request operations such as New, Renew, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark displays in the **Certificate Authority** pane against the **EJBCA** option to indicate the details are successfully stored.



15. Click **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.		+ Create	Delete
Search...		1 to 3 of 3		<	>
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict		
☐ Presales		Demo-AppViewX	Strict		

Configuring Policy for Entrust CA

To configure an Entrust CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

CA Policy

+ Create

Delete

Search...

1 to 2 of 2

<>↺↻

Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Entrust details, click Entrust in the **Certificate Authority** pane on the left side of the page.

Certificate Authority

* CAAccounts: Select... ⓘ

* Certificate Type: Select... ⓘ

* Validity: Type validity and press enter Days ⓘ

Type validity and press enter Months ⓘ

Type validity and press enter Years ⓘ

Vendor Specific Details

Additional Emails:

Add

CA Accounts	Certificate Type	validity	Edit	Remove
EntrustCA	EV	view		

The following table provides the field description in the **CA Details** section:

Field	Description
*CA Account	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 Type from the list to create the policy.
*Validity	Enter the 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.
Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Vendor Specific Details section**, select/enter the details as listed in the table:

Field	Description
Additional Emails	Enter the valid email address in the field.

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use the **Edit** option in the table to modify the configuration and **the Remove** option to delete the configuration.

CA Accounts	Certificate Type	validity	Edit	Remove
entrust	Standard	view		
	UC MultiDomain			
	Wildcard			
	Advantage			
	EV			

12. In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type ⓘ

* ECDSA curve ⓘ

* Hash Function ⓘ

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify

Name	Description	Purpose
	can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description under the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Organization	You can provide the organization's name.

Name	Description
	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. 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.

Name	Description
	The discovered certificate's mail address will be compared against the email address provided in the policy to identify if they are complaints. 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **Entrust** option to indicate the details are successfully stored.
15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy					Policy created.		+ Create	Delete
Q Search...					1 to 3 of 3		<	>
Policy Name	Description	Group	Type					
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive					
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict					
☐ Presales		Demo-AppViewX	Strict					

Configuring Policy for Entrust MPKI CA

To configure an Entrust MPKI CA policy,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

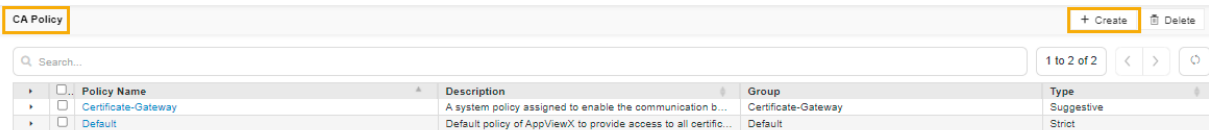
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **GROUPS & POLICIES**.

5. Click **CA Policy**.



Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifo...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Entrust MPKI details, click Entrust MPKI in the **Certificate Authority** pane on the left side of the page.

The following table provides the field description in the **CA Details** section:

Field	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. • The selected CA account will be listed in the CA Accounts table.
*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 drop-down. 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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down. The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function is enforced while performing any certificate request operations such as New, Renew, Regenerate.

Field	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is compliant. Additionally, below will also be enforced on a certificate request.

Common Name	AppViewX	
Organization	Example: AppViewX	
Organization Unit	Example: Your org unit	
Locality	Example: Seattle	
State	Example: Washington	
Country code	Example: Search your country and select country code.	
Email	Example: admin@email.com , user123@email.com .	
Subject Alternative Name		

[Save CA Details](#)

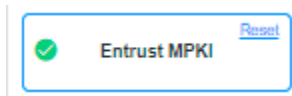
The following table provides the field description under the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com

Name	Description
	It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.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

Name	Description
	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. 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 complaints. 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

- Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **Entrust MPKI** option to indicate the details are successfully stored.



Note: The Pop-up message is displayed as **Entrust MPKI - CA details added.**

11. Refer **Configuring Policy Details** section in admin guide to configure,
 - **Group Selection** section
 - **Compliance Check** section
12. Click the **Create Policy** button to create a new policy.
13. The policy is created and a confirmation message is displayed.

CA Policy

Policy created.

+ Create

Delete

Search...

1 to 8 of 8

<

>

↺

Policy Name	Description	Group	Type
☐ Banking-app		Banking-app	Suggestive
☐ Certificate-Gateway	A system policy assigned to enable the communi...	Certificate-Gateway	Strict
☐ Default	Default policy of AppViewX to provide access to ...	SopraGr, Networking, SopraGrp, CryptoOps, En...	Suggestive
☐ Demo-Policy		DEV	Strict
☐ MSG-CA-Policy		MSG	Suggestive
☐ TestPolicy		test	Suggestive
☐ aut-mobile		Auto-mobile	Suggestive
☐ healthcare-app		health-care	Suggestive

Configuring Policy for GlobalSign CA

To configure a GlobalSign CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

CA Policy

+ Create

Delete

Search...

1 to 2 of 2

<

>

↺

Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifo...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with GlobalSign details, click **GlobalSign** in the **Certificate Authority** pane on the left side of the page.

The screenshot shows the 'Certificate Authority' section on the left with a list of providers: AppViewX, Comodo Certificate Manager, DigiCert, Ejbca, Entrust, GlobalSign (highlighted), and GlobalSignMSSL. Each has a 'Reset' link. The main form area has the following fields:

- * CA Accounts:** GlobalSign
- * Certificate Type:** Extended SSL
- * Validity:** 365 Days

The 'Vendor Specific Details' section contains:

- * Incorporating Agency Reg. No:** AGENCY12456
- * Designation:** PM
- * Business Category:** Private organization

An 'Add' button is located below these fields. At the bottom, a table displays the configured CA details:

CA Accounts	Certificate Type	validity	Edit	Remove
GlobalSign	Organization SSL	view		

9. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

Field	Description
*Incorporating Agency Reg. No	Enter the agency registration number.
*Designation	Enter the designation.
*Business Category	Select the business category from the dropdown list.

Note: The asterisk (*) symbol indicates a mandatory field.

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

12. In the **CA details** section, select **Bit Length -Key Type, ECDSA curve, and Hash Function**.

* Bit Length - Key Type × 521 - EC × 4096 - RSA × 2048 - DSA Clear ?

* ECDSA curve × secp521r1 / P-521 Clear ?

* Hash Function × SHA512 × SHA384 Clear ?

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while

Name	Description	Purpose
		performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name

Test.Userguide.com

Organization

AppViewX_Tech Doc Team

Organization Unit

AppViewX_Tech Doc Team

Locality

Coimbatore

State

Tamil Nadu

Country code

India

Email

<username>@<domainname>.com

Subject Alternative Name

Save CA Details

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

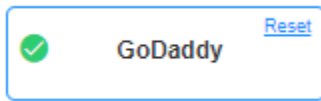
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com. It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, and Regenerate.

Name	Description
	 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.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, 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, 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, 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.

Name	Description
	The state is enforced while performing any certificate request operations such as New, Renew, 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. Country code is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Email	You can provide an organization unit mail address. The discovered certificate's mail address will be compared against the mail 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, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the GlobalSign option to indicate the details are successfully stored.



15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy

Policy created.

+ Create

Delete

Search...

1 to 3 of 3

<

>

↺

Policy Name	Description	Group	Type
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict
☐ Presales		Demo-AppViewX	Strict

Configuring Policy for GoDaddy CA

To configure a GoDaddy CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with GoDaddy details, click GoDaddy in the **Certificate Authority** pane on the left side of the page.

Certificate Authority

- Ejbca [Reset](#)
- Entrust [Reset](#)
- GlobalSign [Reset](#)
- GlobalSignMSSL [Reset](#)
- GoDaddy** [Reset](#)
- Google [Reset](#)
- InCommon [Reset](#)

* CA Accounts: Godaddy ⓘ

* Certificate Type: Premium SSL - SAN (UCC_EV_SSL) ⓘ

* Validity: 365 x Days ⓘ

Vendor Specific Details

* Slot Size: 5

[Add](#)

CA Accounts	Certificate Type	validity	Edit	Remove
Godaddy	Premium SSL - SAN (UCC_EV_SSL)	view	Edit	Remove
Godaddy	Standard UCC SSL - SAN (UCC_DV_SSL)	view	Edit	Remove
Godaddy	Standard Wildcard SSL (D V WILDCARD SSL)	view	Edit	Remove

The following table provides the field description in the **CA Details** section:

Field	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.
* 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	Enter the 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.
Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Vendor Specific Details** section, select/enter the details as listed in the table:

Field	Description
*Slot Size	Select the size of the slot from the dropdown list.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

CA Accounts	Certificate Type	validity	Edit	Remove
Godaddy	Standard SSL (DV_SSL)	view		
	Standard Wildcard SSL (DV_WILDCARD_SSL)			
	Standard UCC SSL - SAN (UCC_DV_SSL)			

12. Select **Bit Length -Key Type, ECDSA curve, Hash Function** in the **CA details** section.

* Bit Length - Key Type ⓘ

* ECDSA curve ⓘ

* Hash Function ⓘ

The following table provides the description of other fields under the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request

Name	Description	Purpose
		operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

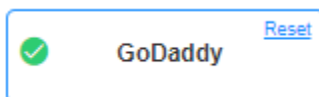
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Organization	You can provide the organization's name.

Name	Description
	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, 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. 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.

Name	Description
	The discovered certificate's mail address will be compared against the email address provided in the policy to identify if they are complaints. 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 (@)

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **GoDaddy** option to indicate the details are successfully stored.



15. Click **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy					Policy created.		+ Create	Delete
Q Search...					1 to 3 of 3		<	>
Policy Name	Description	Group	Type					
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive					
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict					
☐ Presales		Demo-AppViewX	Strict					

Configuring Policy for Google CA

To configure a Google CA policy,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

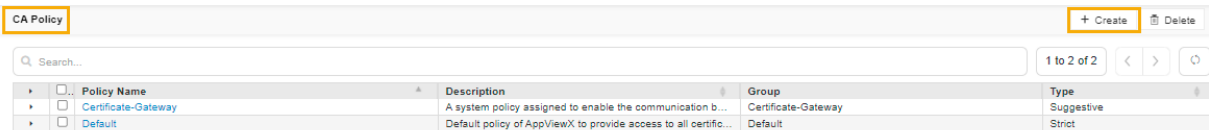
The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **GROUPS & POLICIES**.

5. Click **CA Policy**.



Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifo...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Google details, click *Google* in the **Certificate Authority** pane on the left side of the page.

* CAAccounts ⓘ

* Issuer Location ⓘ

* Issuer Name ⓘ

* Validity x Days ⓘ

x Months ⓘ

x Years ⓘ

* Bit Length - Key Type Clear ⓘ

* ECDSA curve Clear ⓘ

* Hash Function Clear ⓘ

The following table provides the field description **in the CA Details** section:

Field	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 Location corresponding to the selected CA account is listed. Select an Issuer Location from the list to create the policy.
*Issuer Name	The Issuer Name corresponding to the selected issuer location is listed. Select an Issuer Name from the list to create the policy.
*Validity	Provide the value and press Enter . Enforce Validity period for selected Issuer Name. The validity for Google CA can be represented in Day(s)/ Month(s)/ Year(s). One (or) more than one Validity period can be added.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the CA details section, select the **Bit Length -Key Type(s)**, **ECDSA curve(s)**, and **Hash Function(s)**.

The screenshot shows the 'CA Details' section with three selection fields:

- * Bit Length - Key Type:** A multi-select dropdown containing '521 - EC', '4096 - RSA', and '2048 - DSA'. There is a 'Clear' button and an information icon.
- * ECDSA curve:** A single-select dropdown containing 'secp521r1 / P-521'. There is a 'Clear' button and an information icon.
- * Hash Function:** A multi-select dropdown containing 'SHA512' and 'SHA384'. There is a 'Clear' button and an information icon.

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.

Name	Description	Purpose



Note: The asterisk (*) symbol indicates a mandatory field.

10. You can fill the **Certificate parameters** section based on your organization's policies and standards.

For the Policy Enforcement Type = **Strict**

Certificate parameters

Compare the discovered certificate with the below to identify if it is compliant. Additionally, below will also be enforced on a certificate request.

* Host Name

?

* Allowed Domain Names

x axn.com

x wes.com

x

?

Common Name

?

Organization

?

Organization Unit

?

Locality

?

State

?

Country code

?

Email

?

Subject Alternative Name

?

Save CA Details

CA Accounts	Issuer Location	View	Edit	Remove
No records added...				

For the Policy Enforcement Type = **Suggestive**

Certificate parameters

Compare the discovered certificate with the below to identify if it is compliant. Additionally, below will also be enforced on a certificate request.

Host Name

Allowed Domain Names

Blocked Domain Names

Common Name

Organization

Organization Unit

Locality

State

Country code

Email

Subject Alternative Name

Save CA Details

CA Accounts	Issuer Location	View	Edit	Remove
No records added...				

The following table provides the field description in the **Certificate parameters** section:

Name	Description
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	This is a non-editable field. It has comma-separated values of possible domain names which are allowed. It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)

Name	Description
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, 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, 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, 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, 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. Country code is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Email	You can provide an organization unit mail address.

Name	Description
	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, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

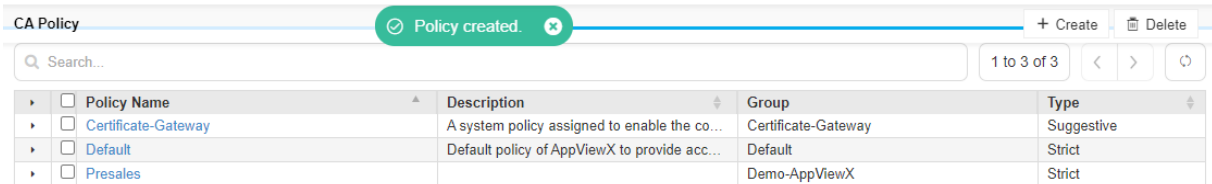
11. You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

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		

12. A green tick mark will be displayed in the **Certificate Authority** pane against the **Google** option to indicate the details are successfully stored.



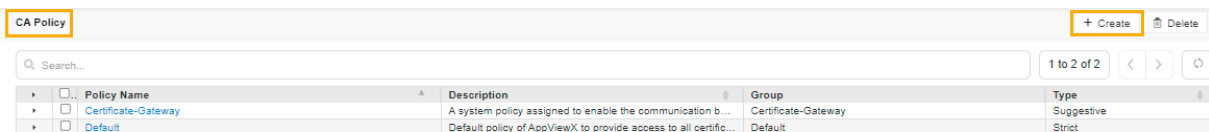
13. Click the **Create Policy** button to create a new policy.
14. The policy is created and a confirmation message displays.



Configuring Policy for Let's Encrypt CA

To configure the Let's Encrypt CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.



The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with LetsEncrypt details, click **LetsEncrypt** in the **Certificate Authority** pane on the left side of the page.

The screenshot shows the 'Certificate Authority' section with a list of providers: Entrust, GlobalSign, GlobalSignMSSL, GoDaddy, Google, and LetsEncrypt. The 'LetsEncrypt' option is selected and highlighted with an orange box. To the right, the 'Vendor Specific Details' section is visible, showing a dropdown for 'CA Accounts' set to 'LetsEncrypt', 'Certificate Type' set to 'EliteSSL Certificate (customized for United Parcel ...)', and 'Validity' set to '365' days. Below this, the 'Challenge Type' is set to 'HTTP'. An 'Add' button is present. At the bottom, a table displays the configured CA details.

CA Accounts	Certificate Type	validity	Edit	Remove
LetsEncrypt	EliteSSL Certificate (customized for United Parcel Service)	view		
LetsEncrypt	Comodo PlatinumSSL Will	view		

9. In the **Vendor Specific Details** section, select the challenge type from the dropdown list.
10. Click the **Add** button.
The CA details are saved to the table and the confirmation message displays.
11. You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
12. Select **Bit Length -Key Type, ECDSA curve, Hash Function** in the **CA details** section.

The 'CA Details' section contains three configuration fields:

- * Bit Length - Key Type:** A multi-select dropdown with options '521 - EC', '4096 - RSA', and '2048 - DSA'. A 'Clear' button and an information icon are also present.
- * ECDSA curve:** A dropdown with the option 'secp521r1 / P-521'. A 'Clear' button and an information icon are also present.
- * Hash Function:** A multi-select dropdown with options 'SHA512' and 'SHA384'. A 'Clear' button and an information icon are also present.

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while

Name	Description	Purpose
		performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

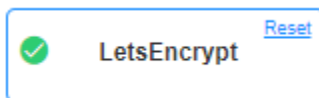
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.).
Organization	You can provide the organization's name.

Name	Description
	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, 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, 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, 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, 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. Country code is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Email	You can provide an organization unit mail address.

Name	Description
	The discovered certificate's mail address will be compared against the email address provided in the policy to identify if they are complaints. Mail address is enforced while performing any certificate request operations such as New, Renew, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **LetsEncrypt** option to indicate the details are successfully stored.

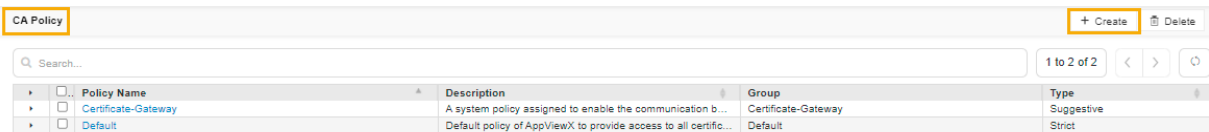


15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.	+ Create	Delete
Search...		1 to 3 of 3	<	>
Policy Name	Description	Group	Type	
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive	
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict	
☐ Presales		Demo-AppViewX	Strict	

Configuring Policy for Microsoft Enterprise CA

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.



Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Microsoft Enterprise details, click **Microsoft Enterprise** in the **Certificate Authority** pane on the left side of the screen.

The following table provides the field description under **CA Details** section:

Name	Description
*CA Accounts	The Microsoft Enterprise CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
*MS Template List	The MS template(s) configured for the selected CA account are listed. Select MS template(s) from the list to associate with the policy.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. Select **CA accounts** and **MS Template List** under **CA details** section.

* CA Accounts ⓘ

* MS Template List Clear ⓘ

Add

10. Click **Add** button. The CA details are saved to the table and the confirmation message displays.

11. You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

CA Accounts	MS Template List	Edit	Remove
avxdevlab-AVXENTCA-CA	Administrator EFS EFSRecovery		

12. In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type × 521 - EC × 4096 - RSA × 2048 - DSA Clear ⓘ

* ECDSA curve × secp521r1 / P-521 Clear ⓘ

* Hash Function × SHA512 × SHA384 Clear ⓘ

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while

Name	Description	Purpose
		performing any certificate request operations such as New, Renew, Regenerate.


Note: The asterisk (*) symbol indicates a mandatory field.

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name ⓘ

Organization ⓘ

Organization Unit ⓘ

Locality ⓘ

State ⓘ

Country code ⓘ ✕

Email ⓘ ✕

Subject Alternative Name

[Save CA Details](#)

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

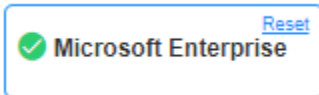
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, and Regenerate.

Name	Description
	 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.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, 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, 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, Regenerate.

Name	Description
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. Country code is enforced while performing any certificate request operations such as New, Renew, 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 complaints. Mail address is enforced while performing any certificate request operations such as New, Renew, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

- Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **the Microsoft Enterprise** option to indicate the details are successfully stored.



15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.	+ Create	Delete
Search...		1 to 3 of 3		
Policy Name	Description	Group	Type	
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive	
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict	
☐ Presales		Demo-AppViewX	Strict	

Configuring Policy for Microsoft Standalone CA

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

CA Policy		+ Create	Delete
Search...		1 to 2 of 2	
Policy Name	Description	Group	Type
☐ Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
☐ Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Microsoft Standalone details, click **Microsoft Standalone** in the **Certificate Authority** pane on the left side of the screen.

The following table provides the field description in the **CA Details** section:

Name	Description
*CA Accounts	The Microsoft Standalone accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.


Note: The asterisk (*) symbol indicates a mandatory field.

9. Select **CA accounts** in the **CA details** section.
10. Click **Add** button. The CA account is saved to the table and confirmation message displays.
11. You can use the **Remove** option to delete the configuration.
12. In the **CA details** section, select the **Bit Length -Key Type, ECDSA curve, and Hash Function**.

*** Bit Length - Key Type**

× 521 - EC
 × 4096 - RSA
 × 2048 - DSA
 Clear
ⓘ

*** ECDSA curve**

× secp521r1 / P-521
 Clear
ⓘ

*** Hash Function**

× SHA512
 × SHA384
 Clear
ⓘ

The following table provides the description of other fields in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and

Name	Description	Purpose
		Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.


Note: The asterisk (*) symbol indicates a mandatory field.

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name ⓘ

Organization ⓘ

Organization Unit ⓘ

Locality ⓘ

State ⓘ

Country code ⓘ ✕

Email ⓘ ✕

Subject Alternative Name

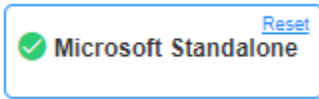
CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description under **Certificate parameters** section:

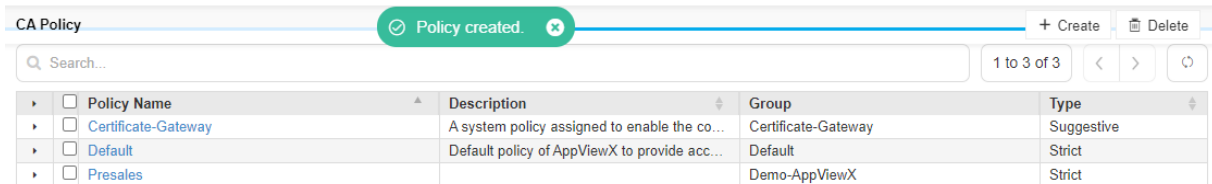
Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, and Regenerate.  Note: Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain.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, 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, 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, Regenerate.
State	You can provide state.

Name	Description
	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, 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. Country code is enforced while performing any certificate request operations such as New, Renew, 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, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **Microsoft Standalone** option to indicate the details are successfully stored.

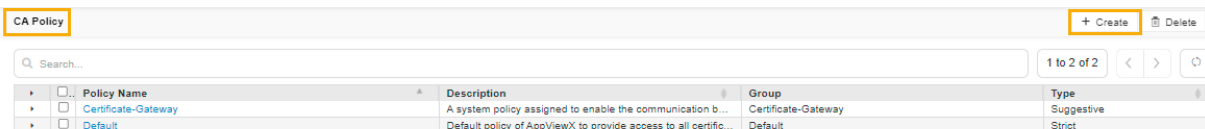


15. Click the **+ Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.



Configuring Policy for OpenTrust CA

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.



The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with OpenTrust details, click OpenTrust in the **Certificate Authority** pane on the left side of the page.

The screenshot shows the 'Certificate Authority' section on the left with a list of providers: Google, InCommon, LetsEncrypt, Microsoft Enterprise, Microsoft Standalone, **OpenTrust** (highlighted with a yellow box), Symantec, and Thawte. Each provider has a 'Reset' link. The main form area contains the following fields:

- * CA Accounts:** A dropdown menu with 'OpentrustCA' selected.
- * Certificate Management Profile:** A dropdown menu with 'ocsp' selected.
- * Zone:** A dropdown menu with 'AppViewX-Zone1' selected.
- Profile Parameters:** A section containing three text input fields:
 - * Common Name:** 'appviewx.com'
 - Organizational Unit:** 'AppViewX Org'
 - Organization:** 'AppViewX'

Below the Profile Parameters section is an 'Add' button. At the bottom, there is a table with the following data:

CA Accounts	View	Edit	Remove
OpentrustCA	view		

A thumbs-up icon is visible in the bottom right corner of the interface.

The following table provides the field description **in the CA Details** section.

Field	Description
*CA Account	The OpenTrust CA accounts configured in 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.
Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Profile Parameters** section, select/enter the details as listed in the table.

Field	Description
*Common Name	Enter the common name for the policy.
Organizational Unit	Enter the organizational unit.
Organization	Enter the name of the organization.

Field	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. Click the **Add** button.

The CA details are saved to the table and the confirmation message displays.

11. You can use the **Remove** option to delete the configuration.

12. In the **CA details** section, select **Bit Length -Key Type, ECDSA curve, and Hash Function**.

* Bit Length - Key Type: 521 - EC 4096 - RSA 2048 - DSA ⓘ

* ECDSA curve: secp521r1 / P-521 ⓘ

* Hash Function: SHA512 SHA384 ⓘ

The following table provides the description of other fields in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected

Name	Description	Purpose
	curve from the drop-down. for a certificate.	ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

The following table provides the field description under the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, Regenerate.

Name	Description
	 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.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, 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, 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, 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 complaint.

Name	Description
	The state is enforced while performing any certificate request operations such as New, Renew, 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. Country code is enforced while performing any certificate request operations such as New, Renew, 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, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark displays in the **Certificate Authority** pane against the **OpenTrust** option to indicate the details are successfully stored.
15. Click **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.

CA Policy		Policy created.		+ Create	Delete
Search...		1 to 3 of 3		<	>
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict		
☐ Presales		Demo-AppViewX	Strict		

Configuring Policy for Sectigo CA

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

CA Policy				+ Create	Delete
Search...		1 to 2 of 2		<	>
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict		

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Sectigo details, click **Comodo Certificate Manager** in the **Certificate Authority** pane on the left side of the screen.

* CA Accounts ⓘ

* Certificate Type ⓘ

* Validity Days ⓘ

Add

The following table provides the field description in the **CA Details** section:

Name	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 from the list to create the policy.
*Validity	Provide the value and press Enter . Enforce Validity period for selected Certificate Type(s). The validity for Sectigo CA can be represented in Day(s). One (or) more than one Validity period can be added.
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. Select **CA accounts** and **Certificate Type** in the **CA details** section and provide the **Validity** period.
10. Click **Add** button. The CA details are saved to the table and the confirmation message displays.
11. You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

CA Settings	Certificate Type	Edit	Remove
Sectigo	Comodo PlatinumSSL Wildcard Certificate (customized for United Parcel Service)		
	Comodo Unified Communication Certificate (customized for United Parcel Service)		
	EliteSSL Certificate (customized for United Parcel Service)		

12. In the **CA details** section, select the **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type × 521 - EC × 4096 - RSA × 2048 - DSA Clear ?

* ECDSA curve × secp521r1 / P-521 Clear ?

* Hash Function × SHA512 × SHA384 Clear ?

The following table provides the description of other fields in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down. for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend to use P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced

Name	Description	Purpose
		while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

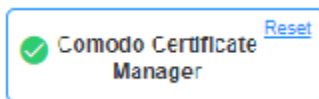
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.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

Name	Description
	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. 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 complaints. 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.

Name	Description
	 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

14. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Comodo Certificate Manager** option to indicate the details are successfully stored.



15. Click **Create Policy** button to create a new policy.
 16. The policy is created and a confirmation message displays.

CA Policy		Policy created.	+ Create	Delete
Search...		1 to 3 of 3	<	>
Policy Name	Description	Group	Type	
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive	
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict	
☐ Presales		Demo-AppViewX	Strict	

Configuring Policy for Symantec CA

To configure the Symantec CA policy,

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.

CA Policy				
Search...				+ Create Delete
1 to 2 of 2				
Policy Name	Description	Group	Type	
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive	
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict	

The CA Policy home page appears.

- Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description 1996 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval? ☒

When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key? ☒

When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user ☒

Enable certificate push-bind access for read-only user ☒

Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

[Create Policy](#) [Cancel](#)

The **Create** policy page appears.

- Refer [Configuring Policy Details](#) section in admin guide to configure,

- **Policy Details**
- **Group Selection**
- **Compliance Check**

8. To configure a policy with Symantec details, click **Symantec** in the **Certificate Authority** pane on the left side of the page.

Certificate Authority

- Let's Encrypt [Reset](#)
- Microsoft Enterprise [Reset](#)
- Microsoft Standalone [Reset](#)
- OpenTrust
- ProgrammableCA
- Symantec** [Reset](#)
- Thawte
- Trustwave [Reset](#)

* CA Accounts: SymantecCA ⓘ

* Certificate Type: Standard ⓘ

* Validity: 365 Days ⓘ, 12 Months ⓘ, 1 Year ⓘ

Vendor Specific Details

* Server Type: Microsoft

[Add](#)

CA Accounts	Certificate Type	validity	Edit	Remove
Symantec	Standard	view	Edit	Remove
Symantec	EV Premium	view	Edit	Remove

The following table provides the field description in the **CA Details** section.

Field	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 from the list to create the policy.
*Validity	Enter the 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.

Field	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

- In the **Vendor Specific Details** section, select the server type from the dropdown list.
- Click the **Add** button.
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 **Remove** option to delete the configuration.
- In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type: Clear 

* ECDSA curve: Clear 

* Hash Function: Clear 

The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing

Name	Description	Purpose
		certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

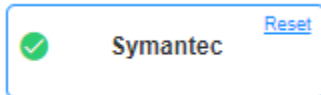
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)

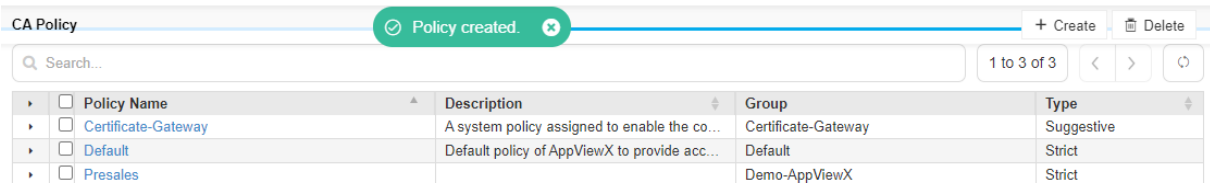
Name	Description
Organization	You can provide the organization's name. The discovered certificate's Subject Organization will be compared against the organization provided in the policy to identify if they are complaints. The organization is enforced while performing any certificate request operations such as New, Renew, 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, 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, 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.

Name	Description
	The discovered certificate's Country code will be compared against the country code provided in the policy to identify if they are complaints. Country code is enforced while performing any certificate request operations such as New, Renew, 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, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

- Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **the Symantec** option to indicate the details are successfully stored.

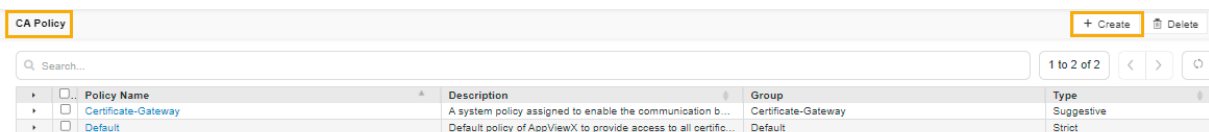


15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.



Configuring Policy for Trustwave CA

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 **GROUPS & POLICIES**.
5. Click **CA Policy**.



The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description

1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Trustwave details, click **Trustwave** in the **Certificate Authority** pane on the left side of the screen.
9. Select **CA accounts and Certificate Type** under the **CA details** section and provide the **Validity** period.

* CAAccounts ⓘ

* Certificate Type ⓘ

* Validity Days ⓘ

Months ⓘ

Years ⓘ

Add

The following table provides the field description under **CA Details** section:

Name	Description
*CA Accounts	The Trustwave 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 from the list to create the policy.
*Validity	Provide the value and press Enter . Enforce Validity period for selected Certificate Type(s). The validity for Trustwave CA can be represented in Day(s)/ Month(s)/ Year(s). One (or) more than one Validity period can be added.


Note: The asterisk (*) symbol indicates a mandatory field.

- Click the **Add** button. 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 **Remove** option to delete the configuration.

CA Settings	Certificate Type	Edit	Remove
Trustwave CA_Server	SecureTrust Organization Validation		
	SecureTrust OV Wildcard		

- In the **CA details** section, select **Bit Length -Key Type, ECDSA curve, and Hash Function**.

* Bit Length - Key Type 521 - EC 4096 - RSA 2048 - DSA

* ECDSA curve secp521r1 / P-521

* Hash Function SHA512 SHA384

The following table provides the field description under **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any

Name	Description	Purpose
		certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name ⓘ

Organization ⓘ

Organization Unit ⓘ

Locality ⓘ

State ⓘ

Country code ⓘ ✕

Email ⓘ ✕

Subject Alternative Name

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

The following table provides the field description in the **Certificate parameters** section:

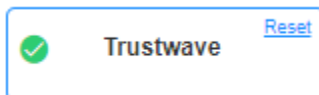
Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing

Name	Description
	any 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.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, 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, 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, Regenerate.
State	You can provide state.

Name	Description
	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, 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. Country code is enforced while performing any certificate request operations such as New, Renew, 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 complaints. Mail address is enforced while performing any certificate request operations such as New, Renew, 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 (@)

Name	Description
 Note: The asterisk (*) symbol indicates a mandatory field.	

- Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Trustwave** option to indicate the details are successfully stored.



- Click **Create Policy** button to create a new policy.
- The policy is created and a confirmation message displays.

CA Policy		Policy created.	+ Create	Delete
Q Search...		1 to 3 of 3	<	>
Policy Name	Description	Group	Type	
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive	
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict	
☐ Presales		Demo-AppViewX	Strict	

Configuring Policy for GlobalSign MSSL CA

- Log in to AppViewX application with valid credentials.
- Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
- Click **CERT+** on the left navigation pane.
A new left pane with certificate actions appears.
- Click **CA Policy** under **Groups & Policies**.

CA Policy

+ Create

Delete

Search...

1 to 2 of 2

<>↺

Policy Name	Description	Group	Type
Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive
Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict

- The CA Policy inventory appears.
- CERT+** is packaged with default policies they are **Default** and **Certificate-Gateway**.
- Click **+ Create** button to configure GlobalSign MSSL based policy.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description
1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval?



When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key?



When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user



Enable certificate push-bind access for read-only user



Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

Create Policy

Cancel

8. Refer [Configuring Policy Details](#) section in the admin guide to configure,
 - **Policy Details** section
 - **Group Selection** section
 - **Compliance Check** section
9. To configure policy with GlobalSign MSSL details, click **GlobalSign MSSL** in the **Certificate Authority** pane on the left side of the screen.

The following table provides the field description under **CA Details** section:

Name	Type	Mandatory	Description	Validation
CA Accounts	Select	Yes	The GlobalSign MSSL CA accounts configured on the CA settings screen are listed. Select a CA account from the list to create the policy.	NA
Product Type	Select	Yes	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.	NA
Signature Algorithm	Select	Yes	Select the Signature Algorithm from the drop-down list.	NA
MSSL Profile Allowed Domain Name	Select	Yes	Select the MSSL Profile Allowed Domain Name from the drop-down list.	NA
Validity	Text	Yes	Provide the value and press Enter . Enforce Certificate Validity period for selected Certificate Type. The certificate validity of GlobalSign MSSL CA is represented in Day(s) and Year(s). One (or) more than one period can be added.	NA
 Note: The asterisk (*) symbol indicates a mandatory field.				

10. Select **CA accounts**, **Product Type**, **Signature Algorithm**, **MSSL PProfile Allowed Domain Name**, and **Validity** under **CA details** section and provide **Validity** period.
11. Click **Add** button. The CA details are saved to the table and the confirmation message is displayed.
12. You can use **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

The following table provides the field description under the **CA Details** section:

Name	Type	Mandatory	Description	Purpose
Bit Length - Key Type	Multi select	Yes	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 drop-down.	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, Regenerate.
ECDSA Curve	Multi select	Yes	The ECDSA curve's values get auto-populated once the details are configured/selected and the Add button is clicked.	A discovered certificate's key elliptic curves will be compared against the information to identify if there is a complaint. Additionally, the below details will also be enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using the P256/ P384/ P521 ECDSA curve while enrolling for a certificate.
 Note: The asterisk (*) symbol indicates a mandatory field.				

13. Select **Bit Length -Key Type, ECDSA curve, Hash Function** under **CA details** section.

The following table provides the field description under the **Certificate parameters** section:

Name	Type	Mandatory	Description	Validation
Host Name	Text	No	You can provide the hostname.	The hostname should not start and end with a dot/ fullstop(.)
Common Name	Text	No	You can provide the common name. For example, *.domain.com	Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow

Name	Type	Mandatory	Description	Validation
			It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any certificate request operations such as New, Renew, Regenerate.	users to request certificates with domain.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Organization	Text	No	You can provide organization name. The discovered certificate's SubjectOrganization will be compared against the organization provided in the policy to identify if there are complaints. Organization is enforced while performing any certificate request operations such as New, Renew, Regenerate.	NA
Organization Unit	Text	No	You can provide an organizational unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to identify if there is a Complaint. Organization Unit is enforced while performing any certificate request operations such as New, Renew, Regenerate.	NA
Locality	Text	No	You can provide a locality.	NA

Name	Type	Mandatory	Description	Validation
			The discovered certificate's Locality will be compared against the locality provided in the policy to identify if they are Complaint. Locality is enforced while performing any certificate request operations such as New, Renew, Regenerate.	
State	Text	No	You can provide state. The discovered certificate's State will be compared against the state provided in the policy to identify if there is a complaint. State is enforced while performing any certificate request operations such as New, Renew, Regenerate.	NA
Country code	Text	No	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 there are complaints. Country code is enforced while performing any certificate request operations such as New, Renew, Regenerate.	NA
Email	Text	No	You can provide the organization unit mail address. The discovered certificate's mail address will be compared against the mail address provided in	NA

Name	Type	Mandatory	Description	Validation
			the policy to identify if there is a complaint. Mail address is enforced while performing any certificate request operations such as New, Renew, Regenerate.	
Subject Alternative Name	Text Area	No	You can provide the subject's 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.	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 (@)


Note: The asterisk (*) symbol indicates a mandatory field.

14. You can fill in the **Certificate parameters** section based on your organization's policies and standards.
15. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **GlobalSign MSSLOption** to indicate the details are successfully stored.
16. Click **Create Policy** button to create a new policy.
17. The policy is created and a confirmation message is displayed.

Configuring Policy for Nexus CA

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 **GROUPS & POLICIES**.

5. Click **CA Policy**.

CA Policy				+ Create	Delete
Search...				1 to 2 of 2	< > ↺
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the communication b...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide access to all certifi...	Default	Strict		

The CA Policy home page appears.

6. Click **+ Create** on the top-right of the page.

CA Policy : Create

Policy Details

Define rules and templates to ensure certificate attributes are in compliance with the Organization.

* Policy Name ⓘ x

Description 1998 remaining

Policy Enforcement Type ☒ Strict ☐ Suggestive ⓘ

Certificate Requests Need Approval? ☒

When enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. Peer approving the request is defined in the approval workflow.

Enable Access to Private Key? ☒

When enabled allows user to download private key from the Holistic View and Inventory.

Enable private key access for read-only user ☒

Enable certificate push-bind access for read-only user ☒

Enabling the option would allow user, with read only user group, to perform certificate push, bind and rollback operations from the Holistic View.

The **Create** policy page appears.

7. Refer [Configuring Policy Details](#) section in admin guide to configure,
 - **Policy Details**
 - **Group Selection**
 - **Compliance Check**
8. To configure a policy with Nexus details, click **Nexus** in the **Certificate Authority** pane on the left side of the screen.

The screenshot shows the 'Create Policy' page. On the left, the 'Certificate Authority' pane lists various CAs, with 'Nexus' highlighted. The main form contains the following fields:

- CA Accounts:** A dropdown menu showing 'Demo_Nexus_CA'.
- Validity:** A field with '365' entered, followed by 'Days', 'Months', and 'Years' options.
- Vendor specific details:**
 - Certificate Type:** Radio buttons for 'Server' and 'Client'.
 - Procedures:** A dropdown menu showing 'Select...'.

At the bottom, there is an 'Add' button and a table with the following structure:

CA Accounts	View	Edit	Remove
No records added...			

Buttons at the bottom include 'Create Policy' and 'Cancel'.

9. Select **CA accounts** and **Certificate Type** under the **CA details** section and provide the **Validity** period.

The screenshot shows the 'CA details' section with the following fields:

- CA Accounts:** A dropdown menu showing 'Select...'.
- Certificate Type:** A dropdown menu showing 'Select...'.
- Validity:** Three rows for 'Days', 'Months', and 'Years', each with a 'Type validity and press enter' input field.

An 'Add' button is located at the bottom.

The following table provides the field description under **CA Details** section:

Name	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.
*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	Provide the value and press Enter . Enforce Validity period for selected Certificate Type(s). The validity for Nexus CA can be represented in Day(s)/ Month(s)/ Year(s). One (or) more than one Validity period can be added.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. 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 drop-down list and click **Add** to save the CA details to the table. You can also use the **Remove** option to delete the configuration.

Vendor specific details

* Certificate Type ☐ Server ☐ Client

* Procedures

CA Accounts	View	Edit	Remove
No records added...			

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 2** - 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*

11. Click the **Add** button. The CA details are saved to the table and the confirmation message displays.
12. You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

CA Settings	Certificate Type	Edit	Remove
Trustwave CA_Server	SecureTrust Organization Validation SecureTrust OV Wildcard		

13. In the **CA details** section, select **Bit Length -Key Type**, **ECDSA curve**, and **Hash Function**.

* Bit Length - Key Type

×

521 - EC

×

4096 - RSA

×

2048 - DSA

Clear

ⓘ

* ECDSA curve

×

secp521r1 / P-521

Clear

ⓘ

* Hash Function

×

SHA512

×

SHA384

Clear

ⓘ

The following table provides the field description under **CA Details** section:

Name	Description	Purpose
*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 drop-down.	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 complaint with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate

Name	Description	Purpose
		request operations such as New, Renew, Regenerate.
*ECDSA curve	When Key Type is selected as EC, ECDSA curve corresponding to selected Key Type is listed. You can select one (or) more than one ECDSA curve from the drop-down for a certificate.	The discovered certificate's Key elliptic curves will be compared against the selected ECDSA curve(s) to identify if they are complaint with the policy. Selected ECDSA curve(s) is enforced while performing certificate request operations such as New, Renew, and Regenerate. We recommend using P256/ P384/ P521 ECDSA curve while enrolling.
*Hash Function	Supported Hash Function(s) are listed. You can select one (or) more than one Hash Function(s) from the drop-down.	The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are complaint with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as New, Renew, Regenerate.
 Note: The asterisk (*) symbol indicates a mandatory field.		

14. You can fill the **Certificate parameters** section based on your organization's policies and standards.

Certificate parameters

Compare the discovered certificate with the below to identify if it is Complaint. Additionally, below will also be enforced on a certificate request.

Common Name	Test.Userguide.com	
Organization	AppViewX_Tech Doc Team	
Organization Unit	AppViewX_Tech Doc Team	
Locality	Coimbatore	
State	Tamil Nadu	
Country code	India	
Email	<username>@<domainname>.com	
Subject Alternative Name		

CA Accounts	Issuer Region	Issuer Name	View	Edit	Remove
No records added...					

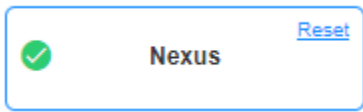
The following table provides the field description in the **Certificate parameters** section:

Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. Common Name is enforced while performing any 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.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)

Name	Description
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, 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, 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, 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, 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

Name	Description
	policy to identify if they are complaints. Country code is enforced while performing any certificate request operations such as New, Renew, 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 complaints. Mail address is enforced while performing any certificate request operations such as New, Renew, 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 (@)
 Note: The asterisk (*) symbol indicates a mandatory field.	

15. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Nexus** option to indicate the details are successfully stored.
16. Click **Create Policy** button to create a new policy.



17. The policy is created and a confirmation message displays.

CA Policy		Policy created.		+ Create	Delete
Q Search...		1 to 3 of 3		<	>
Policy Name	Description	Group	Type		
☐ Certificate-Gateway	A system policy assigned to enable the co...	Certificate-Gateway	Suggestive		
☐ Default	Default policy of AppViewX to provide acc...	Default	Strict		
☐ Presales		Demo-AppViewX	Strict		

Certificate Group

- Overview
- Assign Certificate to a Group
- Create a Group
- Delete a Group
- Modify a Group
- Unassign Certificate from a Group

Overview

Before you Begin

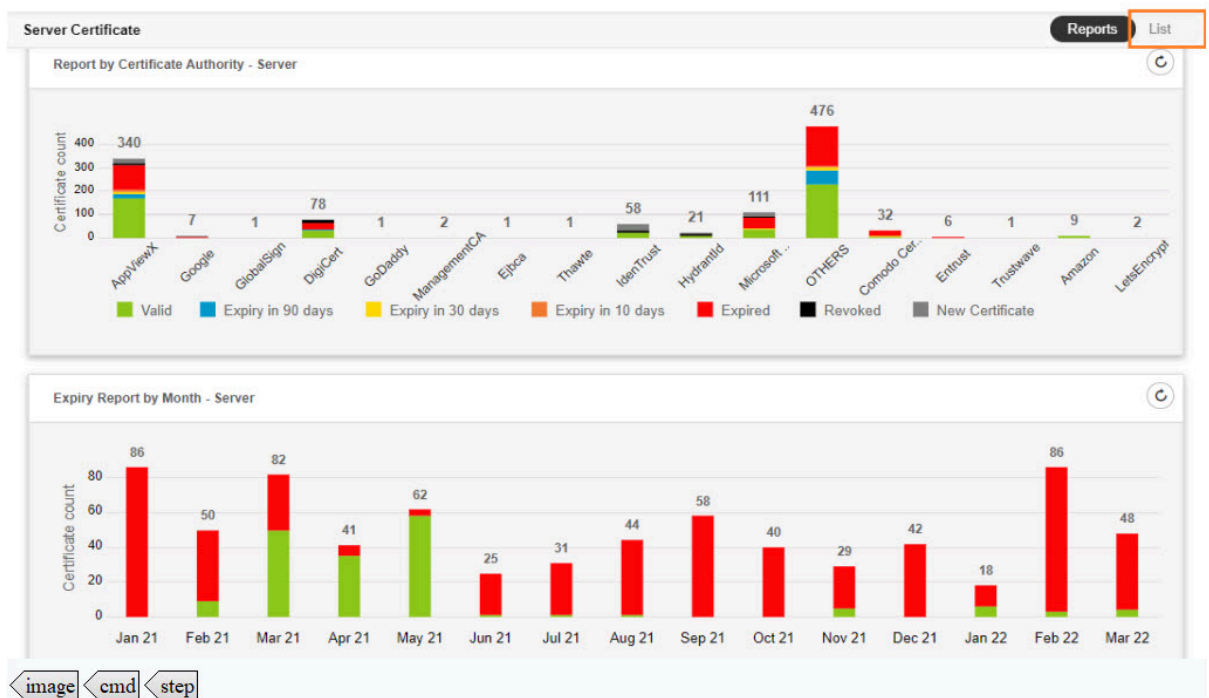
Following are the points needed to be known before starting **Certificate Groups** configuration:

- **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

Assign Certificate to a Group

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 **Server Certificate** Inventory appears.
4. Click **List** button on upper right of the server certificate inventory screen.



5. Select the check box against the certificate(s) you want to assign to a group.
6. Click the **Actions** drop-down and select the **Assign Group** option from the drop-down.

Server Certificate 222 Reports List

Groups All Certificates 222 Type your search and press Enter Actions Columns 1 to 25 of 222

Common Name	Serial Number	Group	Valid to (GMT)	Status
testcertacmnew1.appviewx.plus	12:CF:16:A1:2...	Default (RW)	04/22/2022 10:39	Managed
qaregressionawstesting	9D:C8:D6:F2:B...	Default (RW)	03/22/2022 05:47	Managed
ApacheWinPush.appviewx.comQS4DN	16:77:F7:DE:D...	Demo-... (RW)	03/22/2022 12:39	Managed
ApacheWinPush.appviewx.comPVDYY	B8:4E:43:0A:6...	Demo-... (RW)	03/22/2022 12:48	Managed
ApacheWinPush.appviewx.com88451	31:12:97:D3:65...	Demo-... (RW)	03/22/2022 12:34	Managed
ApacheWinPush.appviewx.comOYO15	1F:70:AB:E8:C...	Demo-... (RW)	03/22/2022 12:44	Managed
ApacheWinPush.appviewx.com8QL4L	41:10:2E:10:B9...	Demo-... (RW)	03/22/2022 12:29	Managed
ApacheWinPush.appviewx.comFQ5D9	54:19:3F:FD:D...	Demo-... (RW)	03/19/2022 09:01	Managed
ApacheWinPush.appviewx.com6Y4DD	C1:98:94:A5:C...	Demo-... (RW)	03/19/2022 09:11	Managed
ApacheWinPush.appviewx.comGPP1F	7F:BD:80:7F:B...	Demo-... (RW)	03/19/2022 08:55	Managed
ApacheWinPush.appviewx.comVQF92	D1:29:14:91:2...	Default (RW)	03/19/2022 09:06	Managed

Export Certificates
Download Certificates
Delete
Change Status
Assign Group
Unassign Group
Add/Modify Comments
Certificate Attributes
Renew Certificate
CA Switch
RC Revocation Check

Certificates can be assigned to another group for which certificate standards are applied.

- The **Assign to Group** pop-up appears. Select the **Group** from the list.
- Click the **Assign** button to move the certificate(s) to the selected **Group**.
- Click the **Groups** drop-down and select your **Group** from the drop-down.

Server Certificate 222 Reports List

Groups All Certificates 222 Type your search and press Enter Actions Columns 1 to 25 of 222

Search...

All Certificates 222

Default RW 214

Certificate-Gateway RW 8

Demo-AppViewX RW 8

Common Name	Serial Number	Group	Issuer Common Name	Valid to (GMT)	Status
AppViewX-AWS-SubCA	12:CF:16:A1:2...	Default (RW)	AppViewX-AWS-SubCA	04/22/2022 10:39	Managed
AppViewX Intermediate ...	9D:C8:D6:F2:B...	Default (RW)	AppViewX Intermediate ...	03/22/2022 05:47	Managed
AppViewX Intermediate ...	16:77:F7:DE:D...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:39	Managed
AppViewX Intermediate ...	B8:4E:43:0A:6...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:48	Managed
AppViewX Intermediate ...	31:12:97:D3:65...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:34	Managed
AppViewX Intermediate ...	1F:70:AB:E8:C...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:44	Managed
AppViewX Intermediate ...	41:10:2E:10:B9...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:29	Managed
AppViewX Intermediate ...	54:19:3F:FD:D...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:01	Managed
AppViewX Intermediate ...	C1:98:94:A5:C...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:11	Managed
AppViewX Intermediate ...	7F:BD:80:7F:B...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 08:55	Managed
AppViewX Intermediate ...	D1:29:14:91:2...	Default (RW)	AppViewX Intermediate ...	03/19/2022 09:06	Managed

10. You can view the certificate(s) assigned to the **Group**. The table provides certificate(s) details.

Server Certificate 222								Reports	List
Groups	Demo-AppViewX			Type your search and press Enter	Actions	Columns	1 to 8 of 8	<	>
☐	Common Name	Serial Number	Group	Issuer Common Name	Valid to (GMT)	Status			
☐	ApacheWinPush.appviewx.comQS4DN	16:77:F7:DE:D...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:39	Managed			
☐	ApacheWinPush.appviewx.comPVDYY	B8:4E:43:0A:6...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:48	Managed			
☐	ApacheWinPush.appviewx.com88451	31:12:97:D3:65...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:34	Managed			
☐	ApacheWinPush.appviewx.comOYO15	1F:70:AB:E8:C...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:44	Managed			
☐	ApacheWinPush.appviewx.com8QL4L	41:10:2E:10:B9...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:29	Managed			
☐	ApacheWinPush.appviewx.comFQ5D9	54:19:3F:FD:D...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:01	Managed			
☐	ApacheWinPush.appviewx.com6Y4DD	C1:98:94:A5:C...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:11	Managed			
☐	ApacheWinPush.appviewx.comGPP1F	7F:BD:80:7F:B...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 08:55	Managed			

Create a Group

Assign the user to a user group that (inherits from resource and role) have access to certificate group

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. Click **Groups** under **Groups & Policies**.
The Group inventory appears.
5. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway**.
6. Click the **+ Create** button in the command bar to create a new group.

Group									
	Search...							+ Create	Delete
								1 to 2 of 2	< > ↺
☐	Name	Description	Application ID	Server Certifi...	Client Certific...	Device Certifi...	Code Signing...	Policy Associated	App Pol
☐	Certificate-Gateway (RW)			0	0	0	0	Certificate-Gateway	
☐	Default (RW)	Default Group		222	0	0	0	Default	

The following table provides the field description under the **Group Details** section:

Name	Type	Mandatory	Description	Validation
Select Group Hierarchy	Select	Yes	Select the parent group to which the new group should be associated	NA
Group Name	Text	Yes	Enter a unique name for the new group	The name should not start with special characters and spaces. No special characters are allowed except('.', '-', '_') and name cannot end with space
Application ID	Text	No	Provide organization ID (if any) to associate with the new group	NA
Description	Text	No	Provide the purpose of the new group	NA
 Note: The asterisk (*) symbol indicates a mandatory field.				

7. Group Name is mandatory in the **Group Details** section. Provide the **Group Name** to create a new group.

Group Details

* Select Group Hierarchy ⓘ

* Group Name ⓘ

Application ID ⓘ

Description

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
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
 Note: The asterisk (*) symbol indicates a mandatory field.				

8. The fields in the **Other Details** section are used based on the organization's needs.

Other details

Contact Name		
Line of Business Name		
Email		
Environment Name		
Phone Number		
Inventory Number		
Cost Center/Hierarchy		
Push Certificate Automatically	☐	
Renew Automatically	Off	
* Associated Policy	Default 	

9. 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**. Refer the [Create a Resource](#) section to configure user access.

10. The newly created **Group** is added to the Group inventory. Click the **Name** (Group name) to view the group details.

Q Search...

+ Create

Delete

1 to 3 of 3

<

>

☐	Name	Description	Application ID	Server Certifi...	Client Certific...	Device Certifi...	Code Signing...	Policy Associ...	App Policy
☐	Certificate-Gateway	(RW)		0	0	0	0	Certificate-Gat...	
☐	Default	(RW)	Default Group	222	0	0	0	Default	
☒	DemoAppViewX	(RW)		0	0	0	0	Default	

11. Post certificate discovery, you can view the count of certificates (Server, Client, Device, and Code Signing) associated with this group.

12. Click the count to view the certificates.

Q Search...

+ Create

Delete

1 to 3 of 3

<

>

↺

☐	Name	Description	Application ID	Server Certifi...	Client Certific...	Device Certifi...	Code Signing...	Policy Associ...	App Policy
☐	Certificate-Gateway (RW)			0	0	0	0	Certificate-Gat...	
☐	Default (RW)	Default Group		217	0	0	0	Default	
☐	DemoAppViewX (RW)			5	0	0	0	Default	

Delete a Group

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. Click **Groups** under **Groups & Policies**.
The **Group** inventory appears.
5. In the group inventory, select the check box against the group you want to delete.

6. Click the **Delete** () icon in the command bar to delete the Group.

Group

Q Search...

+ Create

Delete

1 to 3 of 3

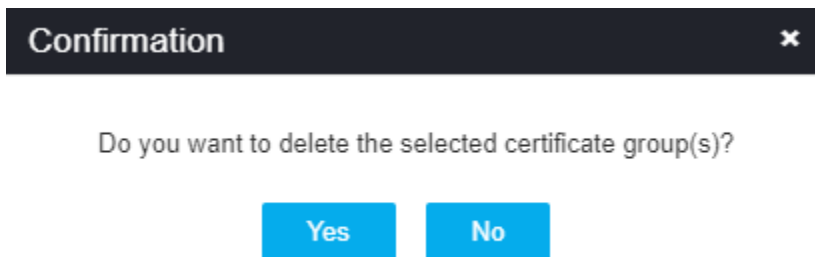
<

>

↺

☐	Name	Description	Application ID	Server Certi...	Client Certifi...	Device Certi...	Code Signin...	Policy Asso...	App Policy ...
☐	Certificate-Gateway (RW)			0	0	0	0	Certificate-G...	
☐	Default (RW)	Default Group		217	0	0	0	Default	
☒	DemoAppViewX (RW)			5	0	0	0	Default	

7. A confirmation pop-up appears. Click the **Yes** button to proceed.



The group is deleted and a confirmation message displays.

Modify a Group

Assign the user to a user group that (inherits from resource and role) have access to the certificate group

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. Click **Groups** under **Groups & Policies**.

The group inventory appears.

5. Click the **Name** (Group name) to view the group details.

Q Search...				+ Create	Delete	1 to 3 of 3	<	>	↺
☐	Name [▲]	Description	Application ID [⬇]	Server Certifi...	Client Certific...	Device Certifi...	Code Signing...	Policy Associ...	App Policy
☐	Certificate-Gateway (RW)			0	0	0	0	Certificate-Gat...	
☐	Default (RW)	Default Group		217	0	0	0	Default	
☐	DemoAppViewX (RW)			5	0	0	0	Default	

6. Modify required fields in the group and click the **Update** button. Field descriptions are available in [Create a Group](#) section.

7. The changes are updated and a confirmation message displays.

Group									
✔ Group updated ✖									
Q Search...				+ Create	Delete	1 to 3 of 3	<	>	↺
☐	Name [▲]	Description	Application ID [⬇]	Server Certifi...	Client Certific...	Device Certifi...	Code Signing...	Policy Associ...	App Policy
☐	Certificate-Gateway (RW)			0	0	0	0	Certificate-Gat...	
☐	Default (RW)	Default Group		217	0	0	0	Default	
☐	DemoAppViewX (RW)			5	0	0	0	Default	

Unassign Certificate from a Group

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+** on the left navigation pane.

The **Server Certificate** Inventory appears.

4. Click the **List** button on the upper right of the server certificate inventory screen.



5. Click the **Groups** drop-down and select a **Group** from the drop-down.

Server Certificate 222 Reports **List**

Groups All Certificates 222

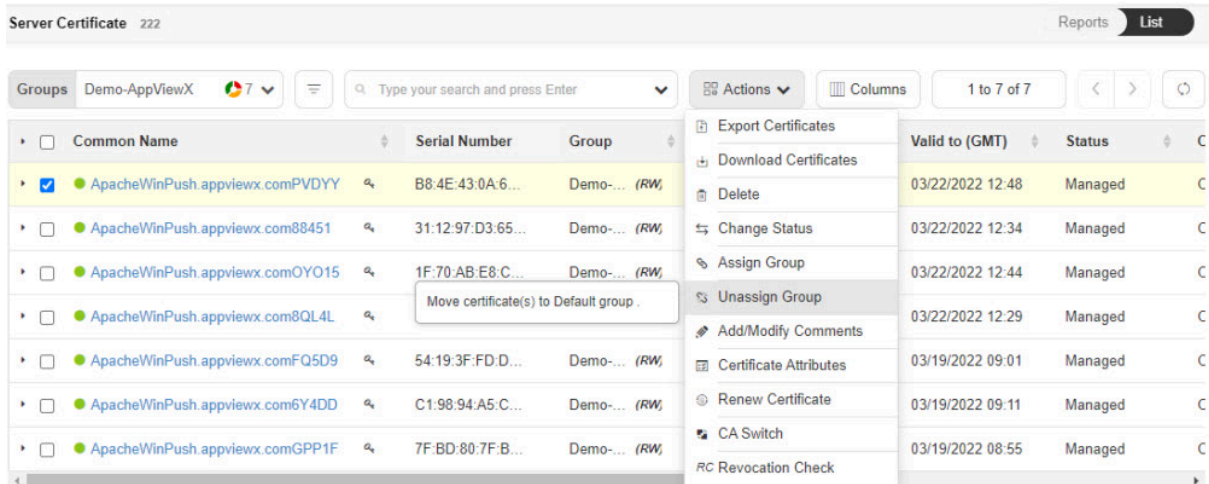
Search... Type your search and press Enter

Actions Columns 1 to 25 of 222

Serial Number	Group	Issuer Common Name	Valid to (GMT)	Status
12:CF:16:A1:2...	Default (RW)	AppViewX-AWS-SubCA	04/22/2022 10:39	Managed
9D:C8:D6:F2:B...	Default (RW)	AppViewX Intermediate ...	03/22/2022 05:47	Managed
16:77:F7:DE:D...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:39	Managed
B8:4E:43:0A:6...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:48	Managed
31:12:97:D3:65...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:34	Managed
1F:70:AB:E8:C...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:44	Managed
41:10:2E:10:B9...	Demo-... (RW)	AppViewX Intermediate ...	03/22/2022 12:29	Managed
54:19:3F:FD:D...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:01	Managed
C1:98:94:A5:C...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 09:11	Managed
7F:BD:80:7F:B...	Demo-... (RW)	AppViewX Intermediate ...	03/19/2022 08:55	Managed
D1:29:14:91:2...	Default (RW)	AppViewX Intermediate ...	03/19/2022 09:06	Managed

6. Select the check box against the certificate you want to unassign from the group.

7. Click the **Actions** drop-down and select the **Unassign Group** option from the drop-down.



8. 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**.

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

Following are the prerequisites for configuring Password Vault AppViewX:

- Need to have a valid certificate password for password-protected certificates to decrypt.

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 **ADMINISTRATION**, and then click **Password Vault**.

5. On the screen that appears, enter an Identity Name of the password you want to add in the vault.

6. From the **Device Name** dropdown, select the ADC device whose password-protected certificate details you want to store.

7. In the **File Name** field, enter a certificate file name to help users identify it.

8. In the **Password** field, enter the password that is associated with the certificate.

9. Click **Save**.

10. 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.

The top screenshot shows the 'Password Vault' page in AppViewX. The left navigation pane is open, showing 'CERT+' and 'ADMINISTRATION' with 'Password Vault' selected. The main content area has a 'General Information' section with a description: 'Using vault you can store the keystore passwords and encrypted key passwords which will be used while discovery'. Below this are four required fields: 'Identity Name', 'Device Name' (a dropdown menu), 'File Name', and 'Password'. There are 'Save' and 'Reset' buttons at the bottom. In the top right corner, there are 'Import' and 'Export Password' buttons, with 'Import' highlighted by a red box.

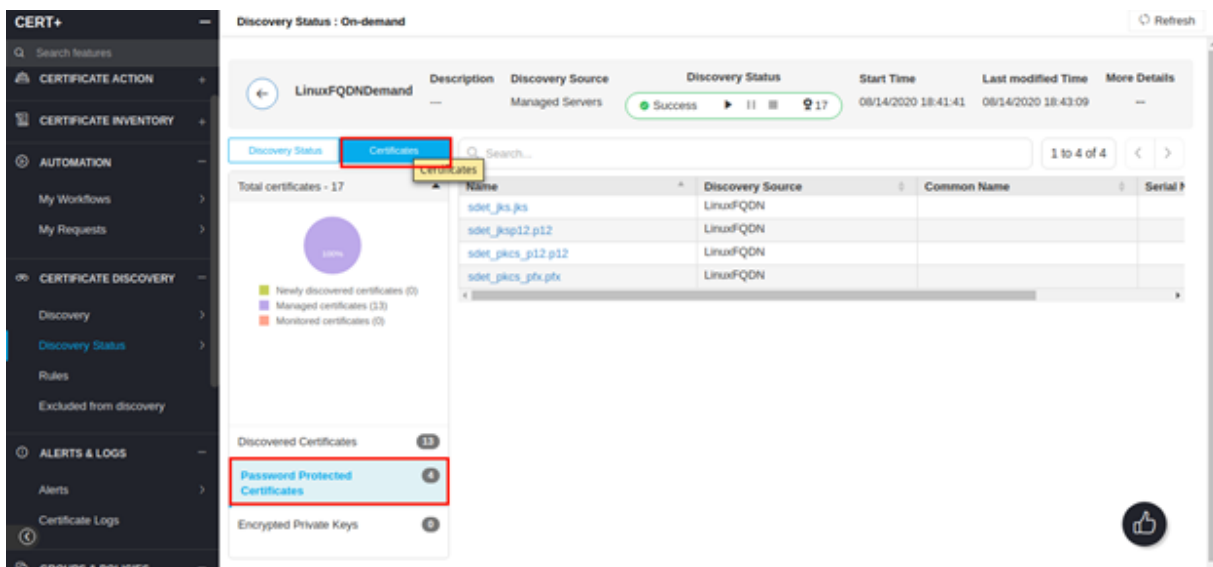
The bottom screenshot shows the 'Import' dialog. It has a title bar 'Password Vault : Upload' and a status message 'Password vault is updated with selected valid data.' Below this is the 'Import' section with a 'Select a File' field containing 'Cert_PasswordVault_Template.xlsx' and an 'Upload' button. At the bottom, there is a 'Save to Password Vault' button highlighted with a red box, and a 'Cancel' button. A status bar at the very bottom indicates 'Imported :3; Invalid records :0; Not selected :0'.

11. Click **Export Password** on the top-right to export all stored certificate passwords from the vault as a zip file to your computer.
12. To modify the existing details, Click **Edit**.
13. To update the password, click **Update**.
14. 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. 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 > **CERT+** > **CERTIFICATE DISCOVERY**.
5. Under **Certificate Discovery**, navigate to **Discovery Status > OnDemand**.
6. Click on the **discovery name** under discovery inventory.
7. Click **Certificates** under the tab.
8. To view all password-protected certificates, click **Password Protected Certificates**.



Configuring Certificate Attributes

- [Configuring Attribute Information](#)
- [Update Certificate Attribute](#)
- [Delete Certificate Attribute](#)
- [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 requestor enrolling a certificate can fill and use for future tracking.

Before you Begin

Following are the points needed to be known before starting the configuration for Certificate attributes:

- 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.

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. **Expand ADMINISTRATION**, and then select **Certificate Attributes**.

5. Click **Add New**.

6. Configure the **Attribute Information** details as mentioned below.

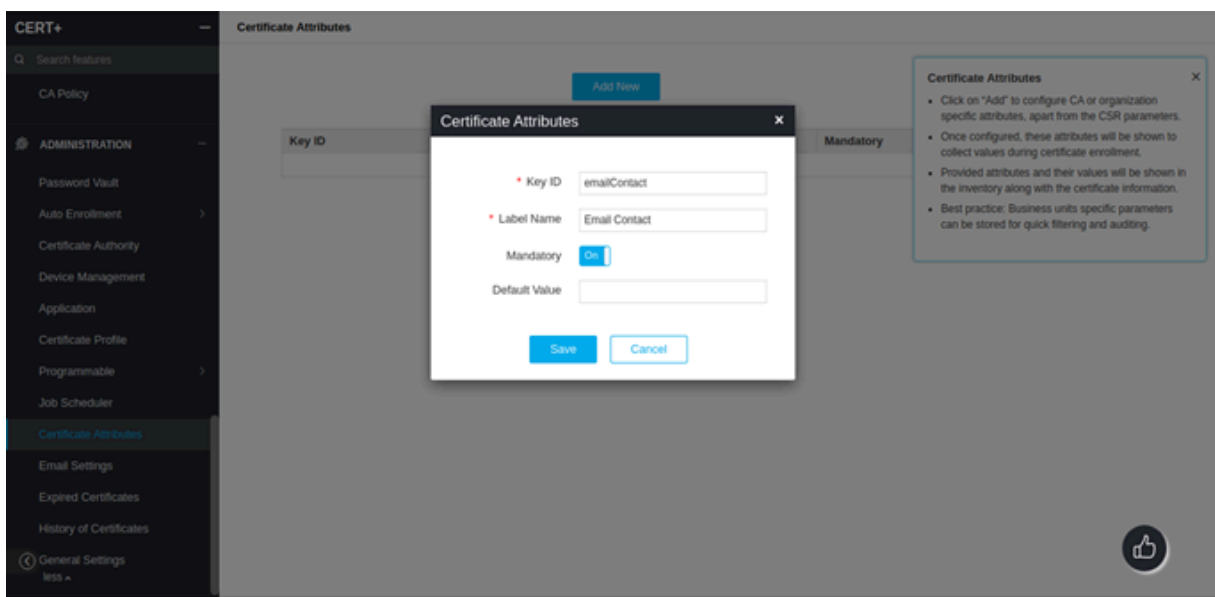
Name	Description	Validation
*Key ID	Unique key for the attribute.	Key ID must not start with special characters. No special characters except -, _ are allowed.
*Label Name	Attribute name which will be shown during certificate enrollment. Eg. Email Contact, Owner.	Label name should not start with special characters. No special characters except -, _ and spaces are allowed.

Name	Description	Validation
Mandatory	Enable if this field needs to be mandatory.	NA
Default Value	Set default value to the attribute.	NA



Note: These attributes support only text fields and are applicable for all CAs.

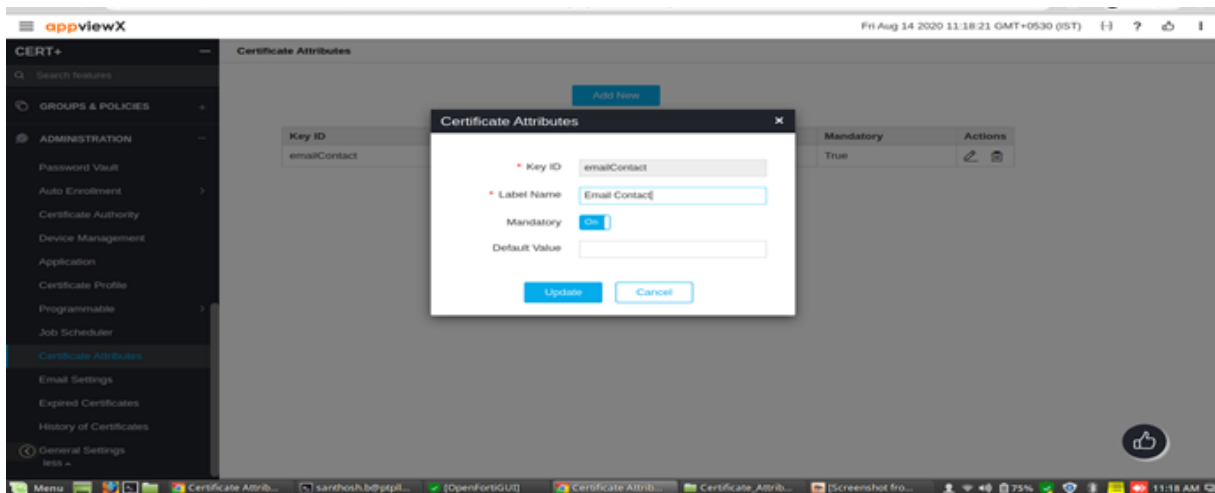
7. **Save** the attribute.



Update Certificate Attribute

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. **Expand ADMINISTRATION**, and then select **Certificate Attributes**.
5. Select the **Edit** icon under **Actions**.

6. Update the Edit existing values.



Delete Certificate Attribute

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. **Expand ADMINISTRATION**, and then select **Certificate Attributes**.
5. Under **Actions**, click **Delete**.

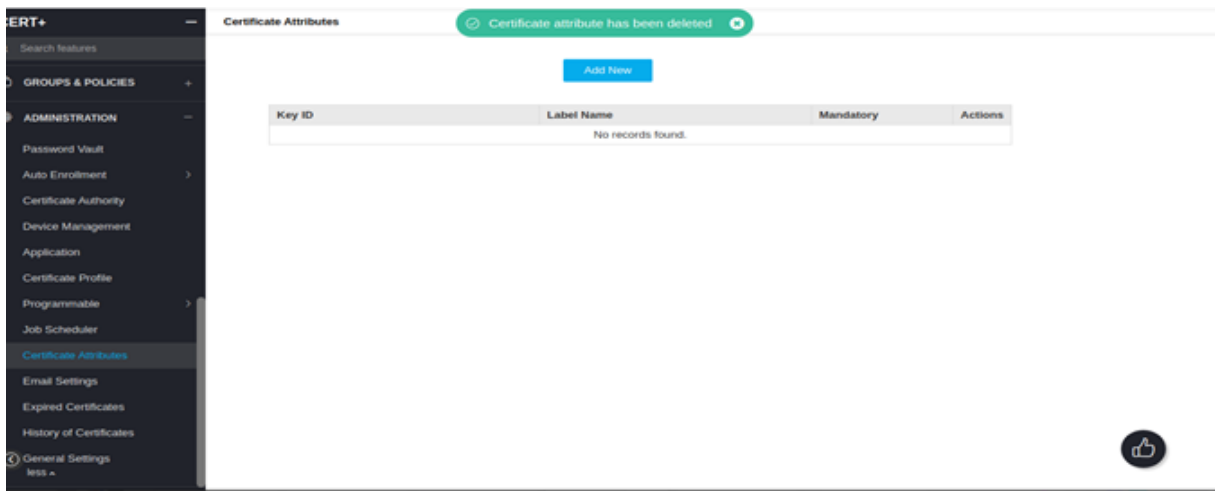
Certificate Attributes in Certificate Enrollment

After configuring certificate attributes, these attributes will be displayed in the certificate enrollment page. We can provide values for these attributes.

if we already provide default values for these attributes in configuration those values will be shown.

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. **Expand CERTIFICATE ACTION**, and then select **Enroll Certificate**.

5. Select any one **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. 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. **Expand CERTIFICATE INVENTORY**, and then select **Server** or **Client** or **Code Signing**.
5. Click the **Columns** icon.

Select certificate attributes to display in the certificate inventory.

- [Configuring Auto-Removal of Expired Certificates](#)

Configuring Auto-Removal of Expired Certificates

Before you Begin

Following are the points needed to be known before starting the configuration for expired certificates:

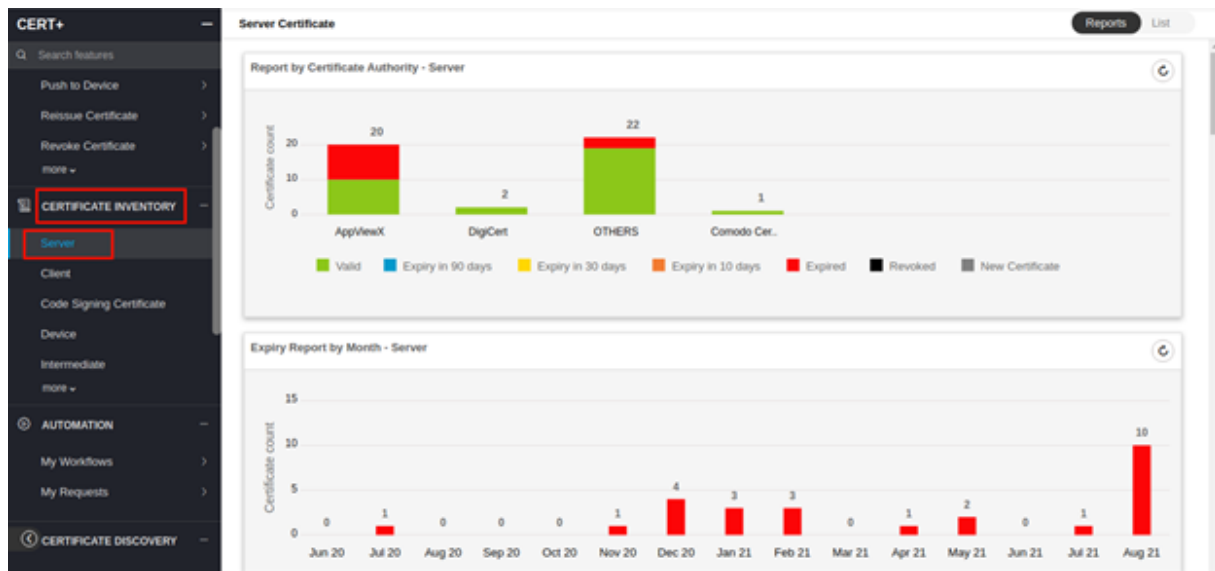
- This feature, if enabled, will delete all the expired certificates after configured no. of days from their expiration date and will remove them from the certificate inventory.

- Fetch Expired Certificates in the Inventory
- Configuring Expired Certificates
- Configuring Renew/Regenerate History

Fetch Expired Certificates in the Inventory

All the Expired certificates can be fetched in the certificate inventory by following the steps shown below.

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. Expand **CERTIFICATE INVENTORY**, and then select anyone **Server** or **Client** or **Code Signing** or **Certificate** or **Device**.
5. 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.
6. Click on the **Filter Summary** icon then select **Expired** to get a list of all the expired certificates present in the inventory.



Configuring Expired Certificates

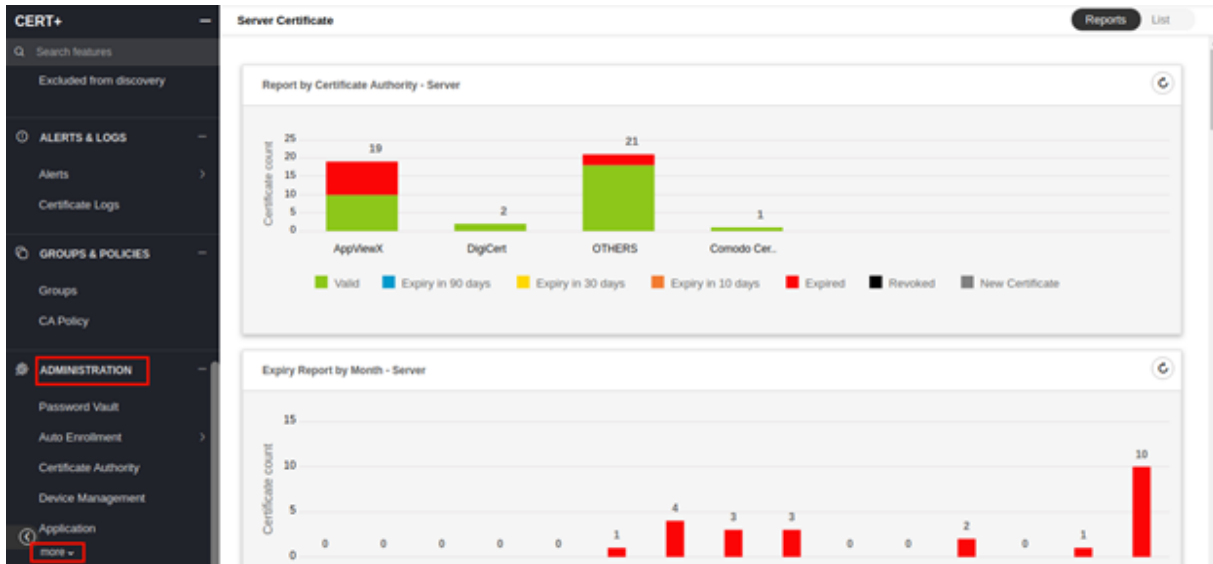
1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button.

The left navigation pane appears.

3. Click **CERT+**.

The **CERT+** left navigation pane appears.

4. Expand **ADMINISTRATION**.



5. Under **Administration**, click **Expired Certificates**.

The screenshot shows the 'Expired Certificates' settings page. The left navigation pane is visible with 'Expired Certificates' selected. The main content area includes a confirmation dialog and a settings form.

Expired Certificates

Do you want to delete the expired certificate after its expiry? ☒ Yes ☐ No

* Number of days after expiry:

Expired Certificates

- Enable "Yes" to delete the expired certificates.
- Once enabled, the certificate will be automatically deleted once expired after configured number of days.
- Best Practice: During certificate discovery, rule can be applied to not to discover the expired certificates.

6. Enter the information required as per the table given below. Each of the fields used for configuration of expired certificates.

Name	Description	Validation
*Do you want to delete the expired certificate after its expiry?	Option to enable/disable auto removal of expired certificates after expiry.	NA
*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.



Note: The asterisk (*) symbol indicates a mandatory field.

7. Click **Save**.
8. Click **Reset** to revert to the previously saved settings.

Configuring Renew/Regenerate History

Before you Begin

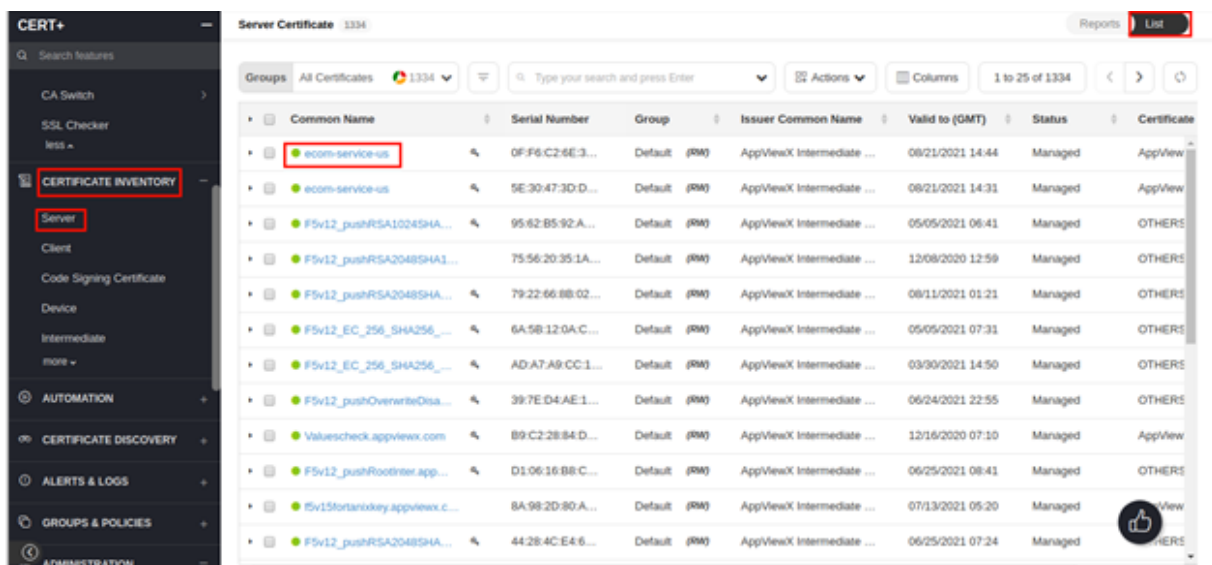
Following are the points needed to be known before starting the configuration for the history of certificates:

- 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.
- [Check History of Renewed/Regenerated Certificates](#)
- [Configuring History of Certificates](#)

Check History of Renewed/Regenerated Certificates

History of certificates, if enabled, can be checked on the Certificate Topology page by following these steps:

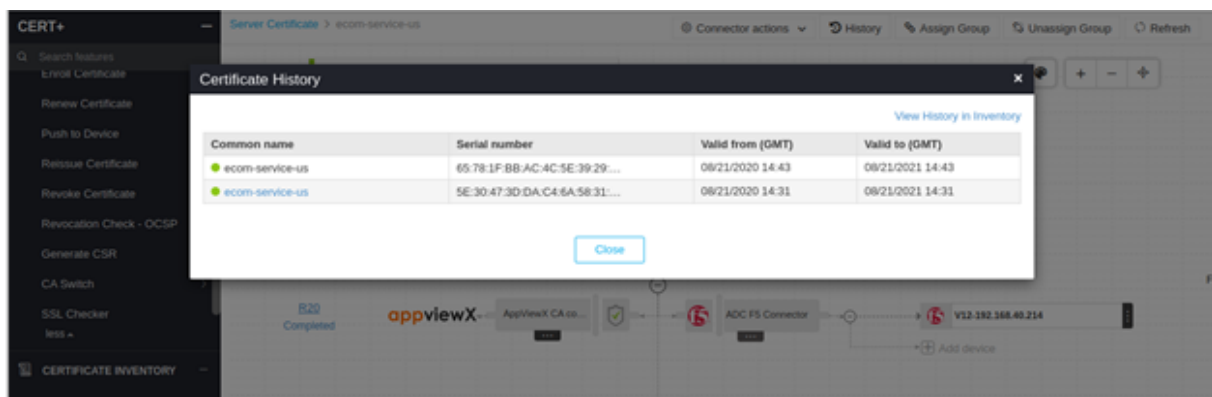
1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button.
The left navigation pane appears.
3. Click **CERT+**.
The **CERT+** left navigation pane appears.
4. **Expand CERTIFICATE INVENTORY.**
5. Under **CERTIFICATE INVENTORY**, select the type of certificate for which history is to be checked.
6. Click on the **List** tab on the top-right corner to view the certificates list page.
7. 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.



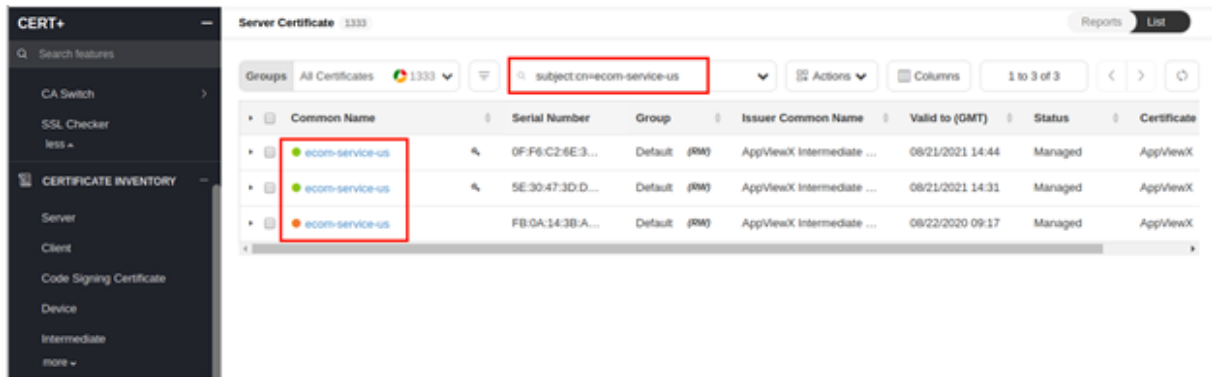
8. Click on the (History) icon on the certificate topology page to check the History of certificate. If the certificate renewal/regeneration was successful, the History icon will be present.



9. Click on the History to view the history of the certificate in the pop-up window.



10. The respective query for this will be automatically framed and search results will be shown.



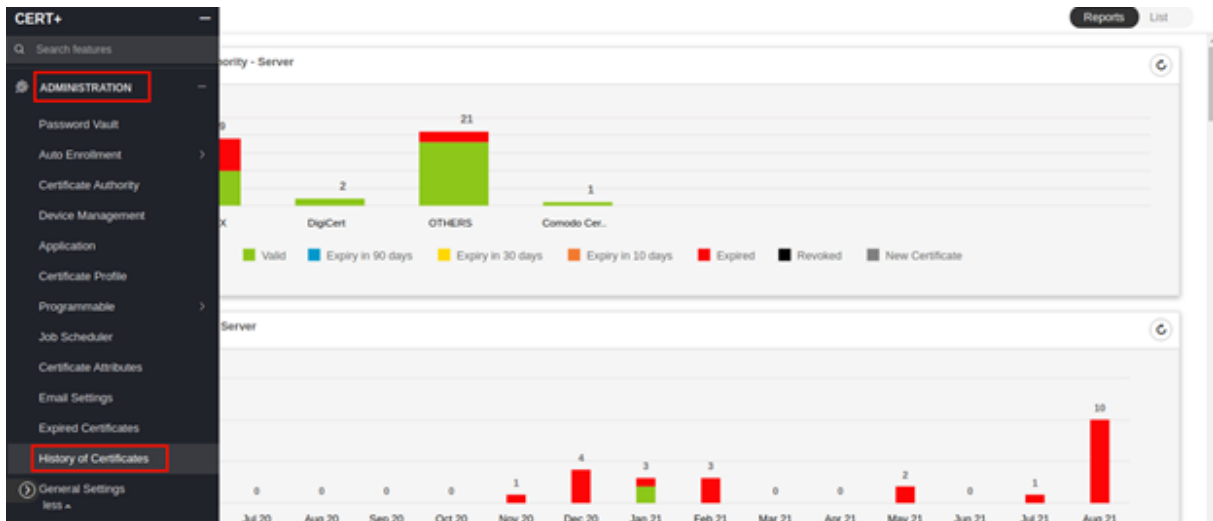
Common Name	Serial Number	Group	Issuer Common Name	Valid to (GMT)	Status	Certificate
ecom-service-us	0FF6C26E3...	Default (RM)	AppViewX Intermediate ...	08/21/2021 14:44	Managed	AppViewX
ecom-service-us	5E30473D...	Default (RM)	AppViewX Intermediate ...	08/21/2021 14:31	Managed	AppViewX
ecom-service-us	FB0A143B...	Default (RM)	AppViewX Intermediate ...	08/22/2020 09:17	Managed	AppViewX



Note: 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 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 History of Certificates

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 ADMINISTRATION.**
5. Under **Administration**, click **History of Certificates**.



6. Refer to the fields table below and fill out the information to configure.

Name	Type	Mandatory	Description	Validation
Do you want to maintain the history of the certificate after its renew/reissue/regeneration?	Option button	Yes	Option to select if the user wants to maintain the history of the certificates after it's renewed/reissue/regeneration or not.	NA

7. Click **Save**.

8. Click **Reset** to revert to the previously saved settings.

History Of Certificates

Do you want to maintain the history of certificate after its renew/reissue/regeneration?

☒ Yes ☐ No

Save **Reset**

History Of Certificates

On click "Yes", the history of old certificates before renew/regenerate/reissue action will be available in the inventory and tracked in the holistic view as well.

Configuring Certificate Profiles

- [Overview](#)
- [Configuring Certificate Profiles](#)
- [Update Certificate Profile](#)
- [Delete Certificate Profile](#)

Overview

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 whitelabel AppViewX CA through Custom CA.

Before you Begin

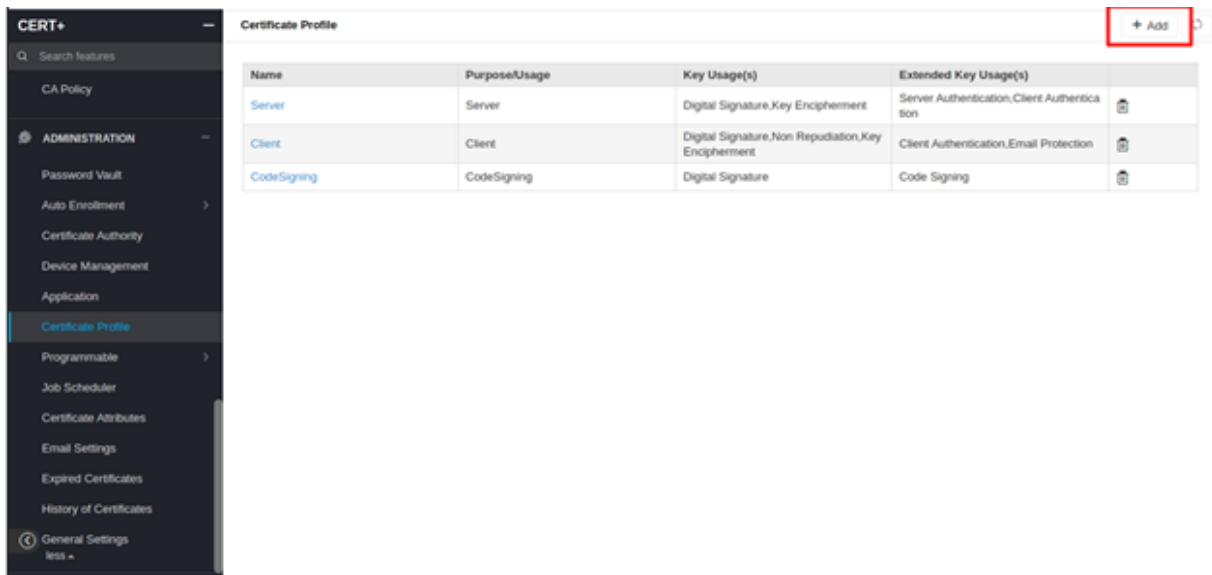
Following are the points needed to be known before starting to configure Certificate profile -

- 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 Whitelabeled 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

To add a new certificate profile:

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+ > ADMINISTRATION**.
4. Under **Administration**, select **Certificate Profile**.
5. Click **+ Add**.



6. Configure the **General Information** details as follows:

Certificate Profile

General Information

* Name

* Purpose/Usage

Name	Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the profile.	Profile name should not start with special characters. Can contain only alphanumeric characters, no special characters except -, _, . are allowed.
Purpose/Usage	Multi - Select	Yes	Certificate Type to which the Key	NA

Name	Type	Mandatory	Description	Validation
			Usage extensions are signed with. For example: Server or Client.	

7. Configure the **Key Usages** as given below.

Key Usages

Critical ☒

* Key Usage(s) Digital Signature, Data Encipherment

Name	Type	Mandatory	Description	Validation
Critical	Checkbox	No	Enable this field to sign the Key Usage extensions as critical .	NA
Key Usage(s)	Multi - Select	Yes	Key Usage extensions along with which the CSR is signed.	NA

8. Configure the **Extended Key Usages** as given below.

Extended Key Usages

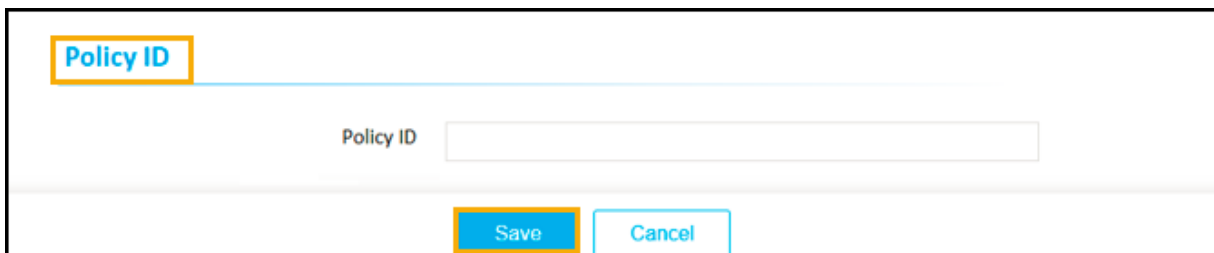
Critical ☐

* Extended Key Usage(s) Server Authentication, Client Authentication

Save Cancel

Name	Type	Mandatory	Description	Validation
Critical	Checkbox	No	Enable this field to sign the Extended Key Usage extensions as critical .	NA
Extended Key Usage(s)	Multi - Select	Yes	Extended Key Usage extensions along with which the CSR is signed.	NA

9. In the **Policy ID** section, enter the policy id in the field as given below.



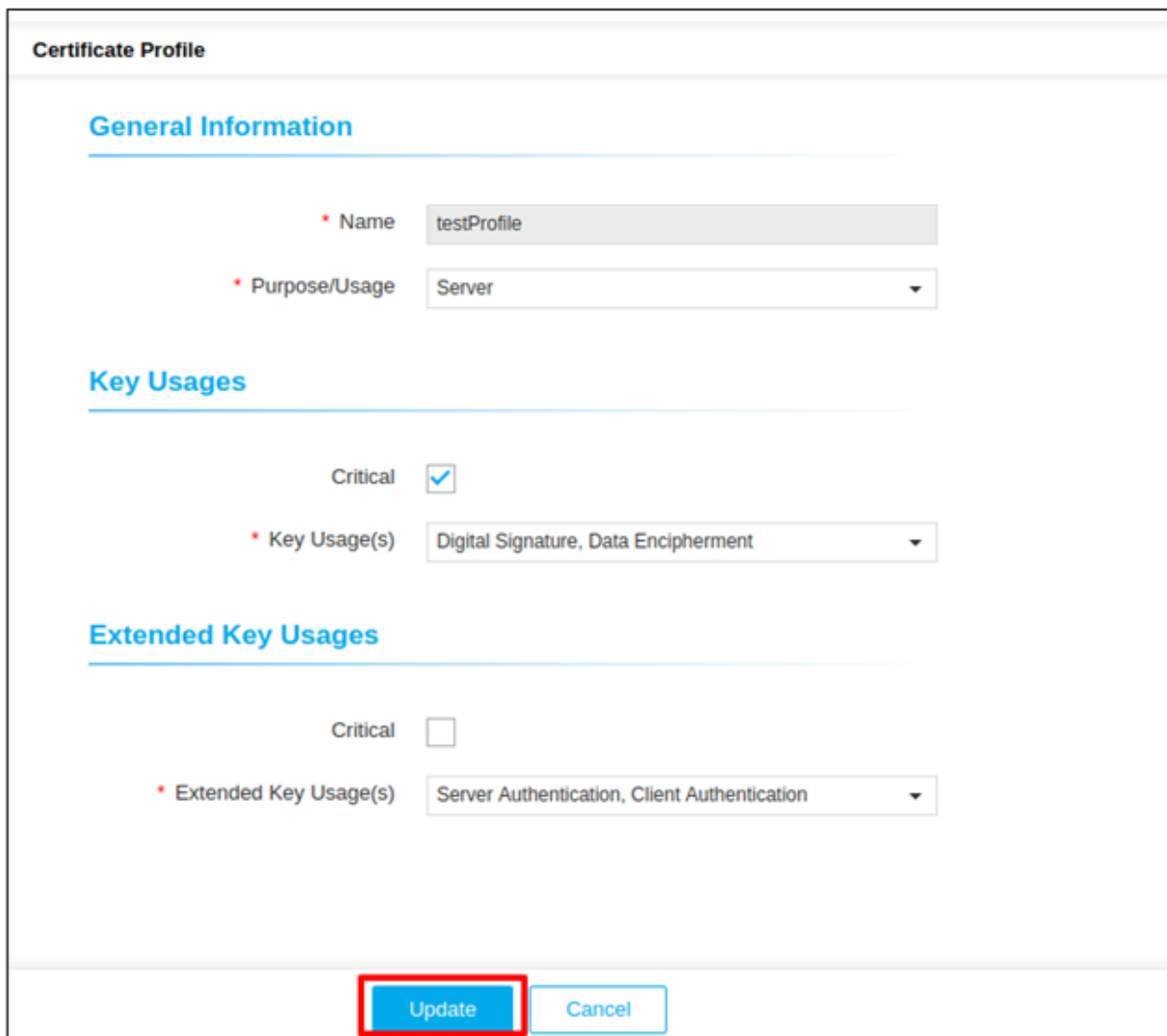
10. Click **Save**.

Update Certificate Profile

To update certificate profile settings:

1. Click **Menu > CERT+ > ADMINISTRATION**.
2. Under Administration, select **Certificate Profile**.
3. Click on the Profile that needs to be edited.
4. Edit existing values.

5. Click **Update**.



The image shows a 'Certificate Profile' configuration window. It has three main sections: 'General Information', 'Key Usages', and 'Extended Key Usages'. In the 'General Information' section, the 'Name' field is set to 'testProfile' and the 'Purpose/Usage' dropdown is set to 'Server'. In the 'Key Usages' section, the 'Critical' checkbox is checked, and the 'Key Usage(s)' dropdown is set to 'Digital Signature, Data Encipherment'. In the 'Extended Key Usages' section, the 'Critical' checkbox is unchecked, and the 'Extended Key Usage(s)' dropdown is set to 'Server Authentication, Client Authentication'. At the bottom, there are two buttons: 'Update' (highlighted with a red rectangle) and 'Cancel'.

Certificate Profile

General Information

* Name: testProfile

* Purpose/Usage: Server

Key Usages

Critical: ☒

* Key Usage(s): Digital Signature, Data Encipherment

Extended Key Usages

Critical: ☐

* Extended Key Usage(s): Server Authentication, Client Authentication

Update **Cancel**

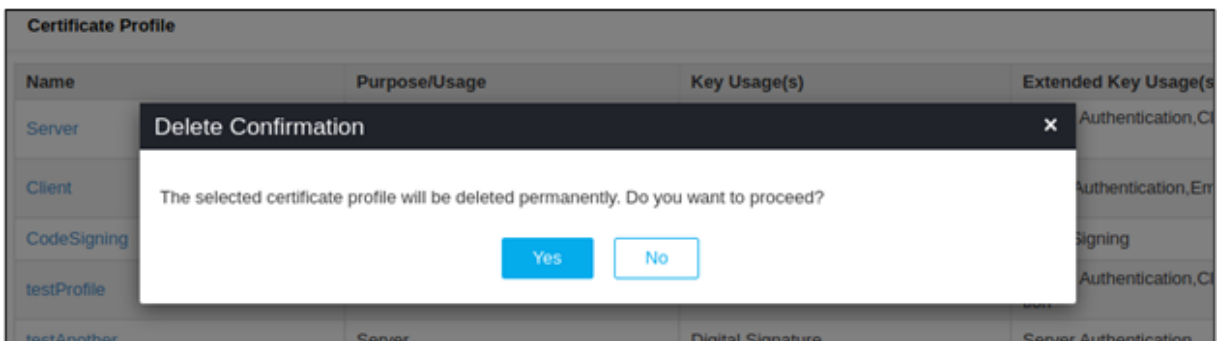
Delete Certificate Profile

To delete the certificate profile settings:

1. Click **Menu > CERT+ > ADMINISTRATION**.
2. Under **Administration**, select **Certificate Profile**.
3. Click **Delete** against the Profile to be deleted.

Certificate Profile				
Name	Purpose/Usage	Key Usage(s)	Extended Key Usage(s)	
Server	Server	Digital Signature,Key Encipherment	Server Authentication,Client Authentication	
Client	Client	Digital Signature,Non Repudiation,Key Encipherment	Client Authentication,Email Protection	
CodeSigning	CodeSigning	Digital Signature	Code Signing	
testProfile	Server	Digital Signature,Data Encipherment	Server Authentication,Client Authentication	
testAnother	Server	Digital Signature	Server Authentication	

4. Click **Yes** in the **Delete Confirmation** popup.



Managing Devices

- [Overview](#)
- [Configuring Servers](#)

Overview

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 an administrator or user 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

- [Add Server Details](#)
- [Delete Server Details](#)
- [Manage Server Details](#)

- [Unmanage Server Details](#)
- [Export Server Details](#)
- [Import Server Details](#)
- [Fetch Config for Server](#)
- [Add Credentials](#)
- [Configuring Firewall](#)
- [Delete a Firewall](#)
- [Manage Firewall](#)
- [Unmanage Firewall](#)
- [Export Firewall Details](#)
- [Import Firewall Details](#)
- [Fetch Config for Firewall](#)
- [Configuring Cloud](#)
- [Delete a Cloud](#)
- [Manage Cloud](#)
- [Unmanage Cloud](#)
- [Export Cloud Details](#)
- [Import Cloud Details](#)
- [Fetch Config for Cloud](#)

Add Server Details

To add the server,

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 **Inventory** > **Device**.

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

4. Click the **Server** tab.
5. Click the **Add** button.

The **Device details** page appears.

6. Select the desired vendor from the Vendors list.
7. In the **Server details** section, select/enter the details as follows.

Server details

* Server type ☐ Apache ☒ Tomcat

* Server name

* Hostname

Data center

Communication mode ☒ Gateway ☐ SSM

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

The following table describes the options available in the Server details section:

Options	Description
*Server Type	Select the required server type.

Options	Description
	 Note: Based on Vendor selected, this option would appear as radio button with options for <i>Apache</i> and <i>Tomcat</i> , or a dropdown option with a list of servers to select from.
*Server name	Enter the name of the server.
Hostname	Enter the name of the host.
Data center	Select the data center from the dropdown list.
Communication mode	Select the required communication mode. The possible options are: • Gateway • SSM
Cert sync	Select the required cert sync. The possible options are: • Managed • Monitored • Ignored.
 Note: The asterisk (*) symbol indicates a mandatory field.	

8. In the **Credentials** section, select/enter the details as follows.

Credentials

* Credential type

* Username

* Password

The following table describes the options available in the **Credentials** section:

Options	Description
*Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. a. Credential List - AppViewX b. Credential List - CyberArk c. Credential List - Thycotic Secret As part of release 2022.1.0 FP1, the value Credential List - Thycotic Secret will now be available for the following vendors: • Linux • Microsoft IIS • Microsoft Server
*Username	Enter the desired username. This field is displayed only if the Credential Type = Manual
*Password	Enter the secure password. This field is displayed only if the Credential Type = Manual
*Credential list	Select the credential value set in the Credentials page. This field is displayed only if the Credential Type is any of the below values: a. Credential List - AppViewX b. Credential List - CyberArk c. Credential List - Thycotic Secret
 Note: The asterisk (*) symbol indicates a mandatory field.	

9. In the **Windows gateway details** section, select/enter the details as follows.

Windows gateway details

* Gateway type ☒ PowerShell ☐ WMI

* Gateway location ☒ Remote

* Select gateway ☐ New ☒ Existing

* Windows gateway

The following table describes the options available in the **Windows gateway details** section:

Options	Description
*Gateway type	Select the required type of gateway. The possible options are: • PowerShell • WMI.
*Gateway location	Select the gateway location.
*Select gateway	Select the gateway. • New • Existing.
*Windows gateway	Select the windows gateway from the dropdown list.
 Note: The asterisk (*) symbol indicates a mandatory field.	

10. In the **Certificate details** section, enter the server path.

Certificate details

* Server path

C:\Tomcat8\Apache-Tomcat-8.5.35

Add

Enter the following path as mentioned in the table, depends on the OS that you choose:

OS	Server Path
Windows	C:\Tomcat8\Apache-Tomcat-8.5.35
Linux	/opt/tomcat/apache-tomcat-9.0.52

- Click the **Add** button.
- Once the server is added successfully, the server path will be listed in the **Server path** section.

Server path	Delete
/opt/tomcat/apache-tomcat-9.0.52	
C:\Tomcat8\Apache-Tomcat-8.5.35	

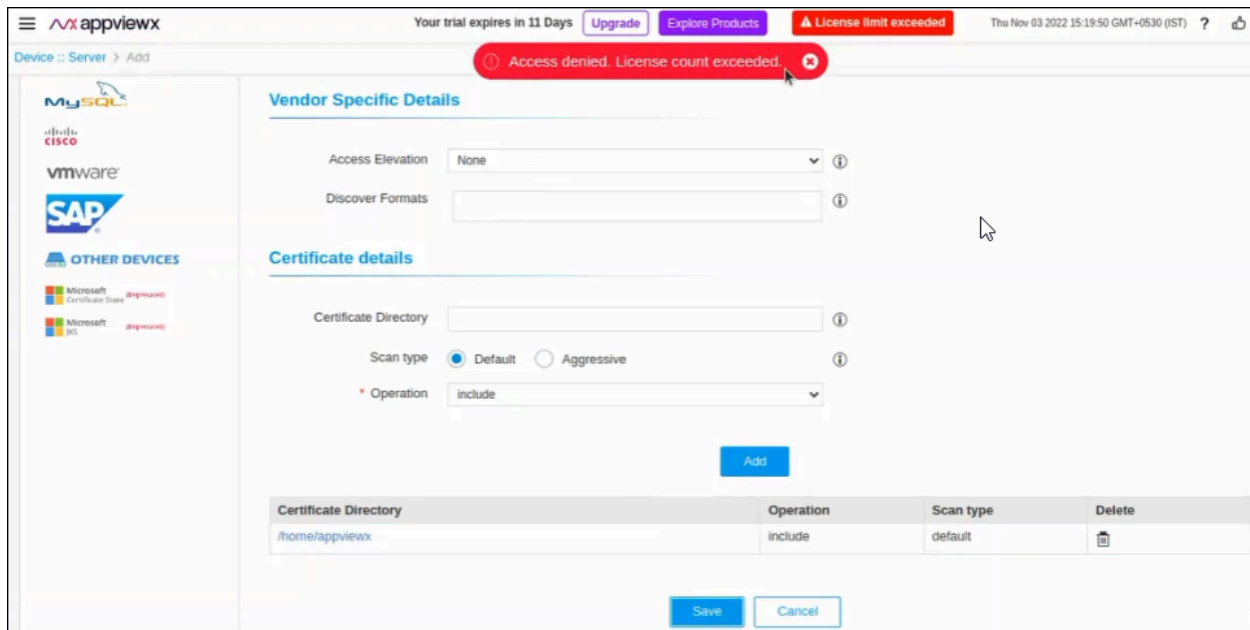
Save

Cancel

- Click the **Delete** icon, if you want to delete the server path from the list.
- The status of the server can be viewed in the Status column.
- You can configure multiple device details for the same vendor.

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.



- A red indicator labeled "**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.

IBM Vendor

As part of the 22.1.0 FP1, for the IBM vendor, the MQClient (Windows) option will be available as one of the **Server types** in the dropdown as shown below:

Device :: Server > Add

Device details

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM**
- DELL
- Linux
- ARBOR
- JBoss
- NT
- RabbitMQ
- MySQL
- CISCO
- vmware
- SAP
- OTHER DEVICES
- Microsoft Certificate Store (deprecated)
- Microsoft JKS (deprecated)

Server details

* Server type MQClient (Windows)

* Server name

Communication mode ☒ Gateway ☐ SSM

* Hostname

Data center absecon

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type Manual entry

* Username

* Password

Windows gateway details

* Gateway type ☒ PowerShell ☐ WMI

* Gateway location ☒ Remote

* Select gateway ☐ New ☒ Existing

* Windows gateway Gateway_108

Certificate details

* Certificate location

Certificate location	Delete
No records found	

ADFS server in Microsoft Server in Device

As a part of FP2 changes, the ADFS server can now be on-boarded into the AppViewX inventory. To onboard the ADFS server,

1. Log in to the AppViewX application with valid credentials.
2. Click the menu icon located in the upper left corner of the screen.

The left navigation pane is displayed.

3. From the menu, click **CERT+**.

4. On the Cert+ page's left menu, in the **Administration** section click **Device Management**.

By default, the ADC tab opens.

5. Click the **Server** tab.

6. Click the **Add (+)** button.

The Device details page is displayed.

7. Select **Microsoft Server** from the Vendors list. The following screen is displayed.

The screenshot shows the 'Device details' page for adding a new server. The 'Vendors' list on the left includes various vendors, with 'Microsoft Server' highlighted. The 'Server details' section shows 'ADFS Server' selected as the server type. The 'Credentials' section shows 'Manual entry' as the credential type. The 'Windows gateway details' section shows 'PowerShell' as the gateway type and 'Remote' as the gateway location. The 'Save' button is highlighted.

Device details

Vendors

- APACHE Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server**
- APACHE Microsoft
- Microsoft SQL
- ORACLE
- IBM
- hp
- DELL
- Linux
- ARBOR
- JBoss
- N
- RabbitMQ
- MySQL
- CISCO
- SAP

Server details

Server type: ☐ Microsoft Server ☒ **ADFS Server**

* Server name:

Data center:

Communication mode: ☒ Gateway ☐ SSM

* Hostname:

Cert sync: ☐ Managed ☒ Monitored ☐ Ignored

Credentials

* Credential type:

* Username:

* Password:

Windows gateway details

* Gateway type: ☒ PowerShell ☐ WMI

* Gateway location: ☒ Remote

* Select gateway: ☐ New ☒ Existing

* Windows gateway:

Save **Cancel**

8. In the **Server Type** radio button, select **ADFS Server**. Enter details as mentioned below.

Field Name	Description
Server Type	Select Server Type as • Microsoft Server - to onboard the Microsoft server to AppViewX • ADFS Server - to onboard the ADFS server to AppViewX
*Server name	Enter the server name.
Data center	Select the data center from the dropdown list.
Communication mode	Select the required communication mode. The possible options are: • Gateway • SSM
Host name	Enter the hostname
Cert sync	Select the required cert sync. The possible options are • <i>Managed</i> - this option is disabled (as push, bind, and rollback are not supported) • <i>Monitored</i> - selected by default (as the discovered certificates will only be in the monitored status) • <i>Ignored</i>

9. In the **Credentials** section, select/enter the details as follows.

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
Password	Select the data center from the dropdown list.

10. In the **Windows gateway details** section, select/enter the details as follows.

Field Name	Description
*Gateway type	Select the required type of gateway. The possible options are: • PowerShell • WMI
*Gateway location	The gateway location is default selected (single option) to Remote.
*Select gateway	Select the required type of gateway. • New • Existing
*Windows gateway	Select the windows gateway from the dropdown list.

11. Click **Save**

The device is onboarded successfully

The ADFS Server device can also be onboarded by the import functionality using the standard .xlsx and .csv templates available.

To onboard the ADFS server into the AppViewX inventory using the import functionality:

1. Log in to the AppViewX application with valid credentials.
2. Click the menu icon located in the upper left corner of the screen. The left navigation pane appears.
3. From the menu, click **CERT+**.
4. On the Cert+ page's left menu, in the **Administration** section click **Device Management**. By default, the ADC tab opens.
5. Click the **Server** tab.
6. Click the **Import** button. The Import details page is displayed.

Device :: Server > Import

Import

Click here to Browse and Upload (csv, xls, and.xlsx)

Uploader Info

Maximum 5 files (.xlsx or .csv) will be processed in parallel

Download sample file here

CSV XLSX

Kindly check if the first row of the import sheet is a title value (For eg. - "Server" in a single cell), if so, delete the first row and import it again or else import will fail. **Only applicable for exported sheets from older AppViewX versions.**

File Histories

Refresh

File name	Status	Server count	Action
 Empty!			

7. Click on the **CSV** or **XLSX** icons in the **Uploader Info** section. The sample templates are downloaded and saved at the default file location.
8. 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.

- 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.

File Histories Refresh			
File name	Status	Server count	Action
Server_Upload_Sample_Sheet (5).xlsx	0% Available: 1 Uploaded: 0 Failed: 0	1	

HPiLO for IBM Vendor

As part of FP2 a new feature of adding a HPiLO server device for the IBM Vendor of Server Type as MQClient(Windows). To onboard the server device,

- Log in to AppViewX application with valid credentials.
- Click the menu button located in the upper left corner of the screen.
- Click **Inventory > Device** OR **CERT+ > Device Management** (under the Administration section of the menu). By default, the ADC tab opens.
- Click the **Server** tab.
- Click the **Add** button.
- Select the **HP** logo from the Vendors list.

Device :: Server > Add

Device details

Vendors














Server details

* Server type ILO

* Server name

* IP address/FQDN

HTTPS Port

Data center

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

Credentials

* Credential type

* Username

* Password

7. In the **Server details** section, select/enter the details as follows (as required).

Server details

* Server type

ILO

* Server name

ilockeek12

* IP address/FQDN

192.168.92.30

HTTPS Port

443

Data center

absecon

Cert sync

☒ Managed
 ☐ Monitored
 ☐ Ignored

8. In the **Credentials** section, select/enter the details as follows:

Credentials

* Credential type

Manual entry

* Username

administrator

* Password

.....

Save

Cancel

9. Click the **Save** button.

Multiple devices can be configured for the same vendor.

Delete Server Details

To delete the server details,

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 **Inventory > Device**.

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

4. Click the **Server** tab.
5. Select a server from server inventory
6. Click the  **Delete** icon in the Command bar.

The **Delete** confirmation pop-up window appears.

7. The server will be removed from the inventory

Manage Server Details

To manage the server details,

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 **Inventory > Device**.

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

4. If the device you want to manage is not listed on the screen, run a search to locate it.
5. Click the **Server tab**.
6. Click the checkbox beside the device name.
7. To start managing the device, click the  **Manage** icon in the command bar at the top of the screen.
8. Click the **Yes** button from the confirmation popup message that appears.
9. Config fetch will be triggered and the server will get managed.
10. The server status is changed to Manage.

Unmanage Server Details

To unmanage the server details,

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 **Inventory > Device**.

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

4. If the device you want to unmanage is not listed on the screen, run a search to locate it.
5. Click the **Server** tab.
6. Click the checkbox beside the device name.
7. Click the  Unmanage icon in the Command bar at the top of the screen.
8. Click the **Yes** button from the confirmation popup message that appears.
9. Server status is changed to UnManaged in Server inventory.

Export Server Details

To export the details of one or more servers,

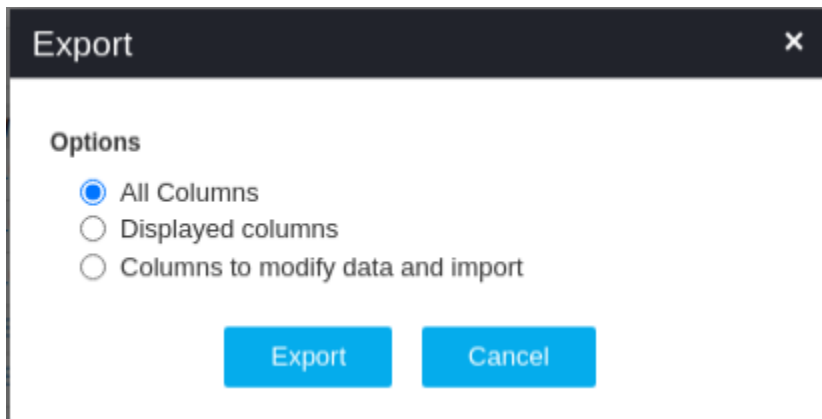
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Click **Inventory > Device**.

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

4. Click the **Server** tab.
5. If the server details you want to export are not listed on the screen, run a search to locate it.
6. Click the checkbox beside the server name. If you are exporting details of multiple servers of the same kind, select the checkboxes for each one.
7. Click the  **Export** icon in the command bar at the upper right of the screen.
8. On the **Export** pop-up screen that appears, select the type of information you want to export:



- 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.
9. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
 10. Cloud details will be downloaded as an Excel <.xls> file.

Import Server Details

To import the server details,

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 **Inventory** > **Device**.

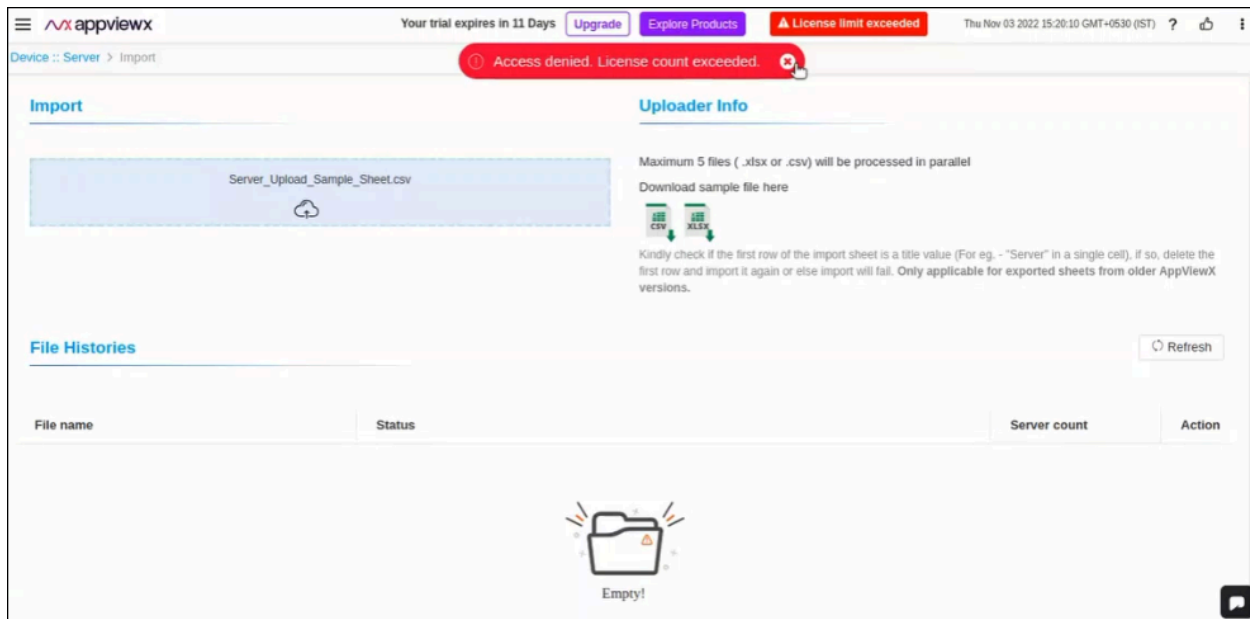
By default, the **ADC** tab opens.

4. Click the **Server** tab.
5. Click the **Import** icon in the command bar.
6. You will be redirected to the import server page.
7. Download the sample <.csv> or <.xls> file.
8. Update the details.
9. Click the browse and upload button.

10. Upload the files.
11. 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**" 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.

Fetch Config for Server

To fetch config for the server,

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 **Inventory > Device**.

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

- Click the **Server** tab.
- If the server is not listed on the screen, run a search to locate it.
- Click the checkbox beside the server name. If you want to fetch configurations for multiple servers of the same type, select their checkboxes, too.
- Click the  **Fetch Config** icon in the command bar.
- A notification appears at the top of the screen stating, "**Fetch config has been triggered for the server.**"
- The configuration will be fetched from the server.

Add Credentials

To add credentials for the server,

- Log in to AppViewX application with valid credentials.
- Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

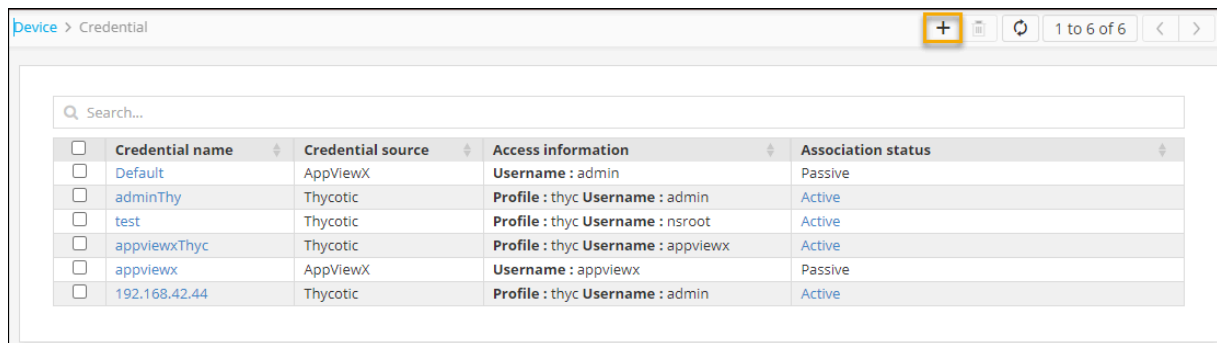
- Click **Inventory > Device**

By default, the ADC tab opens.

- Click the **Server** tab.

- 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.



☐	Credential name	Credential source	Access information	Association status
☐	Default	AppViewX	Username : admin	Passive
☐	adminThy	Thycotic	Profile : thyc Username : admin	Active
☐	test	Thycotic	Profile : thyc Username : nsroot	Active
☐	appviewxThyc	Thycotic	Profile : thyc Username : appviewx	Active
☐	appviewx	AppViewX	Username : appviewx	Passive
☐	192.168.42.44	Thycotic	Profile : thyc Username : admin	Active

- 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.

Device > Credential > Add credential





Credential details

* Credential name

* User name

Credential type ☒ Password ☐ Identity key

* Password

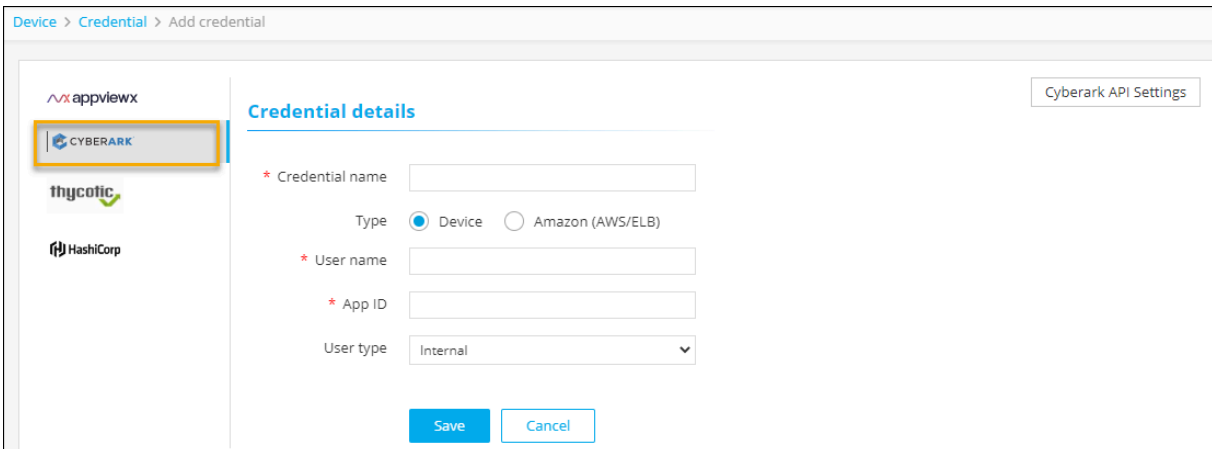
Secondary password

7. To set credentials for **AppViewX**,

Field Name	Field Type	Description
*Credential name	Text	Enter a suitable credential name
*User name	Text	Enter a suitable username
Credential type (Password) • *Password • Secondary password	Radio button • Text • Text and Text fields	Selecting the Password will display the Password and Secondary password text fields. Enter suitable values in both text fields.

Field Name	Field Type	Description
Credential type (Identity key) • *Identity key • Passphrase	Radio button and Text fields	Selecting the Password will display the Identity key field and the Passphrase text field. Select a suitable identity key using the browse button and enter a suitable Passphrase.
 Note: Field names with * (asterisk) are mandatory.		

8. To set credentials for **CyberArk**,



Device > Credential > Add credential

appviewx

CYBERARK

thycotic

HashiCorp

Cyberark API Settings

Credential details

* Credential name

Type ☒ Device ☐ Amazon (AWS/ELB)

* User name

* App ID

User type

Save Cancel

Field Name	Field Type	Description
*Credential name	Text	Enter a suitable credential name
Type (Device) • *User name • *App ID • *User type	Radio button • Text • Text • Dropdown	Selecting the Device will display the User name , App ID , and User Type fields. Enter suitable values in the fields.

Field Name	Field Type	Description
Type (Amazon (AWS/ELB)) • *AWS IAM username • *App ID • *AWS access key ID	Radio button • Text • Text • Text	Selecting the Amazon (AWS/ELB) will display the AWS IAM username , App ID and AWS access key ID text fields. Enter suitable values in the fields.



Note: Field names with * (asterisk) are mandatory.



Note: To configure the API Settings for CyberArk, click the **Cyberark API Settings** button on the right of the screen.

9. To set credentials for **Thycotic**,

Device > Credential > Add credential

Credential details

* Credential name

* API Profile

* Secret type ☒ Device ☐ Amazon (AWS/ELB)

* Username

Thycotic API Settings

Field Name	Field Type	Description
*Credential name	Text	Enter a suitable credential name
*API Profile	Dropdown	Select the desired API profile from the dropdown

Field Name	Field Type	Description
Secret Type (Device) • *User name	Radio button • Text	Selecting Device will display the User name field. Enter suitable value in the field.
Type (Amazon (AWS/ELB)) • *AWS IAM username	Radio button • Text	Selecting Amazon (AWS/ELB) will display the AWS IAM username text field. Enter suitable value in the field.


Note: Field names with * (asterisk) are mandatory.



Note: To configure the API Settings for Thycotic, click the **Thycotic API Settings** button on the right of the screen.

Configuring Firewall

To add a Firewall,

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 **Inventory > Device**.

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

4. Click the **Firewall** tab
5. Click the **Add** button.
6. Enter the *General information, Credentials, Secondary device information* in the device details form.
7. Click the **Add** button
8. You can configure multiple device details for the same vendor.
9. Once the server is added successfully you will redirect to the device server inventory.
10. 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.

- 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.

Delete a Firewall

To delete the firewall from the inventory,

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 **Inventory > Device**.

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

4. Click the **Firewall** tab.
5. Select a firewall from the firewall inventory
6. Click the  **Delete** icon in the Command bar.

The **Delete** confirmation popup window appears.

7. Click **Yes**.
8. The firewall will be removed from the device inventory

Manage Firewall

To manage the firewall,

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 **Inventory > Device**.

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

4. If the device you want to manage is not listed on the screen, run a search to locate it.
5. Click the **Firewall** tab.
6. Click the checkbox beside the firewall name.
7. To start managing the firewall, click the  **Manage** icon in the command bar at the top of the screen.
8. Click the **Yes** button from the confirmation popup message that appears.
9. Config fetch will be triggered and the firewall will get managed.
10. Firewall status is changed to Manage in Firewall inventory.

Unmanage Firewall

To unmanage the firewall,

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 **Inventory > Device**.

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

4. If the device you want to unmanage is not listed on the screen, run a search to locate it.
5. Click the **Firewall** tab.
6. Click the checkbox beside the firewall name.
7. Click the  Unmanage icon in the Command bar at the top of the screen.
8. Click the **Yes** button from the confirmation popup message that appears.
9. Server status is changed to UnManaged in Firewall inventory.

Export Firewall Details

To export the details of one or more firewalls,

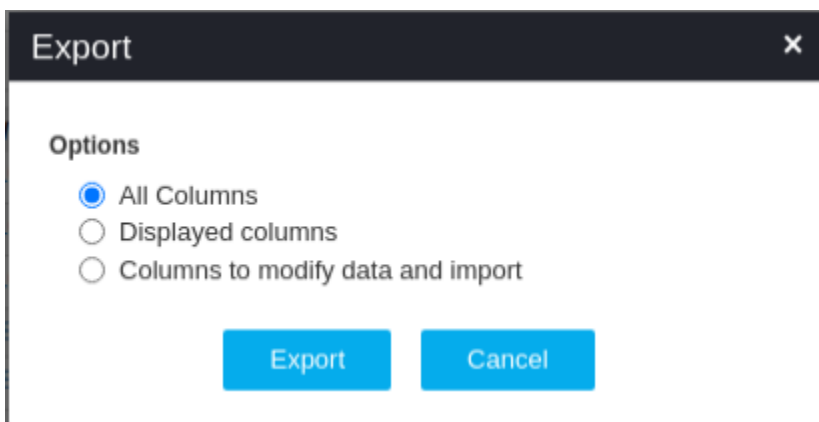
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Click **Inventory > Device**.

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

4. Click the **Firewall** tab.
5. If the firewall details you want to export are not listed on the screen, run a search to locate it.
6. Click the checkbox beside the firewall name. If you are exporting details of multiple firewalls, select the checkboxes for each one.
7. Click the  **Export** icon in the command bar at the upper right of the screen.
8. On the **Export** pop-up screen that appears, select the type of information you want to export:



- 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.
9. On the screen that opens, select the location where you want the firewall details file to go, then click **Save**.
 10. Cloud details will be downloaded as an Excel **<.xls>** file.

Import Firewall Details

To import the firewall details,

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 **Inventory > Device**.

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

4. Click the **Firewall** tab.
5. Click the **Import** icon in the command bar.
6. You will be redirected to the import **firewall** page.
7. Download the sample <.csv> or <.xls> file.
8. Update the details.
9. Click the browse and upload button.
10. Upload the files.
11. Firewall details will be updated to the firewall inventory.

Fetch Config for Firewall

To fetch config for the server,

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 **Inventory > Device**.

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

4. Click the **Firewall** tab.
5. If the firewall is not listed on the screen, run a search to locate it.
6. Click the checkbox beside the firewall name.
7. Click the  **Fetch Config** icon in the command bar.

A popup message appears as **Fetch config has been triggered for the firewall**.

8. The configuration will be fetched from the server.

Configuring Cloud

Add a Cloud details,

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 **Inventory > Device**.

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

4. Click the **Cloud** tab
5. Click the **Add button**.

The **Device details** page appears.

6. Enter the *Basic Information, Key Information, Additional Attributes* in the device details form.
7. Click the **Add** button
8. You can configure multiple device details for the same vendor.
9. Once the Cloud device is added successfully you will redirect to the cloud inventory.
10. 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 a Cloud

To delete a cloud from the inventory,

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 **Inventory > Device**.

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

4. Click the **Cloud** tab
5. Click the **Add button**.

The **Device details** page appears.

6. Select a Cloud from Cloud inventory.
7. Click the  **Delete** icon in the Command bar.

The **Delete** confirmation popup window appears.

8. Click **Yes**.
9. Cloud will be removed from the device inventory

Manage Cloud

To manage cloud in the inventory,

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 **Inventory > Device**.

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

4. Click the **Cloud** tab.
5. Click the **Add button**.

The **Device details** page appears.

6. Select a Cloud from Cloud inventory.
7. Click the **Manage** button
8. To start managing the cloud, click the  **Manage** icon in the command bar at the top of the screen.
9. Click the **Yes** button from the confirmation popup message that appears.
10. Config fetch will be triggered and the firewall will get managed.
11. 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

To unmanage the cloud in the inventory,

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 **Inventory > Device**.

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

4. If the device you want to unmanage is not listed on the screen, run a search to locate it.
5. Click the **Cloud** tab.
6. Click the checkbox beside the cloud name.
7. Click the  Unmanage icon in the Command bar at the top of the screen.
8. Click the **Yes** button from the confirmation popup message that appears.
9. Config fetch will be triggered and the firewall will get managed.
10. Cloud status is changed to **UnManage** in Cloud inventory.

Export Cloud Details

To export the details of one or more firewalls,

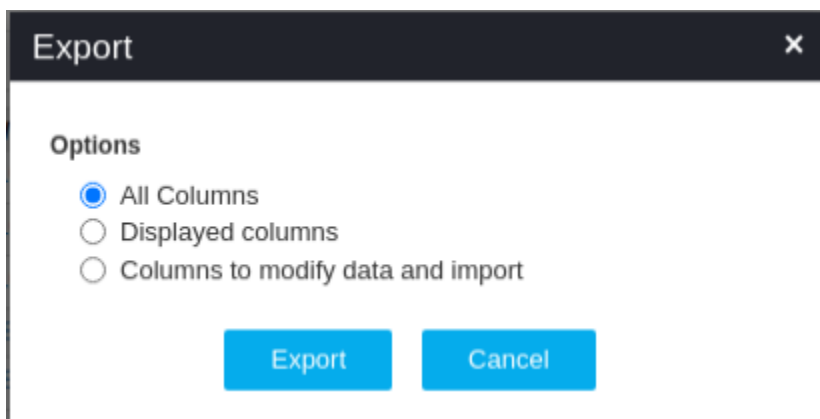
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

3. Click **Inventory > Device**.

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

4. Click the **Cloud** tab.
5. If the cloud details you want to export are not listed on the screen, run a search to locate it.
6. Click the checkbox beside the cloud name.
7. Click the  **Export** icon in the command bar at the upper right of the screen.
8. On the **Export** pop-up screen that appears, select the type of information you want to export:



- 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.
9. On the screen that opens, select the location where you want the cloud details file to go, then click **Save**.
10. Cloud details will be downloaded as an Excel <.xls> file.

Import Cloud Details

To import the cloud details,

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 **Inventory > Device**.

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

4. Click the Cloud tab.
5. Click the **Import** icon in the command bar.
6. You will be redirected to the import cloud page.
7. Download the sample <.csv> or <.xls> file.
8. Update the details.
9. Click the browse and upload button.
10. Upload the files.
11. Cloud details will be updated to the cloud inventory.

Fetch Config for Cloud

To fetch config for the cloud,

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 **Inventory > Device**.

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

4. Click the **Cloud** tab.
5. If the cloud is not listed on the screen, run a search to locate it.
6. Click the checkbox beside the cloud name.
7. Click the  **Fetch Config** icon in the command bar.

A popup message appears as **Fetch config has been triggered for the cloud**.

8. The configuration will be fetched from the Cloud.

Certificate Reports

- [Overview](#)
- [Job Scheduler](#)
- [Types of Scheduled Jobs](#)
- [Device and Certificate Synchronization](#)
- [CRL Certificate Revocation Check](#)
- [Configuring Report Settings and Schedule](#)
- [Report Routing](#)
- [Validation Settings](#)
- [Revocation Check Routing](#)
- [Configure Certificate Authority](#)
- [Securing CERT+](#)

Overview

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.

Before you Begin

Following are the prerequisites for configuring certificate Reports in AppViewX:

- 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](#)

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 appears.

3. Click **Settings**.

The **Settings** page appears.

4. Expand the General menu and then click **SMTP**.

The screenshot shows the AppViewX application interface. On the left, a sidebar menu is visible with 'SMTP' highlighted. The main area is titled 'SMTP configuration' and contains the following fields:

- SMTP host: localhost
- SMTP port: 25
- From address: support@appviewx.com
- Enable SSL: ☐
- Email box: ☐

Below the configuration fields is the 'Authentication' section with the following options:

- Authentication required: ☐
- Username:
- Password:

At the bottom is the 'Test email' section with a 'Send email to' field:

5. Refer to the fields in the table below to update the information on the SMTP page.

Name	Type	Mandatory	Description	Error Message
* SMTP host	Text	Yes	The server that will send the email.	Enter valid Hostname/ IP address <x.x.x.x>.
* SMTP port	Text	Yes	Port to connect to the email server.	• Port can contain only numbers. • Enter a port number between 0-65535.
* From address	Text	Yes	Mail address from which mail is to be received by the user.	• Please enter a valid email.
Enable SSL	Toggle button	No	To enable/disable SSL while sending mail.	NA
Email box	Toggle button	No	Enabling this setting will use IMAP for the mailbox.	NA
* Email	Text	Mandatory if Email box is enabled.	Email for IMAP.	• Please enter a valid email.
Password	Text	Mandatory if Email box is enabled.	Password for IMAP.	This field is mandatory.
* Hostname	Text	Mandatory if Email box is enabled.	The hostname for IMAP.	• Enter valid Hostname/ IP address <x.x.x.x>.
Authentication required	Toggle button	No	To enable/disable Authentication required.	NA

Name	Type	Mandatory	Description	Error Message
* Username	Text	Mandatory if Authentication required is selected as true.	The username if authentication required.	NA
* Password	Text	Mandatory if Authentication required is selected as true.	Password if authentication required.	NA
* Send email to	Text	Mandatory if you want to test.	Test email to check if able to send mail after configuring the above settings.	• Enter a valid email.
 Note: The asterisk (*) symbol indicates a mandatory field.				

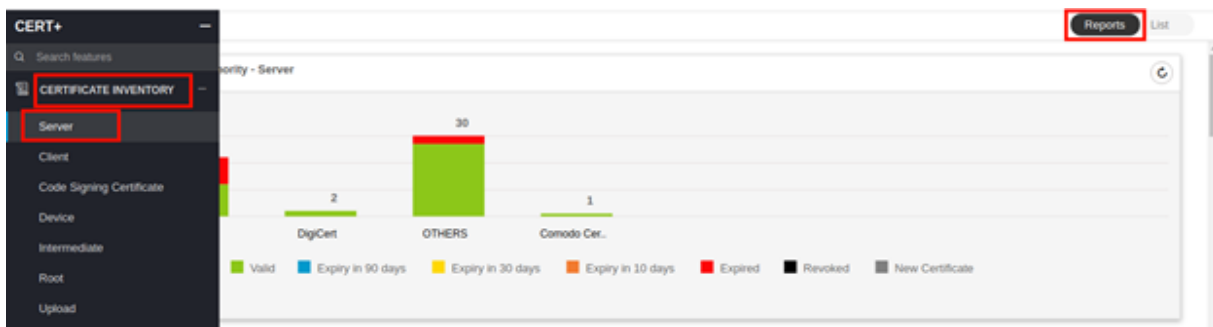
Troubleshooting SMTP

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. 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 **CERTIFICATE INVENTORY**.
5. Select the required submenu such as Server, Client, Code Signing Certificate, Device, and so on to view the corresponding reports.
6. In the top right corner, click **Reports** tab.
The respective report page appears.



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.

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.

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.

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 supports 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.

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. 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 **ADMINISTRATION** and then click more.
5. Click **Expired Certificates**.

The **Expired Certificates** page appears.

6. Enable Yes to delete the expired certificates.

CERT+

Search features

GROUPS & POLICIES

ADMINISTRATION

- Password Vault
- Auto Enrollment
- Certificate Authority
- Device Management
- Application
- Certificate Profile
- Programmable
- Job Scheduler
- Certificate Attributes
- Email Settings
- Expired Certificates**
- History of Certificates
- General Settings

Expired Certificates

Do you want to delete the expired certificate after its expiry? ☒ Yes ☐ No

* Number of days after expiry

Save **Reset**



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.

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.

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

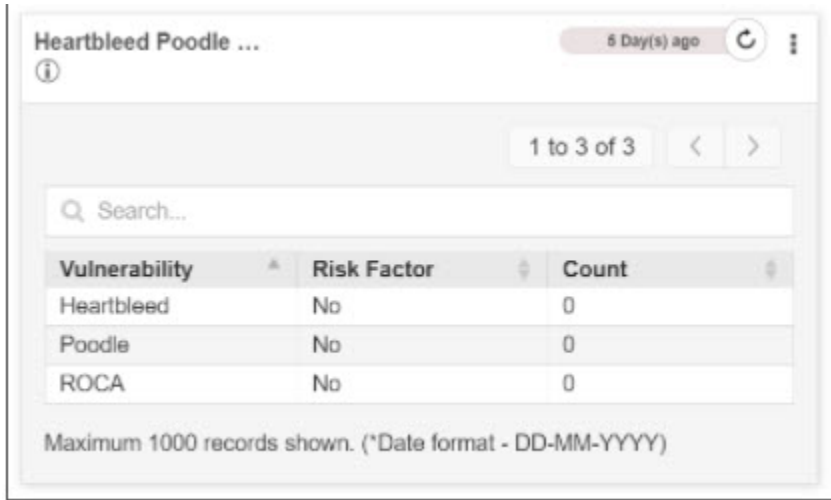
- The cron job is executed to check the certificates and their device association
- There is internal business logic to check the Poodle, Heart bleed, and Roca vulnerabilities for the associated device.
- Once the job is completed the “Vulnerability reports” are updated in “Server_Endpoint_Security”, “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.



Heartbleed Poodle ... 5 Day(s) ago

1 to 3 of 3

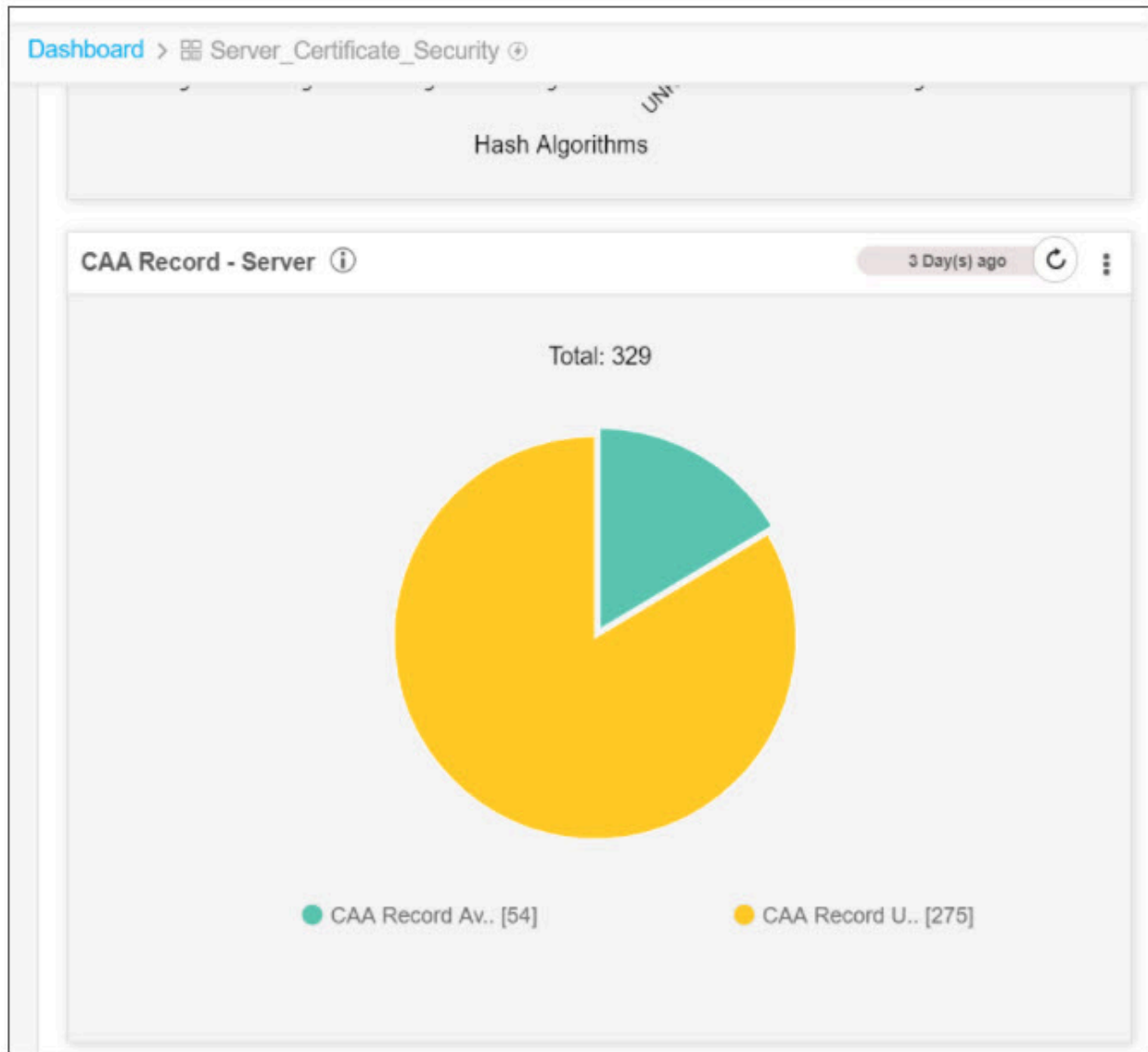
Search...

Vulnerability	Risk Factor	Count
Heartbleed	No	0
Poodle	No	0
ROCA	No	0

Maximum 1000 records shown. (*Date format - DD-MM-YYYY)

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.



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

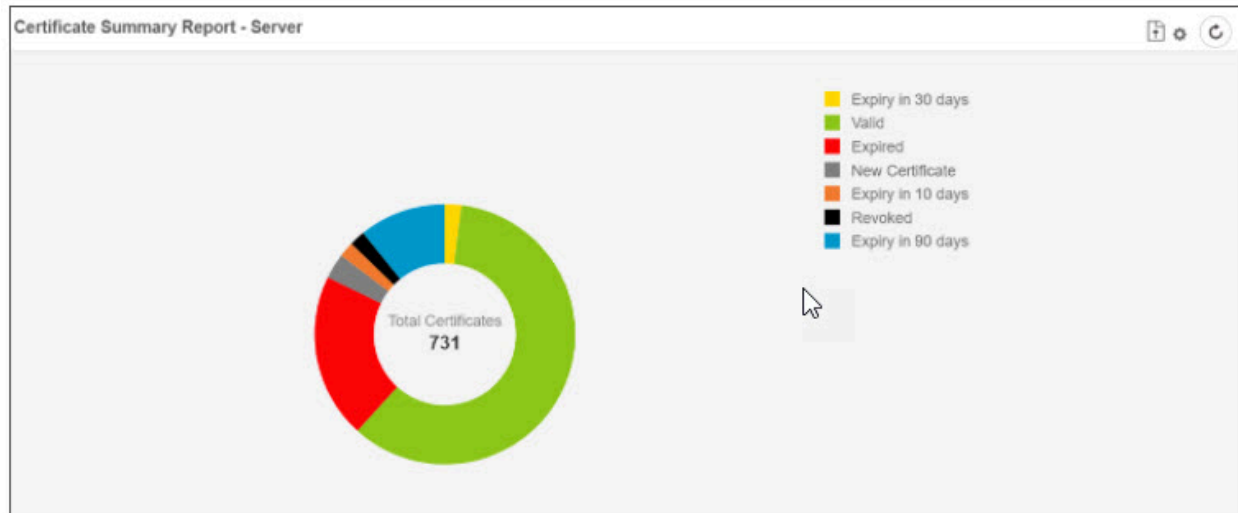
The scheduled job is monitored and triggered by default weekly, on Sunday.

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.

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

Configuring Report Settings and Schedule

The running time of the reports to collect the data can be configured per the organization level using Job Scheduler.

To configure the Job Scheduler,

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 **ADMINISTRATION** and then click **more**.5. Click **Job Scheduler**.

The **Job Scheduler** home page appears.



6. The following table describes the options available on the Job Scheduler home page:

Options	Description
Search Bar	Allows you to search for a job scheduler in the application. Searches for the given keyword in the field and results in the feature that matches the search keyword.
Task Bar	Displays the number of actions available on the page.
Page Count Button	Shows the number of pages available in the job scheduler. Note: Maximum allowed pages are 16.
Previous Page Button	Allows moving to the previous page on the screen.
Next Page Button	Allows moving to the next page on the screen.
Refresh Button	Allows refreshing the job scheduler home page.

7. Click on the desired task name in the list to modify the configuration of the job running time.

Device and Certificate synchronization

* Description

Check Synchronization of devices and its certificates

* Time Zone

UTC (UTC+00:00)

* Occurrence Type

Daily

* Starts On

05/14/2021 16:05:05

Repeat

1

Times

Summary

Daily, 1 Times

Update

Cancel

The following table describes the options available on the task page:

Options	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

Options	Description
	• Monthly • Yearly.
* Start On	Set the start date and time.
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.

8. After configuring the details, click **Update**.

Report Routing

This functionality is applicable only to the following reports:

- Validation report
- Vulnerability report
- CAA report

1. Click the **Menu** () icon.
2. Click **CERT+**.
The CERT+ left navigation pane appears.
3. Click **Administration > Report Settings > Routing**.
The **Report Routing** page is displayed.

4. Enter the following fields:

Field	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: Fields marked with red asterisk (*) symbol are mandatory.

5. Click **Add**.

The table is refreshed with a row entry of the newly added URL and the data center.

6. Click **Save**.

A message that certificate report settings routing is saved successfully appears.

On saving, any report validation such as validation checks or CAA record check is routed through the data center configured on this page.



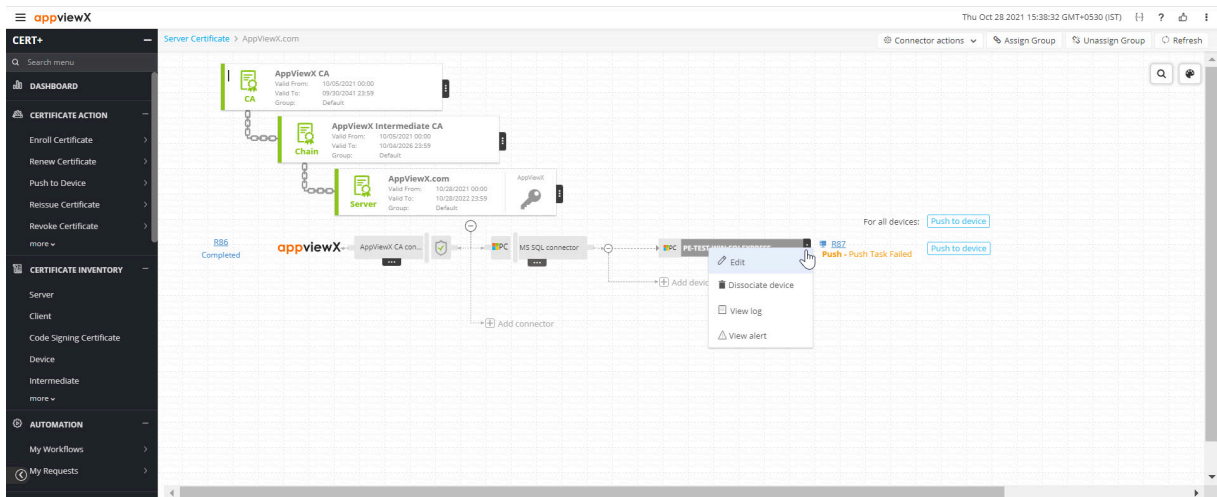
Note: To perform a bulk operation on certificate URLs, you can specify a wildcard character with their domain name, for example, if you want to specify a data center to all the AppViewX certificates at one go, then use wildcard character as in *.appviewx.com and select the data center from the dropdown list.

7. Click **Add**.
8. If you want to edit the certificates, then use the **Edit** option.

Validation Settings

This is an extended feature of Report Routing.

1. From the **Certificate Inventory**, click the **Common Name** link to view the certificate in the holistic view.
2. Hover the mouse over the **More** (⋮) icon of the application connector and click **Edit**.



The **Edit Application Connector** page is displayed.

edit Application Connector

Certificate Details

Certificate Type

PEM (PKCS12)

Registry Restart

☒

Push Root and Intermediate Certificates

☐

Private Key in Device

☐

Push Details

Script Location

☒ In App/Inbox

Pre - Push script

Post - Push script

Push automatically

☒

Validation Settings

☐ Default ☒ Custom ☐ None

IP	Port	Data Center
ip	Port	Data Center atobcon

Add

Save

Cancel

3. Select **Custom** option.
4. 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:

- Revocation check job
- On demand revocation check

1. Click the **Menu** () icon.
2. Click **CERT+**.
The CERT+ left navigation pane appears.
3. Click **Administration > Revocation Check > Routing**.
The **Revocation Routing** page is displayed.

4. Enter the following fields:

Field	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 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 appears on the Certificate Inventory page with a black icon against it.

Field	Description
	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: Fields marked with red asterisk (*) symbol are mandatory.	

5. Click **Add**.

The table is refreshed with the added URL and the data center.

6. Click **Save**.

A message that certificate revocation check routing is saved successfully appears.

The table is refreshed with a row entry of the newly added URL and the data center.

Configure Certificate Authority

To configure a certificate authority:

1. Click the **Menu** () icon.
2. Click **CERT+**.
The **CERT+** left navigation pane appears.
3. Click **Certificate Authority** from **Administration** on the LHS pane.
4. Click a CA from the list of CA vendors.

The screenshot shows the AppViewX CERT+ interface. On the left, a sidebar contains a search bar and a list of features: DASHBOARD, CERTIFICATE ACTION, CERTIFICATE INVENTORY, AUTOMATION, CERTIFICATE DISCOVERY, ALERTS & LOGS, GROUPS & POLICIES, ADMINISTRATION (highlighted), Password Vault, Auto Enrollment, Certificate Authority (highlighted), Device Management, Application, and more. The main content area is titled 'Certificate Authority' and features a '+ Add' button. Below this is a table with the following data:

Name	Purpose/Usage	Connection Status
gca	Server,Client	Failed

Additional buttons like 'Check' and a trash icon are visible next to the 'Failed' status.

- Click **+ Add** on the top-right of the page.
The CA configuration page appears.

< Google

General Information

* Name

* Purpose/Usage None Selected ⓘ

Proxy Required ☐

Data Center (AppViewX's CA agent) e1a ▼

CA Configuration

* Configure With ☒ Certificate Upload ☐ JSON Upload

* Certificate and Key filename.pkcs Upload

* Email Address

* Project Id

Save

Cancel

6. Update the following details in the **General Information** section as described in the table:

Field	Description
Name	A unique name to identify the CA setting. Note: No special characters other than period (.), hyphen (-), and en dash (_) are allowed. The name should not start with special characters.
Purpose/Usage	Certificate Type for which CLM actions are enabled. Options are Server, Client, and Code Signing.
Proxy Required	Certificate Type for which CLM actions are enabled. Options are Server, Client, and Code Signing.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen. Note: This feature is implemented only for EJBCA, OpenTrust, and Entrust certificate authorities.

7. Update the following details in the **CA Configuration** section as described in the table.

Field	Description
Configure With	Configure it as Certificate Upload or JSON Upload . These fields are necessary for invoking the Google CA APIs via Certificate Upload for Certificate Management. If you select the JSON Upload check box, click the Upload button to upload the JSON file.
Certificate and Key	Client authentication certificate for API communication.
Email address	Email address of the user.
Project Id	Id of the project.

8. Click **Validate and Fetch**.

The issuer names available for the CA account are fetched along with the validity of the issuers from the Certificate Authority.

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.

Auto Enrollment Protocols

- [Overview](#)
- [ACME](#)
- [EST](#)
- [Microsoft Intune](#)
- [SCEP](#)

Overview

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

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 **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](#)

Configuring ACME

To perform client certificate enrollments using ACME protocol, the admin or a privileged user needs to first set up the ACME server agent using the AppViewX portal. Upon successful set up of the ACME server Agent through the portal, a URL will be generated. Clients can then use this URL to send enrollment requests to AppViewX via ACME protocol.

The detailed steps for setting up the ACME server agent are listed below:

1. Log in to AppViewX application with admin or privileged user credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **CERT+ > ADMINISTRATION > Auto Enrollment > ACME**.
4. Select **Add** or **Configure Now**.
5. 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 following table provides the field description for adding the Agent Details:

Field Name	Field Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the agent setting.	No special characters other than '.', '-', '_' are allowed. Name should not start with special characters.
IP/FQDN	Text	Yes	Enter the FQDN/ IP address of the appviewx cloud connector.	Invalid FQDN/IP address(example: xxx.xxx.xxx.xxx)
Port	Text	Yes	HTTP gateway port of the AppViewX node.	Port will accept only numerical values between 0 to 65535.
Challenge Type	Dropdown	Yes	Select the one of the following challenge type: • DNS • HTTP	NA

Endpoint Details

* Name

* IP/FQDN

Eg - 192.168.1.1

* Port

30020

* Challenge Type

DNS

6. Configure the **CA Accounts** details as follows:

CA Accounts

*

Certificate Group

Default

▼

ⓘ

*

Certificate Category

☒ Server
 ☐ Client

*

Select CA

AppViewX

▼

ⓘ

The following table provides the field description for CA Accounts section:

Field Name	Field Type	Mandatory	Description	Validation
Certificate Group	Dropdown	Yes	Select a specific group under which certificate needs to be enrolled.	NA
Certificate Category	Radio button	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Dropdown	Yes	Select the required CA from the available options: • AppViewX • Google • DigiCert • Ejbca • Microsoft Standalone • AppViewX PKIaaS • Microsoft Enterprise • Amazon Private CA • DigiCert MPKI • Entrust MPKI • Comodo Certificate Manager • Entrust • Nexus • Globalsecure • Globalsecure MSSL	NA

Field Name	Field Type	Mandatory	Description	Validation
			The certificate will be enrolled under the selected CA.  Note: The Vendor Specific Details section is displayed after the CA Accounts section only if DigiCert, Entrust MPKIEjbca, Entrust, or MS Enterprise is selected as the CA.	

The following fields are displayed as per the selected **CA**:

- When **AppViewX** is selected as CA,

* Select CA

AppViewX

▼

ⓘ

* CA Account

AppviewCA

▼

ⓘ

* CA Connector Name

CA Connector

ⓘ

* Certificate Validity

365

days

ⓘ

The following table provides the field description for AppViewX CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Google** is selected as CA,

* Select CA

Google

▼

i

* CA Account

GCA

▼

i

* Issuer Location

asia-south1

▼

i

* Pool name

OCSPPool

▼

i

* CA Connector Name

CA Connector

i

* Certificate Validity

365

days

i

The following table provides the field description for Google CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Issuer Location	Dropdown	Yes	Select the issuer location associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **DigiCert** is selected as CA,

* CA Account

digicert

* Division

AppViewX Inc.

* Cert Type

SSL Plus

* CA Connector Name

CA Connector

* Certificate Validity

1

Days

The following table provides the field description for DigiCert CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account	NA

Field Name	Field Type	Mandatory	Description	Validation
			associated with the selected CA to be used for certificate creation operations.	
Division	Dropdown	Yes	Select the division associated with the CA account.	NA
Cert Type	Dropdown	Yes	Select certificate type to issue the certificate.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.

Vendor specific details

* Server Type

Apache

* Payment Method

Bill To Account Balance

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
Server Type	Dropdown	Yes	Select a server type.	NA

Field Name	Field Type	Mandatory	Description	Validation
Payment Method	Dropdown	Yes	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.	Alphanumeric characters, spaces, and the special characters <code>-_.*</code> are allowed.

- When **Ejbca** is selected as CA,

* CA Account	ejbca	
* CA Connector Name	CA Connector	
* Certificate Validity	365 days	

The following table provides the field description for Ejbca CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Ejbca**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* End Entity Profile Name

APPVIEWS PROFILE

End entity user name

* Issuer Common Name

AVX EJBCA ENTERPRISE CA

* Certificate Profile Name

AVX EJBCA ENTERPRISE PROFILE

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
End Entity Profile Name	Dropdown	Yes	Select a profile of an end entity.	NA

Field Name	Field Type	Mandatory	Description	Validation
End entity user name	Text	No	Enter the user name for the end entity.	Alphanumeric characters, spaces, and the special characters - _ . * are allowed.
Issuer Common Name	Dropdown	Yes	Select a common name of an issuer.	NA
Certificate Profile Name	Dropdown	Yes	Select a profile name of certificate.	NA

- When **Microsoft Standalone** is selected as CA,

* Select CA

Microsoft Standalone

▼

i

* CA Account

MS standalone

▼

i

* CA Connector Name

CA Connector

i

* Certificate Validity

365

days

i

The following table provides the field description for Microsoft Standalone CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
CA Connector Name	Text	Yes	Name of the CA connector after	No special characters are allowed. Only

Field Name	Field Type	Mandatory	Description	Validation
			the certificate is enrolled.	alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **AppViewX PKIaaS** is selected as CA,

* CA Account	serc-certuser1	▼	i
* Issuer Location	asia-south1	▼	i
* Pool Name	OCSPPool	▼	i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for AppViewX PKIaaS CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Issuer Location	Dropdown	Yes	Select an issuer location that is associated with the CA account.	NA

Field Name	Field Type	Mandatory	Description	Validation
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
Issuer Name	Dropdown	Yes	Select an issuer name to issue the certificate.	NA
CA Certificate	Dropdown	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Microsoft Enterprise** is selected as CA,

* CA Account

MS Enterprise

▼

i

* CA Connector Name

CA Connector

i

* Certificate Validity

365

days

i

The following table provides the field description for Microsoft Enterprise CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Microsoft Enterprise**, a separate section displaying **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* Template Name

Administrator

▼

i

Select a template from the dropdown list.

- When **Amazon Private CA** is selected as CA,

* Select CA	Amazon Private CA	▼	i
* CA Account	Amazon CA	▼	i
* Region	us-east-1	▼	
* Issuer	AppViewX-AWS-SubCA	▼	
* Signature Algorithm	SHA384WITHECDSA	▼	
* CA Connector Name	CA Connector		i
* Certificate Validity	1	▼	Days ▼

* Validity	1	▼	Year ▼
			Year

The following table provides the field description for Amazon Private CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Region	Dropdown	Yes	Select a region from the dropdown list.	NA

Field Name	Field Type	Mandatory	Description	Validation
Issuer	Dropdown	Yes	Select the issuer from the dropdown list.	NA
Signature Algorithm	Dropdown	Yes	Select the SignAlgorithm from the dropdown list. The available options are: • SHA256WITHECDSA • SHA384WITHECDSA • SHA512WITHECDSA • SHA256WITHRSA • SHA384WITHRSA • SHA512WITHRSA	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **DigiCert MPKI** is selected as CA,

* Select CA	DigiCert MPKI	▼	i
* CA Account	DigiCertMпкиCA	▼	i
* Profiles	test_server	▼	
* CA Connector Name	CA Connector		i

The following table provides the field description for DigiCert MPKI CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Profiles	Dropdown	Yes	Select a profile from the dropdown option.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.

- When **Entrust MPKI** is selected as CA,

* Select CA	Entrust MPKI	▼	ⓘ
* CA Account	EntrustMпкиCA	▼	ⓘ
* CA Connector Name	CA Connector		ⓘ
* Certificate Validity	365	days	ⓘ

The following table provides the field description for Entrust MPKI CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Entrust MPKI**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.

Vendor specific details

* CA Name	SEDemo ECS Public SSL AppViewX	▼
* Cert Profiles	advantage profile	▼

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
CA Name	Dropdown	Yes	Select a CA name from the dropdown list.	NA
Cert Profiles	Dropdown	Yes	Select a cert profile from the dropdown list.	NA

- When **Comodo Certificate Manager** is selected as CA,

* Select CA

Entrust MPKI

▼

ⓘ

* CA Account

EntrustMпкиCA

▼

ⓘ

* CA Certificate

ⓘ

* CA Connector Name

CA Connector

ⓘ

* Certificate Validity

365

days

ⓘ

The following table provides the field description for Comodo Certificate Manager CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Cert Type	Dropdown	Yes	Select certificate type to issue the certificate.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Entrust** is selected as CA,

Auto-Enrollment : ACME

CA Accounts

* Certificate Group ⓘ

* Certificate Category ☒ Server ☐ Client

* Select CA ⓘ

* CA Account ⓘ

* Certificate Type

* CA Connector Name ⓘ

* Certificate Validity

The following table provides the field description for Comodo Certificate Manager CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account. If the Certificate Category radiobutton is selected to <i>Server</i>, the dropdown is populated with the first available value. Select an appropriate value as required. If the Certificate Category radiobutton is selected to <i>Client</i>, the dropdown is populated with 'None' as the default value.	NA
CA Connector Name	Text	Yes	Name of the CA connector after	No special characters are

Field Name	Field Type	Mandatory	Description	Validation
			the certificate is enrolled.	allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled (in days/ months/years).	Certificate validity accepts only numerical values.

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Vendor specific details

Additional Emails

Custom Attributes

Demo

Certificate type

Tracking Id



Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed as shown above.

Field Name	Field Type	Mandatory	Description	Validation
Additional Emails	Text	No	Enter the valid email address in the field.	NA
Demo	Text	No	Enter the demo details	NA
Certificate type	Text	No	Enter a valid certificate type	NA
Tracking id	Text	No	Enter the tracking id	NA

- When **GlobalSign MSSL** is selected as CA.

Auto-Enrollment : ACME

CA Accounts

* Certificate Group

Default

* Certificate Category

☒ Server
☐ Client

* Select CA

Nexus

* CA Account

Nexus

* CA Connector Name

CA Connector

* Certificate Validity

1

Days

The following table provides the field description for **GlobalSign MSSL**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Certificate Type	Dropdown	Yes	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.	NA
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Profile name

Field Name	Field Type	Mandatory	Description	Validation
Profile	Dropdown	Yes	Select the Profile based on the configurations made in the Certificate Authority Setting.	NA

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

Point of Contact

CA mandates Point of Contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the Point of Contact information entered here.

* First Name

* Email Address

* Phone Number

here.

Field Name	Field Type	Mandatory	Description	Validation
First Name	Text	Yes	Enter the first name.	NA
Email Address	Text	Yes	Enter the valid email address.	NA
Phone Number	Text	Yes	Enter the valid phone number.	NA

- When **GlobalSign** is selected as CA

Auto-Enrollment : ACME

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
GlobalSign

* CA Account
Global Sign

* Certificate Type
Alpha SSL

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **GlobalSign CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Certificate Type	Dropdown	Yes	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.	NA
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

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 = Server**

Vendor specific details

* Domain Admin Email

@domain

Field Name	Field Type	Mandatory	Description	Validation
Domain Admin Email	Dropdown	Yes	Select the email id to receive the approval requests from GlobalSign CA.	NA

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

CA mandates Point of Contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the Point of Contact information entered here.

* First Name

Field Name	Field Type	Mandatory	Description	Validation
First Name	Text	Yes	Enter the first name	NA

- When **Nexus** is selected as CA.

Auto-Enrollment : ACME

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
Nexus

* CA Account
Nexus

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **Nexus CA**

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Dropdown	Yes	Type 3 or more letters of the certificate keywords and select one issuer certificate from the dropdown. 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.	NA
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Procedure

AppViewX SCEP

Field Name	Field Type	Mandatory	Description	Validation
Procedure	Dropdown	Yes	Select the Procedure based on the configurations made in the Certificate Authority Setting.	NA

7. Configure the **Advanced Settings** details as follows:

Advanced Settings

* Fetch Certificate Parameters
☐ Yes
☒ No

The following table provides the field description for the Advanced Settings section:

Field Name	Field Type	Mandatory	Description	Validation
*Fetch Certificate Parameters	Radio button	Yes	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.	NA

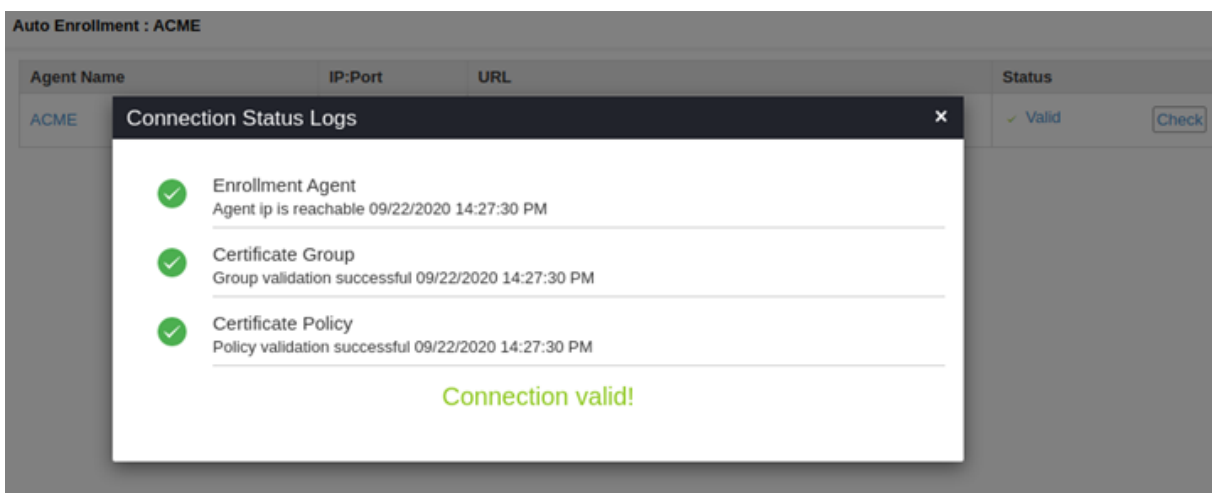
8. Click **Save**.

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. Click the **Menu** button.
2. Navigate to **CERT+ > ADMINISTRATION**.
3. Under the **Administration** section, click **Auto-Enrollment** and then select **ACME**.
4. On the **ACME** page, click **Check** 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.

- 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 OFF the 'Approval Required' flag in **Menu -> Inventory -> Certificate -> Policy** page.
- A valid agent settings should be available in **Menu -> Inventory -> Certificate -> Settings**.

- [Configuring EST](#)

- [Validating EST](#)

Configuring EST

To perform client certificate enrollments using EST protocol, the admin or a privileged user needs to first set up the EST server agent using the AppViewX portal. Upon successful set up of the EST server Agent through the portal, a URL will be generated. Clients can then use this URL to send enrollment requests to AppViewX via EST protocol.

The detailed steps for setting up the EST server agent are listed below:

1. Log in to AppViewX application with admin or privileged user credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **CERT+ > ADMINISTRATION > Auto Enrollment > EST**.
4. Select **Add** or **Configure Now**.
5. 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.

Endpoint Details

* Name

* IP/FQDN

?

* Port

?

The following table provides the field description for Agent Details section:

Field Name	Field Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the Agent setting.	No special characters other than '.', '-', '_' are allowed. Name should not start with special characters.
FQDN/IP	Text	Yes	Enter the FQDN/IP address of the appviewx cloud connector.	Invalid FQDN/IP address(example: xxx.xxx.xxx.xxx)
Port	Text	Yes	HTTP gateway port of the AppViewX node.	Port will accept only numerical values between 0 to 65535.

6. Configure the **Client Authentication** details as follows:

Client Authentication

Authentication Mode

Only Certificate TLS

?

* Issuer Certificate

✗ CN = AppViewX Intermediate CA, SN = 55:CC:CA:AA:D4:84:E6:99:E0:E2:17:9C:AE:A1:B6:56, Category = Intermediate CA

?

Only Client Certificate Authentication Mode

Client Authentication

Authentication Mode: Certificate TLS with HTTP as Fallback ⓘ

* Issuer Certificate: X CN = AppViewX Intermediate CA, SN = 55:CC:CA:AA:D4:84:E6:99:E0:E2:17:9C:AE:A1:B6:56, Category = Intermediate CA ⓘ

* HTTP Authentication Mode: ☒ Basic ☐ Digest ⓘ

* Username: admin

* Password: *****

Client Certificate Authentication with HTTP Fallback Mode

Client Authentication

Authentication Mode: Both Certificate TLS and HTTP ⓘ

* Issuer Certificate: X CN = AppViewX Intermediate CA, SN = 55:CC:CA:AA:D4:84:E6:99:E0:E2:17:9C:AE:A1:B6:56, Category = Intermediate CA ⓘ

* HTTP Authentication Mode: ☒ Basic ☐ Digest ⓘ

* Username: admin

* Password: *****

Both Client certificate and HTTP Authentication Mode

The following table provides the field description for CA Authentication section:

Field Name	Field Type	Mandatory	Description	Validation
Authentication Mode	Dropdown	Yes	Select any one authentication method to be carried out during communication with clients.	NA
Issuer Certificate	Dropdown	Yes	Select one or more issuer certificates which needs to be checked for the client certificate authentication.	NA
HTTP Authentication Mode	Radio button	Yes	Select the type of HTTP auth mode either Basic/Digest.	NA
Username	Text	Yes	Username for HTTP authentication.	NA
Password	Text	Yes	Password for HTTP authentication.	NA

7. Configure the **CA Accounts** details as follows:

The following table provides the field description for CA Accounts section:

Field Name	Field Type	Mandatory	Description	Validation
Certificate Group	Dropdown	Yes	Select a specific group under which certificate needs to be enrolled.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Category	Radio button	Yes	Select a specific certificate type (Server/ Client) to be enrolled.	NA
Select CA	Dropdown	Yes	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 • Google • Ejbca • Microsoft Standalone • AppViewX PKIaaS • Microsoft Enterprise • Entrust MPKI • Entrust • DigiCert MPKI • DigiCert • Amazon Private CA • Nexus • GlobalSign MSSL	NA

Field Name	Field Type	Mandatory	Description	Validation
			 Note: The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs.	

The following fields are displayed as per the selected CA:

- When **AppViewX** is selected as CA,

* Select CA	AppViewX	▼	ⓘ
* CA Account	AppViewX CA	▼	ⓘ
* Server Certificate	No server certificates found		ⓘ
* CA Connector Name	CA Connector		ⓘ
* Certificate Validity	365	days	ⓘ

The following table provides the field description for AppViewX CA:

Field Name	Field Type	Mandatory	Description	Validation
				NA
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Server Certificate	Select	Yes	Type 3 or more letters of the	NA

Field Name	Field Type	Mandatory	Description	Validation
			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.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values

- When **Google** is selected as CA.

* Select CA	Google	▼	i
* CA Account	serc-certuser1-Google_Server_Client_CreateC	▼	i
* Issuer Location	us-east1	▼	i
* Pool Name	EntCApool1	▼	i
* Issuer Name	EntCA1fromPool1	▼	i
* CA Certificate			i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for **Google** CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Issuer Location	Dropdown	Yes	Select an issuer location that is associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA

Field Name	Field Type	Mandatory	Description	Validation
Issuer Name	Dropdown	Yes	Select an issuer name to issue the certificate.	NA
CA Certificate	Dropdown	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Ejbca** is selected as CA.

* Select CA	Ejbca	▼	i
* CA Account	ejbca	▼	i
* CA Certificate	CN = , SN = 11:A9:2D:AB:78:BB:AD:C1:21:6B:5D		i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for Ejbca CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Dropdown	Yes	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	NA

Field Name	Field Type	Mandatory	Description	Validation
			with EST client machine.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Ejbca**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* End Entity Profile Name

APPCVIEWX PROFILE

End entity user name

* Issuer Common Name

AVX EJBCA ENTERPRISE CA

* Certificate Profile Name

AVX EJBCA ENTERPRISE PROFILE

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
End Entity Profile Name	Dropdown	Yes	Select a profile of an end entity.	NA
End entity user name	Text	No	Enter the user name for the end entity.	Alphanumeric characters, spaces, and the special characters <code>-_.*</code> are allowed.

Field Name	Field Type	Mandatory	Description	Validation
Issuer Common Name	Dropdown	Yes	Select a common name of an issuer.	NA
Certificate Profile Name	Dropdown	Yes	Select a profile name of certificate.	NA

- When **Microsoft Standalone** is selected as CA.

* Select CA

Microsoft Standalone

▼

i

* CA Account

MS standalone

▼

i

* CA Certificate

CN = avxdevlab-AVXDEVSRV01-CA-SHA512, ST

i

* CA Connector Name

CA Connector

i

* Certificate Validity

365

days

i

The following table provides the field description for Microsoft Standalone CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Dropdown	Yes	Type 3 or more letters of the certificate keywords after which a list of	NA

Field Name	Field Type	Mandatory	Description	Validation
			server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with EST client machine.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **AppViewX PKIaaS** is selected as CA.

* Select CA	AppViewX PKIaaS	▼	i
* CA Account	serc-certuser1	▼	i
* Issuer Location	asia-south1	▼	i
* Pool Name	OCSPPool	▼	i
* Issuer Name	TestArchfixnew	▼	i
* CA Certificate	CN = AVXSUBCA, SN = F6:28:0B:E7:64:E6:E6:A		i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for AppViewX PKIaaS CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Issuer Location	Dropdown	Yes	Select an issuer location that is associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA

Field Name	Field Type	Mandatory	Description	Validation
Issuer Name	Dropdown	Yes	Select an issuer name to issue the certificate.	NA
CA Certificate	Dropdown	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Microsoft Enterprise** is selected as CA.

* Select CA	Microsoft Enterprise	▼	i
* CA Account	MS Enterprise	▼	i
* CA Certificate	CN = avxdevlab-PTPLD178-CA, SN = 3D:00:00:0		i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for Microsoft Enterprise CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Dropdown	Yes	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	NA

Field Name	Field Type	Mandatory	Description	Validation
			communications with EST client machine.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- If the selected CA is **Microsoft Enterprise**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* Template Name
Administrator

Select a template from the dropdown list.

- When **Entrust MPKI** is selected as CA.

* Select CA
Entrust MPKI

* CA Account
EntrustMпкиCA

* CA Certificate

* CA Connector Name
CA Connector

* Certificate Validity
365
days

The following table provides the field description for Entrust MPKI CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Dropdown	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Amazon Private CA** is selected as CA.

Auto-Enrollment : EST

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
Amazon Private CA

* CA Account
AmazonPCA

* Region
us-east-1

* Issuer
AppViewX-AWS-SubCA

* Signature Algorithm
null

* CA Certificate

* CA Connector Name
CA Connector

* Validity
1
Year
Year

The following table provides the field description for Amazon Private CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Region	Dropdown	Yes	Select a valid region associated with the CA account.	NA

Field Name	Field Type	Mandatory	Description	Validation
			The dropdown is populated with the first available value. Select an appropriate value as required.	
Issuer	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Signature Algorithm	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.	NA
CA Certificate	Text	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in years)	Certificate validity accepts only numerical values.

- When **DigiCert CA** is selected as CA.

Auto-Enrollment : EST

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
DigiCert

* CA Account
DigicertCA

* Division
AppViewX Inc.

* Certificate Type
SSL Plus

* CA Certificate

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **DigiCert CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Division	Dropdown	Yes	Select a division associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account.	NA

Field Name	Field Type	Mandatory	Description	Validation
			The dropdown is populated with the first available value. Select an appropriate value as required.	
CA Certificate	Text	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/ months/years)	Certificate validity accepts only numerical values.

- 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.

Vendor specific details

* Server Type

Apache

▼

* Payment Method

Bill To Account Balance

▼

ⓘ

If the **Select CA =DigiCert**, and the **Certificate type = Client**, a separate section **Vendor Specific Details** is displayed after the CA Accounts section with one field.

Vendor specific details

* Payment Method

Bill To Account Balance



Field Name	Field Type	Mandatory	Description	Validation
Server Type	Dropdown	Yes	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Payment Method	Dropdown	Yes	Select a payment method. The possible options are: 1. Bill To Account Balance - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund. 2. Bill To Default Credit Card - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account	Alphanumeric characters, spaces, and the special characters - _ . * are allowed.

- When **Entrust** is selected as CA.

Auto-Enrollment : EST

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
Entrust

* CA Account
EntrustECS

* Certificate Type
Standard

* CA Certificate

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **Entrust CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account. - If the Certificate Category radiobutton is selected to <i>Server</i>, the dropdown is populated with the first available value. Select an appropriate value as required. - If the Certificate Category radiobutton is selected to <i>Client</i>, the dropdown is populated with 'None' as the default value.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Certificate	Text	Yes	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 EST client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

- If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Vendor specific details

Additional Emails

Custom Attributes

Demo

Certificate type

Tracking Id



Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed as shown above.

Field Name	Field Type	Mandatory	Description	Validation
Additional Emails	Text	No	Enter the valid email address in the field.	NA

Field Name	Field Type	Mandatory	Description	Validation
Demo	Text	No	Enter the demo details	NA
Certificate type	Text	No	Enter a valid certificate type	NA
Tracking id	Text	No	Enter the tracking id	NA

- When **DigiCert MPKI** is selected as CA.

Auto-Enrollment : EST

CA Accounts

* Certificate Group ⓘ

* Certificate Category ☒ Server ☐ Client

* Select CA ⓘ

* CA Account ⓘ

* Profiles ⓘ

* CA Certificate ⓘ ✕

* CA Connector Name ⓘ

The following table provides the field description for **DigiCert MPKI**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Profiles	Dropdown	Yes	Select a profile from the dropdown option.	NA
CA Certificate	Text	Yes	Type 3 or more letters of the certificate keywords and select one issuer certificate from the	NA

Field Name	Field Type	Mandatory	Description	Validation
			dropdown. 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.	
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA



Note: **Email address** is a mandatory field on the enrollment form for DigiCert MPKI, but while passing it in the CSR, it does not get 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

* common_name

?

* dnsName

Field Name	Field Type	Mandatory	Description	Validation
common_name	Text	Yes	This field will be auto-populated from the CSR.	NA
dnsName	Text	Yes	Enter a valid DNS name.	NA



Note: Based on the DigiCert MPKI account configuration Custom Attributes section may also be displayed on the endpoint configuration page.

- When **Nexus** is selected as CA,

Auto-Enrollment : EST

CA Accounts

* Certificate Group ⓘ

* Certificate Category ☐ Server ☒ Client

* Select CA ⓘ

* CA Account ⓘ

* CA Certificate ⓘ

* CA Connector Name ⓘ

* Certificate Validity

The following table provides the field description for **Nexus CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Certificate	Select	Yes	Type 3 or more letters of the certificate keywords and select one issuer certificate from the dropdown. 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.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Select	Yes	Validity of the certificate to be enrolled. (in days/ months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Procedure

AppViewX SCEP

Field Name	Field Type	Mandatory	Description	Validation
Procedure	Dropdown	Yes	Select the Procedure based on the configurations made in the Certificate Authority Setting.	NA

- When **GlobalSignMSSL** is selected as CA,

Auto-Enrollment : EST

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
GlobalSignMSSL

* CA Account
GlobalSignMSSL

* Product Type
Organization MSSL

* CA Certificate

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **GlobalSignMSSL CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Product Type	Dropdown	Yes	Select the specific Product Type. The values are fetched from the CA Settings configuration.	NA
CA Certificate	Select	Yes	Type 3 or more letters of the certificate keywords and select one issuer certificate from the dropdown. This issuer certificate will be used for signing the CSR by the certificate authority.	NA

Field Name	Field Type	Mandatory	Description	Validation
			NOTE: Only the issuer certificates available in the root or intermediate certificates inventory will be shown for selection	
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Profile name

Field Name	Field Type	Mandatory	Description	Validation
Profile name	Dropdown	Yes	Select the Profile based on the configurations made in the Certificate Authority Setting.	NA

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

CA mandates Point of Contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the Point of Contact information entered here.

* First Name

* Email Address

* Phone Number

Field Name	Field Type	Mandatory	Description	Validation
First Name	Text	Yes	Enter the first name	NA
Email Address	Text	Yes	Enter the valid email address	NA
Phone Number	Text	Yes	Enter the valid phone number	NA

8. Configure the **Advanced Settings** details as follows:

Advanced Settings

* Switch to Enroll ☐ Yes ☒ No ⓘ

* Fetch Certificate Parameters ☐ Yes ☒ No ⓘ

* Include Truststore Certificates ☐ Yes ☒ No ⓘ

* Retry Count



* Retry Frequency

seconds



The following table provides the field description for Advanced Settings:

Field Name	Field Type	Mandatory	Description	Validation
*Switch to Enroll	Radio button	Yes	Select Yes or No Selecting the radio button as Yes will convert the re-enrollment requests to enrollment requests	
*Fetch Certificate Parameters	Radio button	Yes	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	Radio button	Yes	Select whether the issuer certificate needs to be sent to client machines after enrolment.	
*Retry Count	Text	Yes	Values accepted between 5 - 99. Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received.	
*Retry Frequency	Text	Yes	Values accepted between 10 - 99. The value specified in this field determines the duration taken between the trigger calls by the EST agent.	

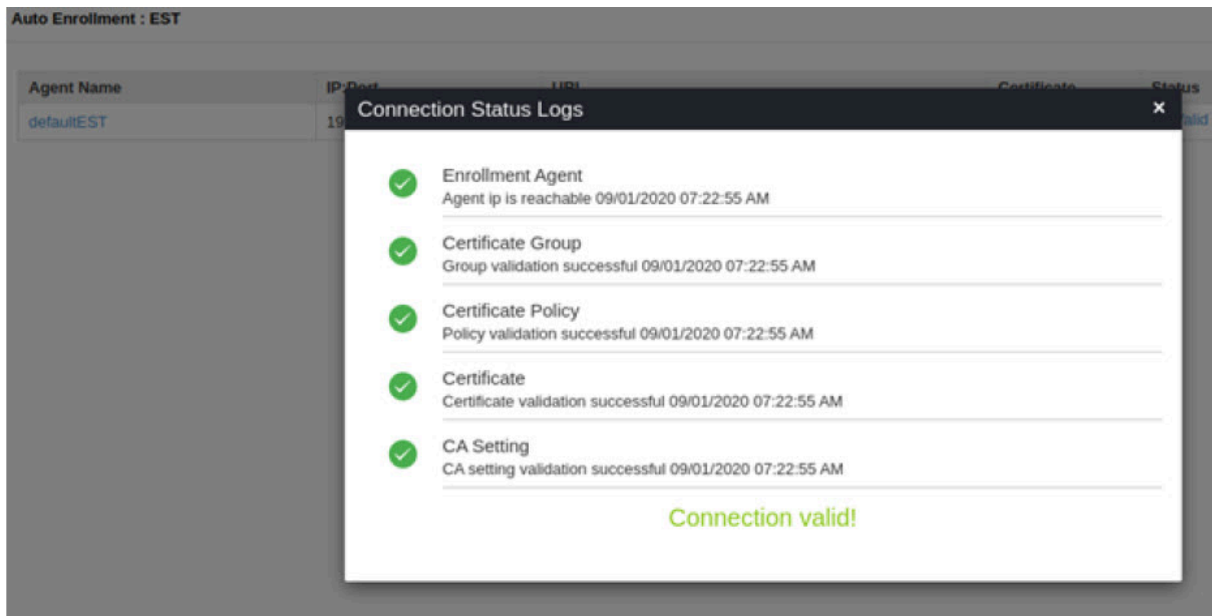
9. Click **Save**.

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. Log in to AppViewX application with valid credentials.
2. Click the **Menu** button.
3. Navigate to **CERT+ > ADMINISTRATION**.
4. Under the **Administration** section, click **Auto-Enrollment** and then select **EST**.
5. On the **EST** page, click **Check** 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 Intune is 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 **OFF** the 'Approval Required' flag in **Menu -> Inventory -> Certificate -> Policy** page.
- A valid agent settings should be available in **Menu -> Inventory -> Certificate -> Settings**.

- [Configuring MS Intune](#)
- [Validating MS Intune](#)

Configuring MS Intune

To perform mobile device certificate enrollments for MS Intune managed devices using the (SCEP based) MS Intune protocol on AppViewX, the admin or a privileged user needs to first set up the MS Intune server agent using the AppViewX portal. Upon successful set up of the MS Intune server agent through the portal, a URL will be generated. Clients can then use this URL to send enrollment requests to AppViewX via MS Intune.

The detailed steps for setting up the MS Intune server agent are listed below:

1. Log in to AppViewX application with admin or privileged user credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **CERT+ > ADMINISTRATION > Auto Enrollment > MS INTUNE**.
4. Select **Add** or **Configure Now**.
5. 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 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.
- If entering the IP the ensure that single cloud connector is used.

Endpoint Details

* Name

* IP/FQDN

Eg - 192.168.1.1

 ⓘ

* Port

30022

 ⓘ

The following table provides the field description for Agent Details section:

Field Name	Field Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the Agent setting.	No special characters other than '.', '-', '_' are allowed. Name should not start with special characters.
Host	Text	Yes	IP address of the AppViewX intune plugin.	Invalid IP address(example: xxx.xxx.xxx.xxx)
Port	Text	Yes	HTTP gateway port of the AppViewX intune plugin node.	Port will accept only numerical values between 0 to 65535.

6. Configure the **Intune Details** as below:

Intune Details

* Client ID

* Tenant ID

* Client Secret

The following table provides the field description for Intune Details section:

Field Name	Field Type	Mandatory	Description	Validation
Client ID	Text	Yes	Client ID of the Intune Account - this value should have been captured during Intune App Registration.	NA

Field Name	Field Type	Mandatory	Description	Validation
Tenant ID	Text	Yes	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 .	NA
Client Secret	Text	Yes	Client Secret for the Intune Account - this value should have been captured during Intune App Registration.	NA

7. Configure the **CA Accounts** as follows:

CA Accounts

- * Certificate Group ⓘ
- * Certificate Category ☒ Server ☐ Client
- * Select CA ⓘ
- * CA Account ⓘ
- * Server Certificate ⓘ
- * CA Connector Name ⓘ
- * Certificate Validity days ⓘ

The following table provides the field description for CA Accounts section:

Field Name	Field Type	Mandatory	Description	Validation
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Category	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Select	Yes	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 • Google • Ejbca • Microsoft Standalone • AppViewX PKIaaS • Microsoft Enterprise • Entrust MPKI • Amazon Private CA • DigiCert • DigiCert MPKI • Nexus • Globalsign MSSL  Note: The Vendor Specific Details section is displayed after the CA Accounts section only if Ejbca, Microsoft Enterprise, or Entrust MPKI is selected as the CA.	NA

The following fields are displayed as per the selected **CA**:

- When **AppViewX** is selected as CA,

* Select CA	AppViewX	▼	i
* CA Account	AppViewX CA	▼	i
* Server Certificate	No server certificates found		i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for AppViewX CA:

Field Name	Field Type	Mandatory	Description	Validation
				NA
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Server Certificate	Select	Yes	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,	NA

Field Name	Field Type	Mandatory	Description	Validation
			one certificate can be selected for further communications with SCEP client machine.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values

- When **Google** is selected as CA,

* Select CA	Google	▼	i
* CA Account	serc-certuser1-Google_Server_Client_CreateC	▼	i
* Issuer Location	us-east1	▼	i
* Pool Name	EntCApool1	▼	i
* Issuer Name	EntCA1fromPool1	▼	i
* Server Certificate	No server certificates found		i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for Google CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Issuer Location	Dropdown	Yes	Select the issuer location associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
Issuer Name	Dropdown	Yes	Select a issuer name to issue the certificate.	NA
Server Certificate	Dropdown	Yes	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.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Ejbca** is selected as CA,

* Select CA	Ejbca	▼	ⓘ
* CA Account	ejbca	▼	ⓘ
* Server Certificate			ⓘ
* CA Connector Name	CA Connector		ⓘ
* Certificate Validity	365	days	ⓘ

The following table provides the field description for Ejbca CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Server Certificate	Dropdown	Yes	Type 3 or more letters of the	NA

Field Name	Field Type	Mandatory	Description	Validation
			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.	
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Ejbca**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* End Entity Profile Name
APPVIEWX PROFILE

End entity user name

* Issuer Common Name
AVX EJBCA ENTERPRISE CA

* Certificate Profile Name
AVX EJBCA ENTERPRISE PROFILE

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
End Entity Profile Name	Dropdown	Yes	Select a profile of an end entity.	NA
End entity user name	Text	No	Enter the user name for the end entity.	Alphanumeric characters, spaces, and the special characters -_.* are allowed.
Issuer Common Name	Dropdown	Yes	Select a common name of an issuer.	NA
Certificate Profile Name	Dropdown	Yes	Select a profile name of certificate.	NA

- When **Microsoft Standalone** is selected as CA,

* Select CA

Ejbca

▼

ⓘ

* CA Account

ejbca

▼

ⓘ

* Server Certificate

ⓘ

* CA Connector Name

CA Connector

ⓘ

* Certificate Validity

365

days

ⓘ

The following table provides the field description for Microsoft Standalone CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with	NA

Field Name	Field Type	Mandatory	Description	Validation
			the selected CA to be used for certificate creation operations.	
Server Certificate	Dropdown	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Microsoft Enterprise** is selected as CA,

* Select CA	Microsoft Enterprise	▼	ⓘ
* CA Account	MS Enterprise	▼	ⓘ
* Server Certificate			ⓘ
* CA Connector Name	CA Connector		ⓘ
* Certificate Validity	365	days	ⓘ

The following table provides the field description for Microsoft Enterprise CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Server Certificate	Dropdown	Yes	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	NA

Field Name	Field Type	Mandatory	Description	Validation
			with SCEP client machine.	
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Microsoft Enterprise**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* CA Name

SEDemo ECS Public SSL AppViewX

▼

* Cert Profiles

advantage profile

▼

Select a template from the dropdown list.

- When **AppViewX PKIaaS** is selected as CA.

* Select CA	AppViewX PKIaaS	▼	i
* CA Account	hdfc	▼	i
* Issuer Location	asia-south1	▼	i
* Pool Name	hdfctenantrootca	▼	i
* Issuer Name	hdfctenantrootca1	▼	i
* Server Certificate		Upload	i
* CA Connector Name	CA Connector		i
* Certificate Validity	365	days	i

The following table provides the field description for AppViewX PKIaaS CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Issuer Location	Dropdown	Yes	Select an issuer location that is associated with the CA account.	NA

Field Name	Field Type	Mandatory	Description	Validation
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
Issuer Name	Dropdown	Yes	Select an issuer name to issue the certificate.	NA
Server Certificate	Browse	Yes	Browse and upload a server certificate with private key to certificate inventory and enter the exact match of common name/serial number to select the same.	NA
CA Certificate	Dropdown	Yes	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 EST client machine.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Entrust MPKI** is selected as CA.

* Select CA

Entrust MPKI

▼

i

* CA Account

EntrustMпкиCA

▼

i

* Server Certificate

Upload

i

* CA Connector Name

CA Connector

i

* Certificate Validity

365

days

i

The following table provides the field description for Entrust MPKI CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Server Certificate	Browse	Yes	Browse and upload a server certificate with private key to certificate inventory and enter the exact match of common name/serial number to select the same.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

If the selected CA is **Entrust MPKI**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* CA Name

SEDemo ECS Public SSL AppViewX

▼

* Cert Profiles

advantage profile

▼

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
CA Name	Dropdown	Yes	Select a CA name from the dropdown list.	NA

Field Name	Field Type	Mandatory	Description	Validation
Cert Profiles	Dropdown	Yes	Select a cert profile from the dropdown list.	NA

- When **Amazon Private CA** is selected as CA.

Auto-Enrollment : SCEP MS INTUNE

CA Accounts

* Certificate Group ⓘ

* Certificate Category ☒ Server ☐ Client

* Select CA ⓘ

* CA Account ⓘ

* Region

* Issuer

* Signature Algorithm

* Server Certificate ⓘ

* CA Connector Name ⓘ

* Certificate Validity

The following table provides the field description for **Amazon Private CA**

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Region	Dropdown	Yes	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Issuer	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Signature Algorithm	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.	NA
Server Certificate	Select	Yes	Browse and upload a certificate for further communications with SCEP MS Intune client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

- When **DigiCert** is selected as CA.

Auto-Enrollment : SCEP MS INTUNE

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server ☐ Client

* Select CA
DigiCert

* CA Account
DigicertCA

* Division
AppViewX Inc.

* Certificate Type
SSL Plus

* Server Certificate

* CA Connector Name
CA Connector

* Certificate Validity
1 Days

The following table provides the field description for **DigiCert CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Division	Dropdown	Yes	Select a division associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Server Certificate	Text	Yes	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 MS Intune client machine.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/ months/years)	Certificate validity accepts only numerical values.

- 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.

Vendor specific details

* Server Type

Apache

▼

* Payment Method

Bill To Account Balance

▼

?

If the **Select CA =DigiCert**, and the **Certificate type = Client**, a separate section **Vendor Specific Details** is displayed after the CA Accounts section with one field.

Vendor specific details

*
Payment Method

Bill To Account Balance
▼

i

Field Name	Field Type	Mandatory	Description	Validation
Server Type	Dropdown	Yes	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Payment Method	Dropdown	Yes	Select a payment method. The possible options are: Bill To Account Balance - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund. Bill To Default Credit Card - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account	Alphanumeric characters, spaces, and the special characters <code>_.*</code> are allowed.

8. Configure the **Advanced Settings** as follows:

Advanced Settings

* Fetch Certificate Parameters

☐ Yes
 ☒ No

* Retry Count

5

* Retry Frequency

10

seconds

* Certificate Poll Type

☒ Issuer and Subject
 ☐ Transaction ID

The following table provides the field description for the Advanced Settings section:

Field Name	Field Type	Mandatory	Description	Validation
*Fetch Certificate Parameters	Radio button	Yes	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.	
*Retry Count	Text	Yes	Values accepted between 5 - 99. Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received.	
*Retry Frequency	Text	Yes	Values accepted between 10 - 99. The value specified in this field determines the duration taken between the trigger calls by the EST agent.	
*Certificate Poll Type	Radio button	Yes	Select <i>Issuer and Subject</i> or <i>Transaction ID</i>.	

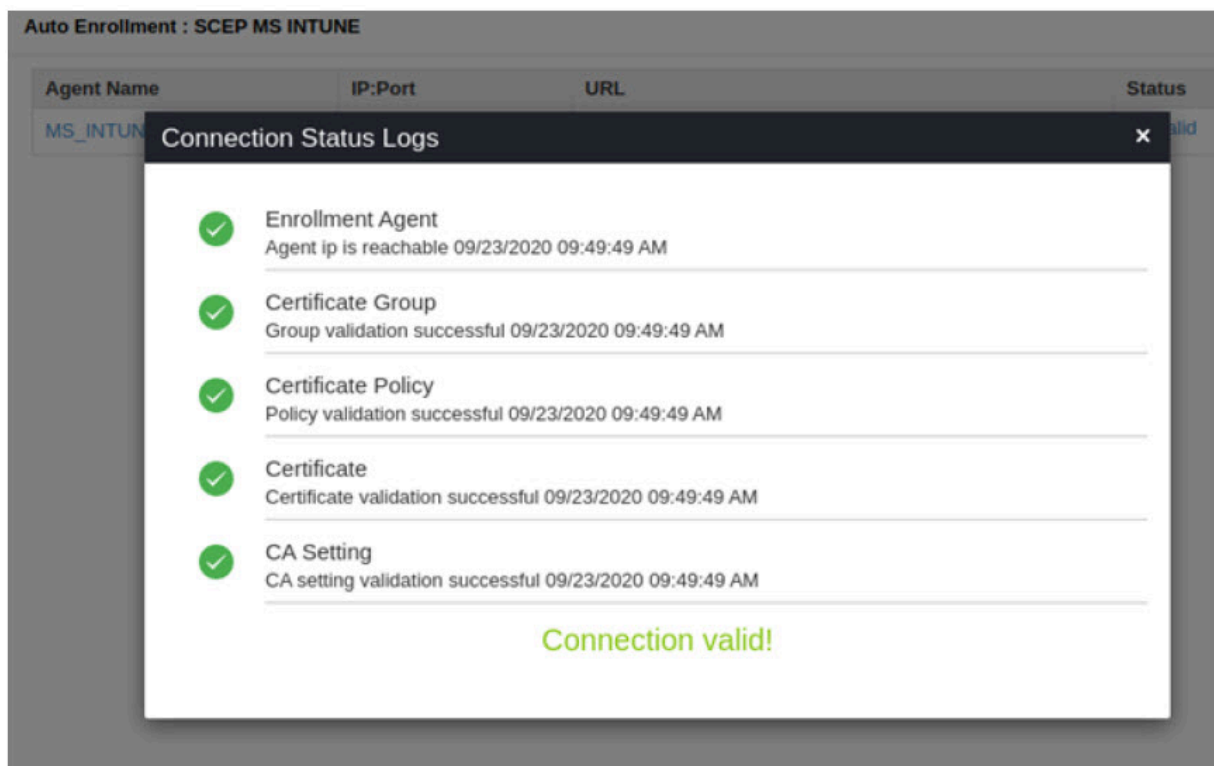
Field Name	Field Type	Mandatory	Description	Validation
			The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.	

9. 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. Click the **Menu** button.
2. Navigate to **CERT+ > ADMINISTRATION**.
3. Under the **Administration** section, click **Auto Enrollment** and then select **MS Intune**.
4. In the **MS Intune** page, click **Check** 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.

- There should be an agent(avx_vendor_cert_scep_agent) up and running for SCEP in appviewx.
- This 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 **OFF** the 'Approval Required' flag in **Menu -> Inventory -> Certificate -> Policy** page.
- A valid agent settings should be available in **Menu -> Inventory -> Certificate -> Settings**.
- [Configuring SCEP](#)
- [Validating SCEP](#)

Configuring SCEP

To perform client certificate enrollments using SCEP protocol, the admin or a privileged user needs to first set up the SCEP server agent using the AppViewX portal. Upon successful set up of the SCEP server Agent through the portal, a URL will be generated. Clients can then use this URL to send enrollment requests to AppViewX via SCEP.

The detailed steps for setting up the SCEP server agent are listed below:

1. Log in to AppViewX application with admin or privileged user credentials.
2. Click the menu button located in the upper left corner of the screen.
The left navigation pane appears.
3. Navigate to **CERT+ > ADMINISTRATION > Auto Enrollment > SCEP**.
4. Select **Add** or **Configure Now**.
5. 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.

Endpoint Details

*

Name

*

IP/FQDN

Eg - 192.168.1.1

i

*

Port

30022

i

Challenge Password

The following table provides the field description for Agent Details section:

Field Name	Field Type	Mandatory	Description	Validation
Name	Text	Yes	A unique name to identify the agent setting.	No special characters other than '.', '-', '_' are allowed. The name should not start with special characters.
IP/FQDN	Text	Yes	Enter the FQDN/IP address of the appviewx cloud connector.	Invalid FQDN/IP address(example: xxx.xxx.xxx.xxx)
Port	Text	Yes	HTTP gateway port of the AppViewX node.	Port will accept only numerical values between 0 to 65535.
Challenge Password	Text	No	A challenge token to be used while enrolling certificates.	NA

6. Configure the **CA Accounts** details as follows:

CA Accounts

* Certificate Group

Auto_Enroll_AppViewX_CA_Group

* Certificate Category

☒ Server
 ☐ Client

* Select CA

AppViewX

* CA Account

AppViewX CA

* Certificate Profile

Server

* Registration Authority Certificate

* CA Connector Name

CA Connector

* Certificate Validity

365

days

The following table provides the field description for CA Accounts section:

Field Name	Field Type	Mandatory	Description	Validation
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.	NA
Certificate Category	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Select	Yes	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 • Google	NA

Field Name	Field Type	Mandatory	Description	Validation
			• Ejbca • AppViewX PKIaaS • Microsoft Enterprise • Entrust MPKI • Entrust • Amazon Private CA • DigiCert • DigiCert MPKI • Nexus • Globalsign MSSL  Note: The Vendor Specific Details section is displayed after the CA Accounts section only if Ejbca, Microsoft Enterprise, Entrust MPKI, or DigiCert is selected as the CA.	
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Registration Authority Certificate.	Select	Yes	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	NA

Field Name	Field Type	Mandatory	Description	Validation
			the exact common name or serial number.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

The following fields are displayed as per the selected **CA**:

- When **AppViewX** is selected as CA,

* Select CA

AppViewX

* CA Account

AppViewX CA

* Certificate Profile

Server

* Registration Authority Certificate

* CA Connector Name

CA Connector

* Certificate Validity

365

days

The following table provides the field description for AppViewX CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for	NA

Field Name	Field Type	Mandatory	Description	Validation
			certificate creation operations.	
Certificate Profile	Dropdown	Yes	Select the certificate profile.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled. Based on this value, the CA connector name on the holistic view will be shown to all certificates issued through this SCEP agent.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Validity	Text	Yes	Validity of the certificate (in days) to be enrolled. This value is applicable for all the certificate issue through the SCEP agent.	Certificate validity accepts only numerical values.

- When **Google** is selected as CA,

* Select CA

Google

▼

ⓘ

* CA Account

google

▼

ⓘ

* Certificate Profile

Server

▼

* Issuer Location

us-east1

▼

ⓘ

* Pool Name

SplunkLab

▼

ⓘ

* Issuer Name

Splunk_Private_RootCA_lab

▼

ⓘ

* Registration Authority Certificate

ⓘ

* CA Connector Name

CA Connector

ⓘ

* Certificate Validity

365

days

ⓘ

The following table provides the field description for Google CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with	NA

Field Name	Field Type	Mandatory	Description	Validation
			the selected CA to be used for certificate creation operations.	
Issuer Location	Dropdown	Yes	Select the issuer location associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
Issuer Name	Dropdown	Yes	Select an issuer name to issue the certificate.	NA
Registration Authority Certificate	Browse	Yes	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.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled. Based on this value, the CA connector name on the holistic view will be shown to all certificates issued through this SCEP agent.	NA
Certificate Validity	Text	Yes	Validity of the certificate (in days) to be enrolled. This value is applicable for all the certificate issue through the SCEP agent.	Certificate validity accepts only numerical values.

- When **Ejbca** is selected as CA,

* Select CA

Ejbca

* CA Account

EJBCA CA

* Registration Authority Certificate

* CA Connector Name

CA Connector

The following table provides the field description for Ejbca CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled. Based on this value, the CA connector name on the holistic view will be shown to all	NA

Field Name	Field Type	Mandatory	Description	Validation
			certificates issued through this SCEP agent.	
Certificate Validity	Text	Yes	Validity of the certificate (in days) to be enrolled. This value is applicable for all the certificate issue through the SCEP agent.	Certificate validity accepts only numerical values.

If the selected CA is **Ejbca**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* End Entity Profile Name

APPVIEWX PROFILE

▼

End entity user name

?

* Issuer Common Name

AVX EJBCA ENTERPRISE CA

▼

* Certificate Profile Name

AVX EJBCA ENTERPRISE PROFILE

▼

The following table provides the field description for Vendor specific details:

Field Name	Field Type	Mandatory	Description	Validation
End Entity Profile Name	Dropdown	Yes	Select a profile of an end entity.	NA
End entity user name	Text	No	Enter the user name for the end entity.	Alphanumeric characters, spaces, and the special characters -_.* are allowed.

Field Name	Field Type	Mandatory	Description	Validation
Issuer Common Name	Dropdown	Yes	Select a common name of an issuer.	NA
Certificate Profile Name	Dropdown	Yes	Select a profile name of certificate.	NA

- When **AppViewX PKIaaS** is selected as CA,

* Select CA	AppViewX PKIaaS	▼	ⓘ
* CA Account	serc-certuser1	▼	ⓘ
* Issuer Location	asia-south1	▼	ⓘ
* Pool Name	OCSPPool	▼	ⓘ
* Issuer Name	TestArchfixnew	▼	ⓘ
* Server Certificate			ⓘ
* CA Connector Name	CA Connector		ⓘ
* Certificate Validity	365	days	ⓘ

The following table provides the field description for AppViewX PKIaaS CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Issuer Location	Dropdown	Yes	Select the issuer location associated with the CA account.	NA
Pool Name	Dropdown	Yes	Select a pool name to issue the certificate.	NA
Issuer Name	Dropdown	Yes	Select a issuer name to issue the certificate.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	No special characters are allowed. Only alphanumeric

Field Name	Field Type	Mandatory	Description	Validation
				and space are allowed.
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values.

- When **Microsoft Enterprise** is selected as CA,

* Select CA

Microsoft Enterprise

* CA Account

Microsoft Enterprise CA

* Registration Authority Certificate

* CA Connector Name

CA Connector

The following table provides the field description for Microsoft Enterprise CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Registration Authority Certificate	Browse	Yes	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.	NA

Field Name	Field Type	Mandatory	Description	Validation
			Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled. Based on this value, the CA connector name on the holistic view will be shown to all certificates issued through this SCEP agent.	NA
Certificate Validity	Text	Yes	Validity of the certificate (in days) to be enrolled. This value is applicable for all the certificate issue through the SCEP agent.	Certificate validity accepts only numerical values.

If the selected CA is **Microsoft Enterprise**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* Template Name ⓘ

Select a template from the dropdown list.

- When **Entrust MPKI** is selected as CA,

* Select CA ⓘ

* CA Account ⓘ

* Registration Authority Certificate ⓘ

* CA Connector Name ⓘ

The following table provides the field description for Entrust MPKI CA:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.	NA
Registration Authority Certificate	Browse	Yes	Add the chosen CA issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.	NA

Field Name	Field Type	Mandatory	Description	Validation
			Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.	
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled. Based on this value, the CA connector name on the holistic view will be shown to all certificates issued through this SCEP agent.	NA
Certificate Validity	Text	Yes	Validity of the certificate (in days) to be enrolled. This value is applicable for all the certificate issue through the SCEP agent.	Certificate validity accepts only numerical values.

If the selected CA is **Entrust MPKI**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

Vendor specific details

* CA Name

* Cert Profiles

Field Name	Field Type	Mandatory	Description	Validation
CA Name	Dropdown	Yes	Select a CA name from the dropdown list.	NA
Cert Profiles	Dropdown	Yes	Select a cert profile from the dropdown list.	NA

- When **Amazon Private CA** is selected as CA.

* Select CA ⓘ

* CA Account ⓘ

* Region

* Issuer

* Signature Algorithm

* Registration Authority Certificate ⓘ

* CA Connector Name ⓘ

* Certificate Validity Days

* Validity

The following table provides the field description for **Amazon Private CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Region	Dropdown	Yes	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Issuer	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Signature Algorithm	Dropdown	Yes	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.	NA
Registration Authority Certificate	Browse	Yes	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.	NA

Field Name	Field Type	Mandatory	Description	Validation
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in years)	Certificate validity accepts only numerical values.

- When **DigiCert CA** is selected as CA.

* Select CA

DigiCert

* CA Account

DigiCert CA

* Division

AppViewX Inc.

* Certificate Type

SSL Plus

* Registration Authority Certificate

* CA Connector Name

CA Connector

* Certificate Validity

1

Days

The following table provides the field description for **DigiCert CA**

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Division	Dropdown	Yes	Select a division associated with the CA account.	NA

Field Name	Field Type	Mandatory	Description	Validation
			The dropdown is populated with the first available value. Select an appropriate value as required.	
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

- 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.

Vendor specific details

* Server Type

Apache

▼

* Payment Method

Bill To Account Balance

▼

ⓘ

- If the **Select CA =DigiCert**, and the **Certificate type = Client**, a separate section **Vendor Specific Details** is displayed after the CA Accounts section with one field.

Vendor specific details

* Payment Method

Bill To Account Balance

▼

ⓘ

Field Name	Field Type	Mandatory	Description	Validation
Server Type	Dropdown	Yes	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.	NA
Payment Method	Dropdown	Yes	Select a payment method. The possible options are: Bill To Account Balance - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund.	Alphanumeric characters, spaces, and the special characters <code>_.*</code> are allowed.

Field Name	Field Type	Mandatory	Description	Validation
			2. Bill To Default Credit Card - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account	

- When **Entrust** is selected as CA.

* Select CA

Entrust

* CA Account

Entrust CA

* Certificate Type

Advantage

* Registration Authority Certificate

* CA Connector Name

CA Connector

* Certificate Validity

1

Days

The following table provides the field description for **Entrust CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA

Field Name	Field Type	Mandatory	Description	Validation
Certificate Type	Dropdown	Yes	Select a valid cert type associated with the CA account. - If the Certificate Category radiobutton is selected to <i>Server</i>, the dropdown is populated with the first available value. Select an appropriate value as required. - If the Certificate Category radiobutton is selected to <i>Client</i>, the dropdown is populated with 'None' as the default value.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Vendor specific details

Additional Emails

Custom Attributes

Demo

Certificate type

Tracking Id



Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed as shown above.

Field Name	Field Type	Mandatory	Description	Validation
Additional Emails	Text	No	Enter the valid email address in the field.	NA
Demo	Text	No	Enter the demo details	NA
Certificate type	Text	No	Enter a valid certificate type	NA
Tracking id	Text	No	Enter the tracking id	NA

- When **DigiCert MPKI** is selected as CA

* Select CA ⓘ

* CA Account ⓘ

* Profiles ⓘ

* Registration Authority Certificate

* CA Connector Name ⓘ

The following table provides the field description for **DigiCert MPKI**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Profiles	Dropdown	Yes	Select a profile from the dropdown option.	NA
Registration Authority Certificate	Browse	Yes	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.	NA
CA Connector Name	Text	Yes	Name of the CA connector after the certificate is enrolled.	NA

The **Custom Attributes** section is displayed on selecting the specific values from the **Profile** dropdown:

Custom Attributes

* common_name

* dnsName

Field Name	Field Type	Mandatory	Description	Validation
common_name	Text	Yes	This field will be auto-populated from the CSR.	NA
dnsName	Text	Yes	Enter a valid DNS name.	NA



Note: Based on the DigiCert MPKI account configuration Custom Attributes section may also be displayed on the endpoint configuration page.

- When **Nexus** is selected as CA

Auto-Enrollment : SCEP

CA Accounts

* Certificate Group ⓘ

* Certificate Category ☒ Server ☐ Client

* Select CA ⓘ

* CA Account ⓘ

* Registration Authority Certificate ⓘ

* CA Connector Name ⓘ

* Certificate Validity

The following table provides the field description for **Nexus CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Registration Authority Certificate	Select	Yes	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.	NA

Field Name	Field Type	Mandatory	Description	Validation
			Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.	
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Select	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Procedure

Field Name	Field Type	Mandatory	Description	Validation
Procedure	Dropdown	Yes	Select the Procedure based on the configurations made in the Certificate Authority Setting.	NA

- When **GlobalSignMSSL** is selected as CA.

Auto-Enrollment : SCEP

CA Accounts

* Certificate Group
Default

* Certificate Category
☒ Server
☐ Client

* Select CA
GlobalSignMSSL

* CA Account
GlobalSignMSSL

* Product Type
Organization MSSL

* Registration Authority Certificate

* CA Connector Name
CA Connector

* Certificate Validity
1
Days

The following table provides the field description for **GlobalSignMSSL CA**:

Field Name	Field Type	Mandatory	Description	Validation
CA Account	Dropdown	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
Product Type	Dropdown	Yes	Select the specific Product Type. The values are fetched from the CA Settings configuration.	NA
Registration Authority Certificate	Select	Yes	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.	NA

Field Name	Field Type	Mandatory	Description	Validation
			Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.	
CA Connector Name	Select	Yes	Name of the CA connector after the certificate is enrolled.	NA
Certificate Validity	Dropdown	Yes	Validity of the certificate to be enrolled. (in days/months/years)	Certificate validity accepts only numerical values.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor specific details

* Profile name

Field Name	Field Type	Mandatory	Description	Validation
Profile	Dropdown	Yes	Select the Profile based on the configurations made in the Certificate Authority Setting.	NA

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

CA mandates Point of Contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the Point of Contact information entered here.

* First Name

* Email Address

* Phone Number

Field Name	Field Type	Mandatory	Description	Validation
First Name	Text	Yes	Enter the first name	NA
Email Address	Text	Yes	Enter the valid email address	NA
Phone Number	Text	Yes	Enter the valid phone number	NA

7. Configure the **Advanced Settings** details as follows:

Advanced Settings

* Include Truststore Certificates

☒ Yes ☐ No



* Fetch Certificate Parameters

☐ Yes ☒ No



* Retry Count

5



* Retry Frequency

10

seconds



* Certificate Poll Type

☒ Issuer and Subject ☐ Transaction ID

The following table provides the field description for Advance Settings section:

Field Name	Field Type	Mandatory	Description	Validation
*Include Truststore Certificates	Radio button	Yes	Select whether the issuer certificate needs to be sent to client machines after enrolment.	
*Fetch Certificate Parameters	Radio button	Yes	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.	
*Retry Count	Text	Yes	Values accepted between 5 - 99. Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received.	
*Retry Frequency	Text	Yes	Values accepted between 10 - 99. The value specified in this field determines the duration taken between the trigger calls by the EST agent.	
*Certificate Poll Type	Radio button	Yes	Select <i>Issuer and Subject</i> or <i>Transaction ID</i> . The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.	

8. Click **Save**.

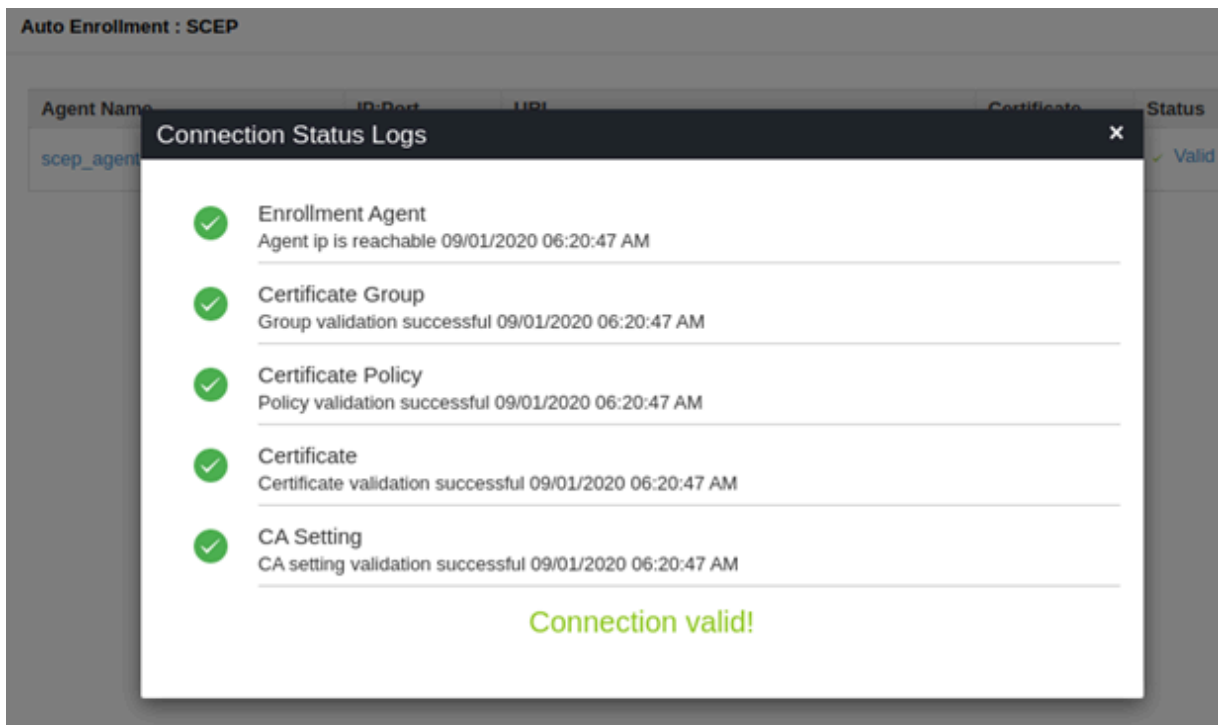
Validating SCEP

Once the SCEP settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

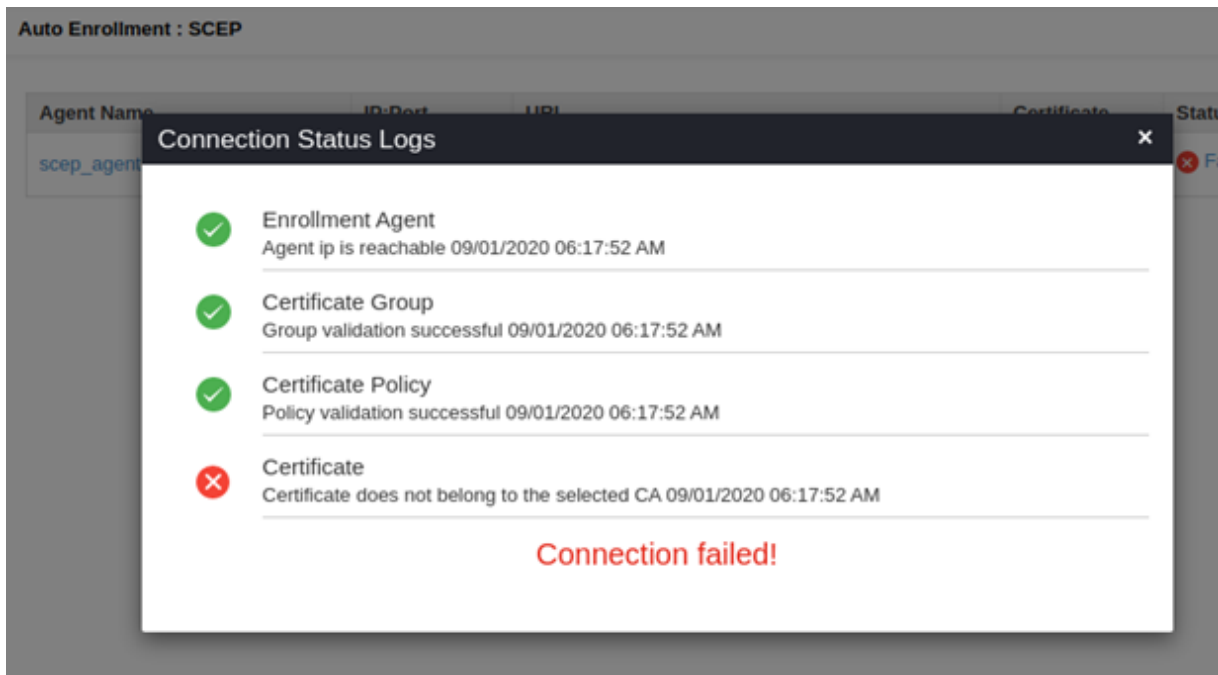
1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** button.
3. Navigate to **CERT+ > ADMINISTRATION**.
4. Under the **Administration** section, click **Auto-Enrollment** and then select **SCEP**.
5. On the **SCEP** page, click **Check** to validate the SCEP setting that has been created.

The SCEP settings will be validated and the **Status** will be shown as either **Success** or **Failure**.

Success Scenario



Failure Scenario



Chapter 4: Glossary

This table describes common terms used in this guide.

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.
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 smartphones, tablet computers, and laptops.
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

Terms	Definition
SCEP	Simple Certificate Enrollment Protocol (SCEP) is an IETF RFC. This enables network users 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.