appviewX

CLMaaS CERT Admin Guide

Version: 2022.1.0

CLMaaS CERT+ Admin Guide

AppViewX's CLMaaS CERT+ provides an end–to–end lifecycle management of x.509 digital certificates across complex networks to secure your business. With CLMaaS 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:

Copyright AppViewX, Inc.

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).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release v2021.1.0	September 2021

About this Guide

This guide outlines the CLMaaS 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Getting Started

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.

CLMaaS CERT+ Overview

AppViewX's CLMaaS 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.

CLMaaS 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:

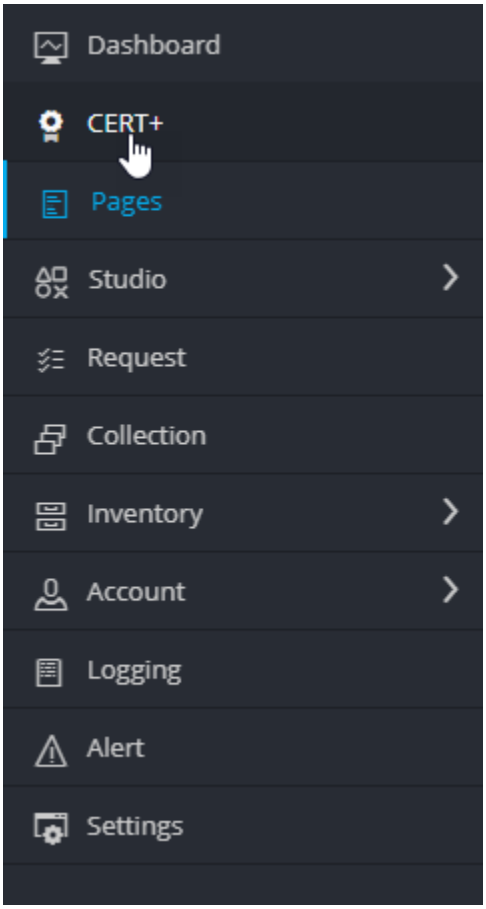
- License Management
- Logging & Alert Management.

Accessing the CLMaaS CERT+

To access the CLMaaS CERT+:

1. In the address bar of your browser, enter your SaaS account URL.
   The AppViewX CLMaaS login page is displayed.

2. Login to the AppViewX CLMaaS.
   The AppViewX CLMaaS landing page appears.
3. From the top-right corner of the landing page, click the button.
   The application header is displayed.
4. From the top-left corner of the landing page, click .
5. From the menu displayed, click **CERT+**.



CLMaaS CERT+ Home Page

The CLMaaS 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 CLMaaS CERT+ home page:

Options	Description
Menu button	Displays the left navigation pane of the AppViewX.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Expand/ Collapse</td><td>Expands/Collapses all the options, which are on the left navigation pane.</td></tr>
<tr><td>Search Field</td><td>Searches for the given key word(s) in the field and results the feature that matches the search key word(s).</td></tr>
<tr><td>Left Navigation Pane</td><td>Displays all the features available in the CERT+.</td></tr>
<tr><td>Collapse/ Expand</td><td>Hides/Displays the left navigation pane.</td></tr>
<tr><td>Helps Tool Bar</td><td>Use the tool-bars for the additional options:
<table><tr><th>Options</th><th>Description</th></tr><tr><td>Date</td><td>Displays Today Date</td></tr><tr><td>Time</td><td>Displays the time based on the locale</td></tr></table></td></tr>
</table>

Chapter 2: Account Module

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

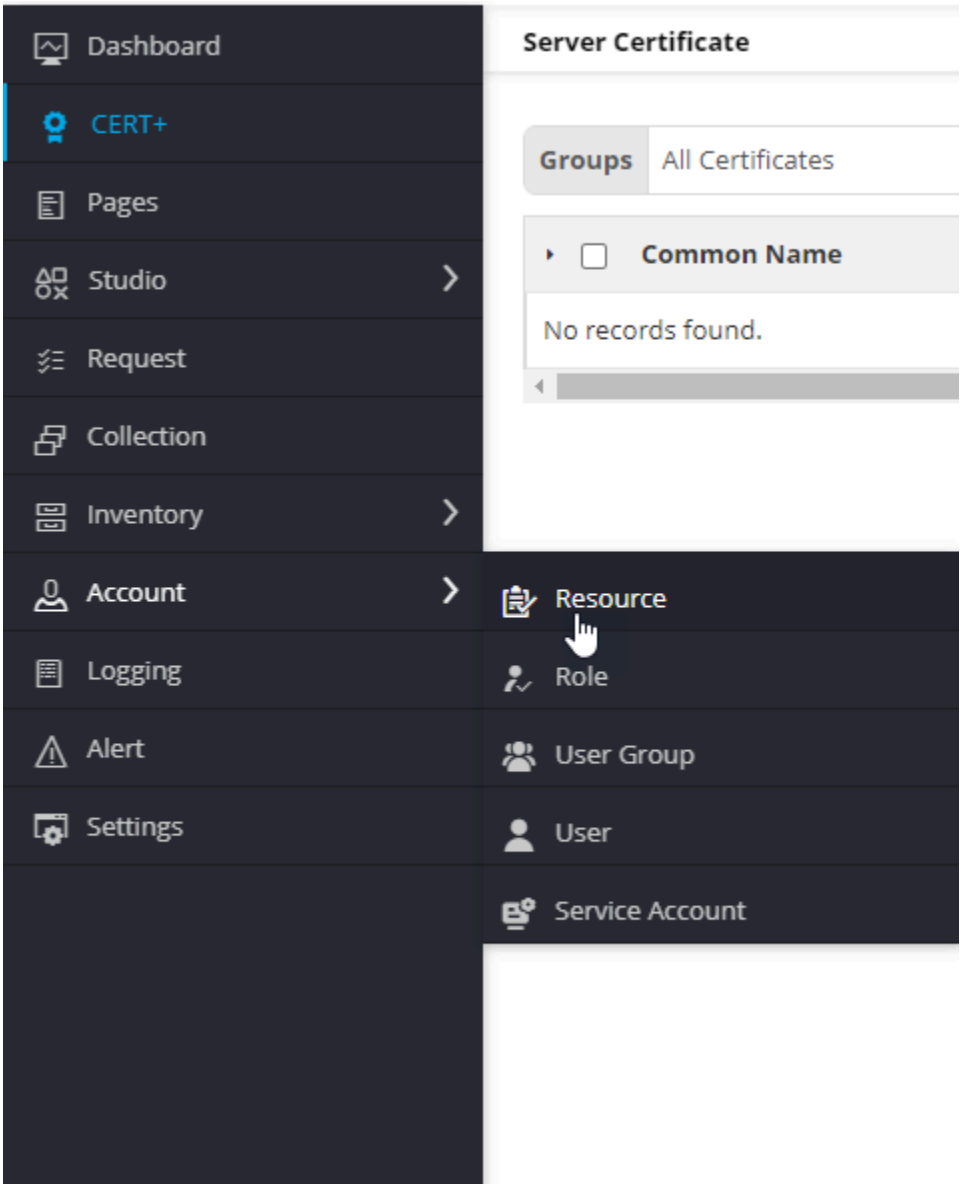
Overview

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

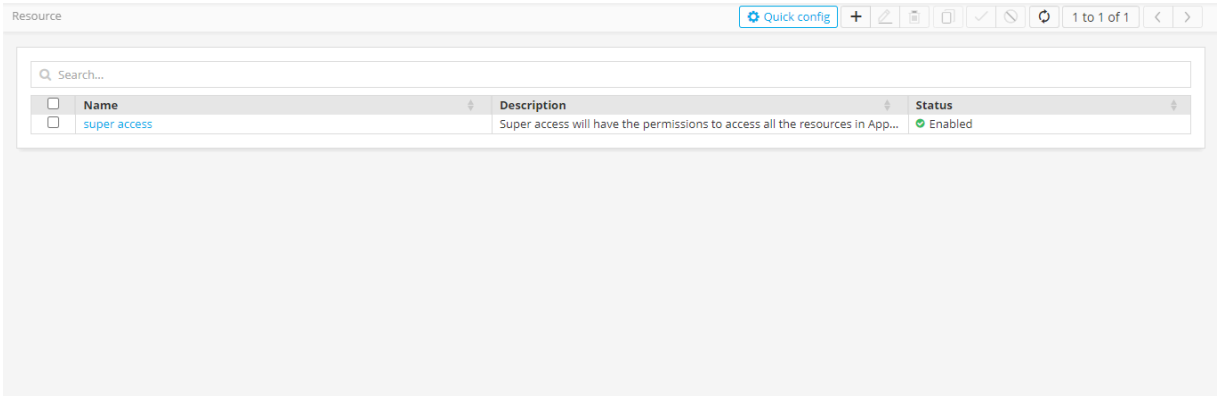
To create a resource,

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.

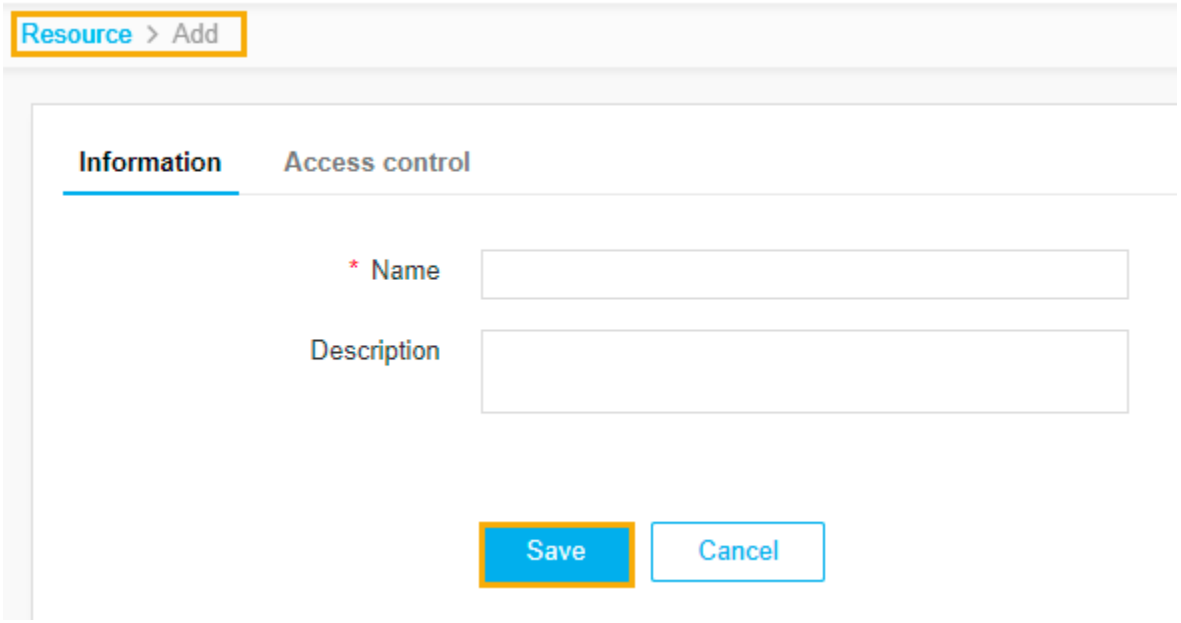
The **Resource** page appears.



4. Click the 

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.

Field	Description
	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

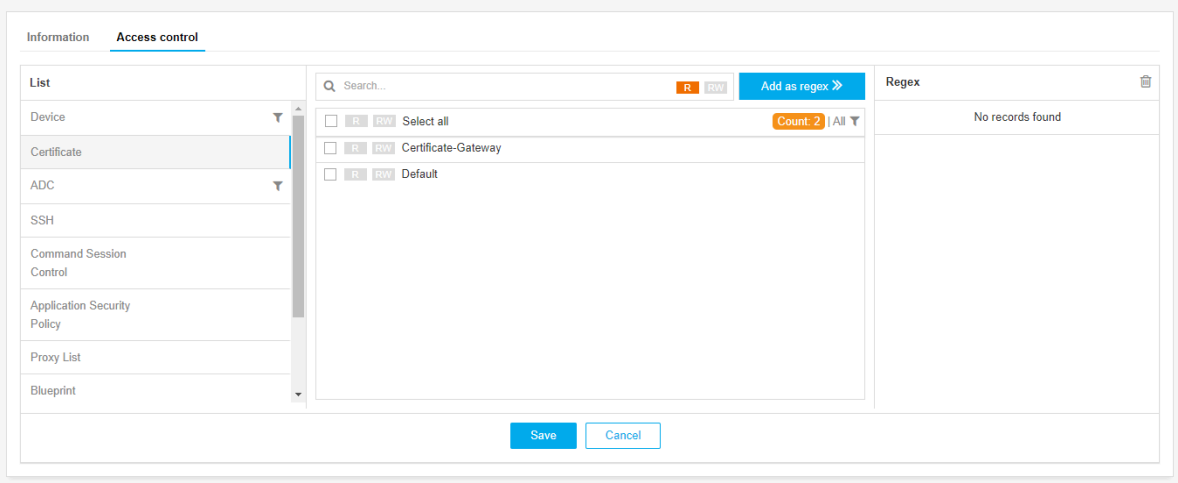
   j. Proxy List

   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:

   a. Click R (Read-only) to assign read-only permissions.

   b. Click RW (Read and Write) to assign read and write permissions.

   c. 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.

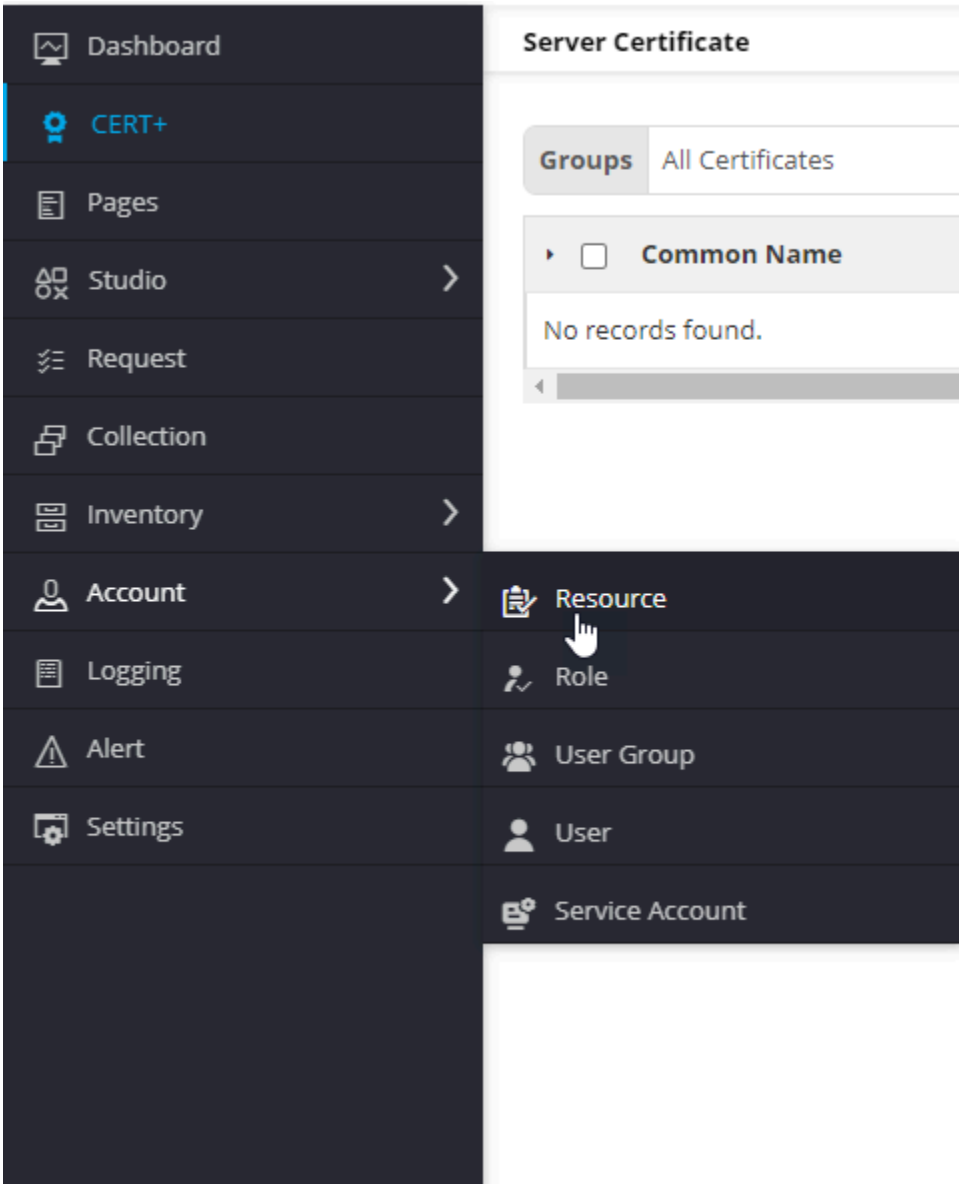
> **Note:** The purpose of the regex is, the search string continues to work in the background and auto-associate all the new certificate groups to the resource when the certificate group matches the regex you created.

11. Click **Save**.

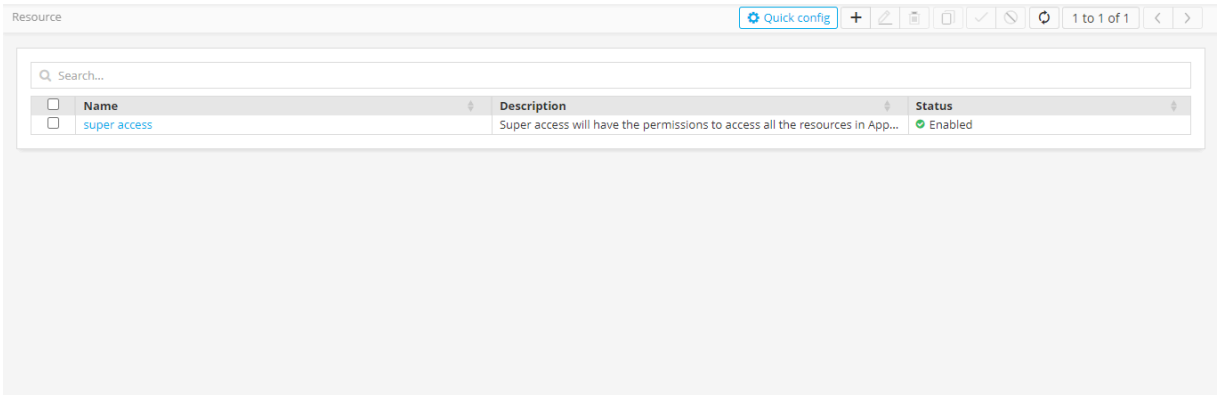
Modify a Resource

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.

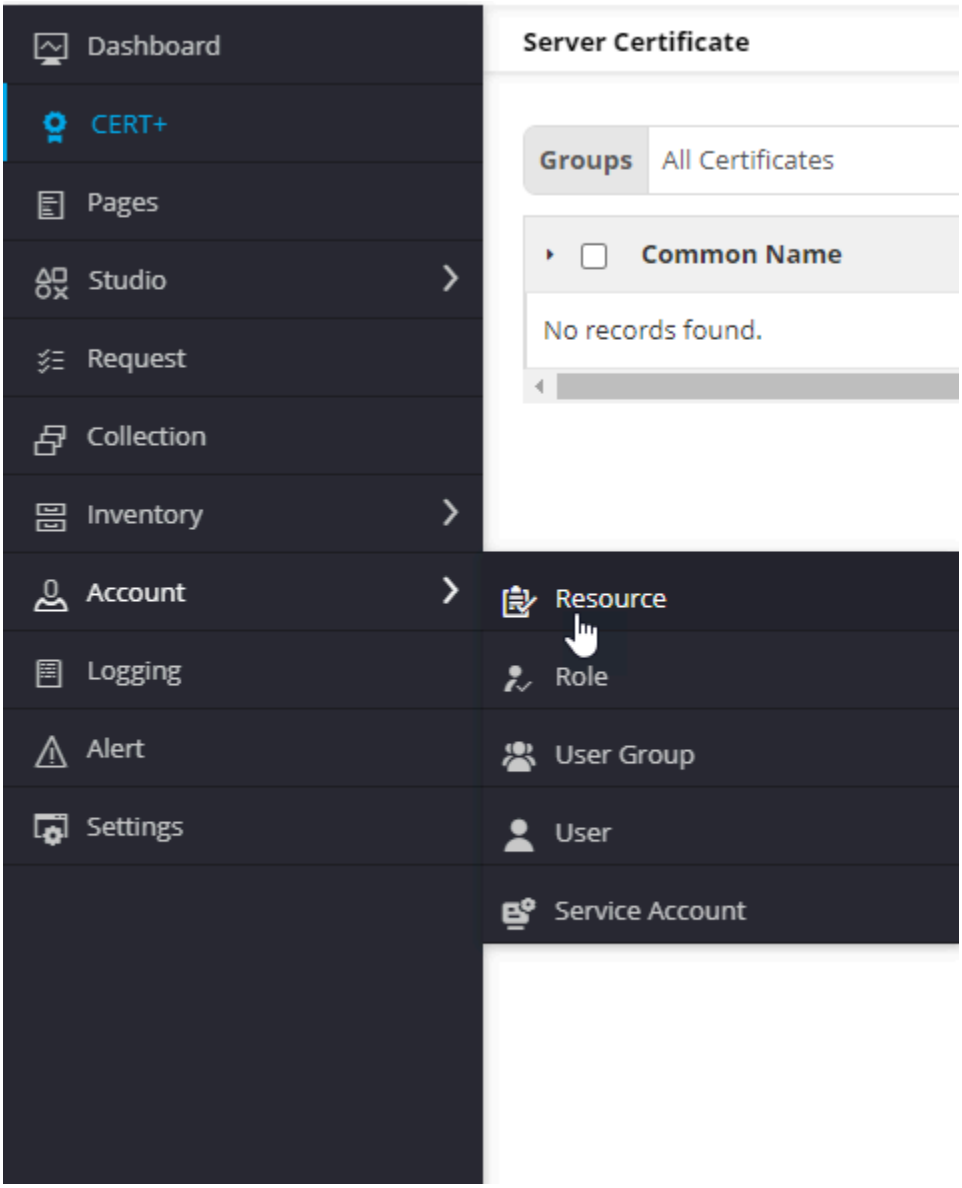
> **Note:** You can also modify Read (R) and Read/Write (RW) permissions for the certificate groups associated with a resource.

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.

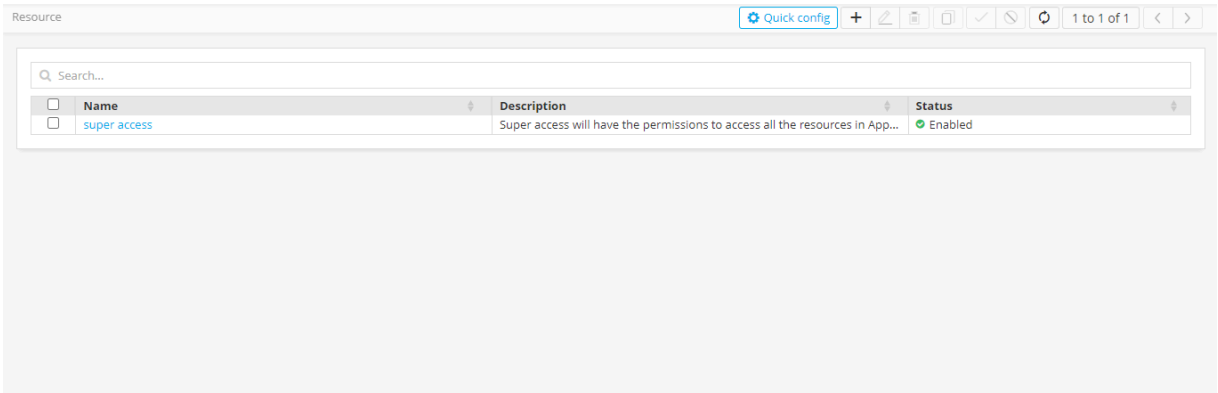
Delete a Resource

To delete a resource,

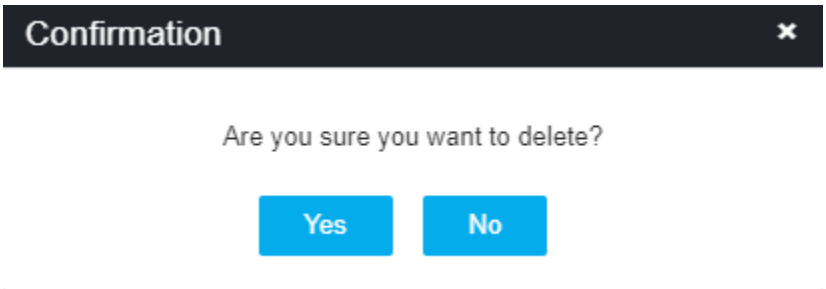
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Navigate to **Account**, and then click **Resource** from the list.



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.



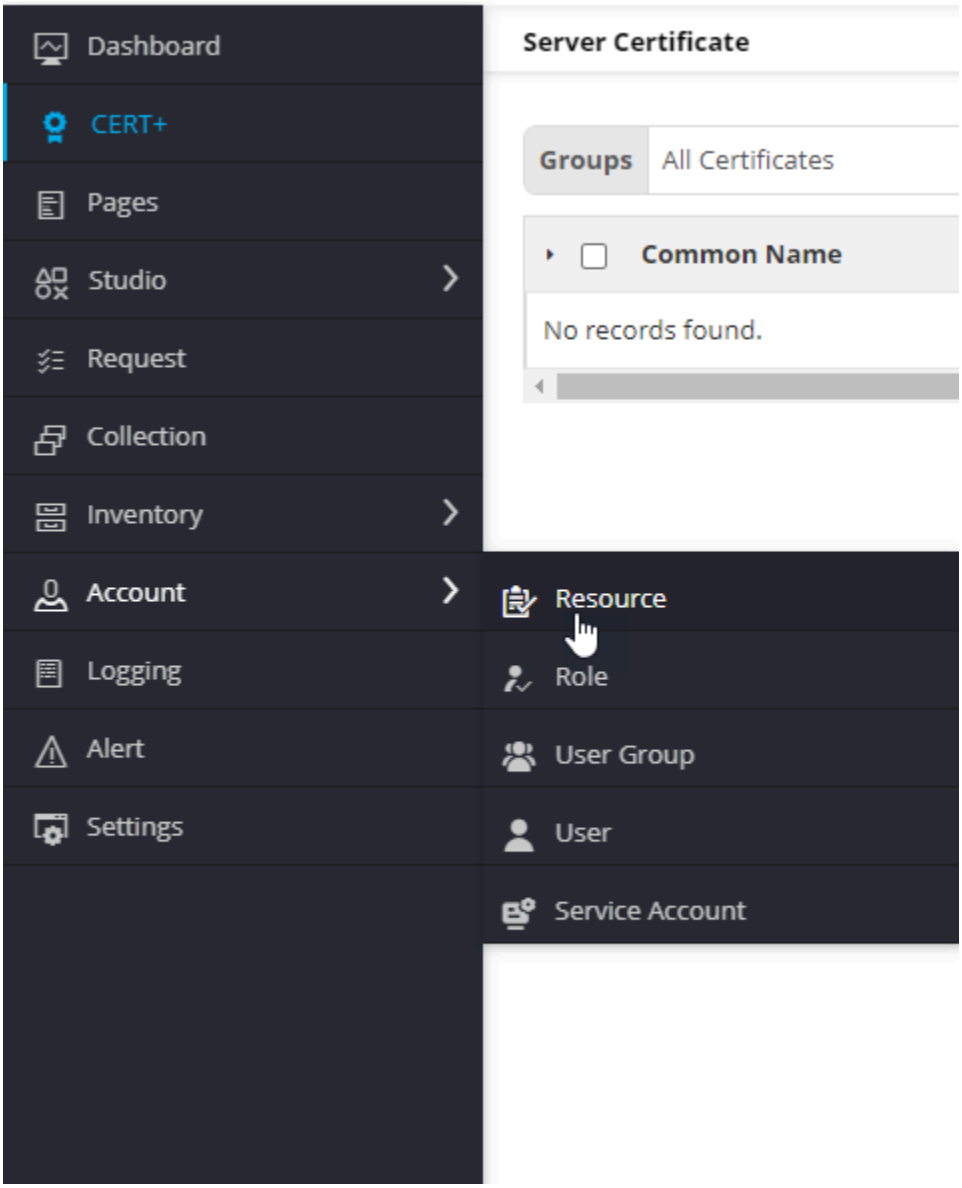
7. Click **Save.** The resource is deleted and a pop-up message displays as **Operation performed successfully**.

Clone a Resource

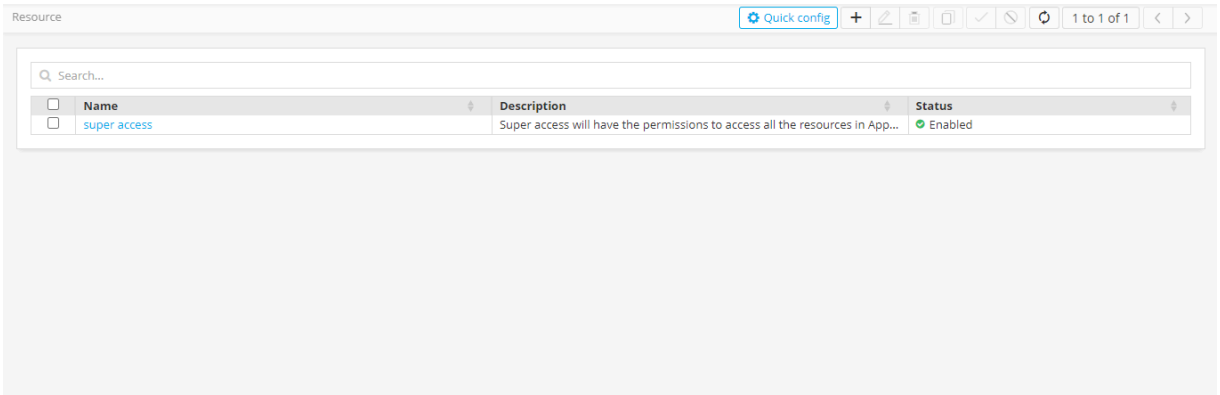
Clone allows you to create an exact copy of an existing resource with all the access control permissions.

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.

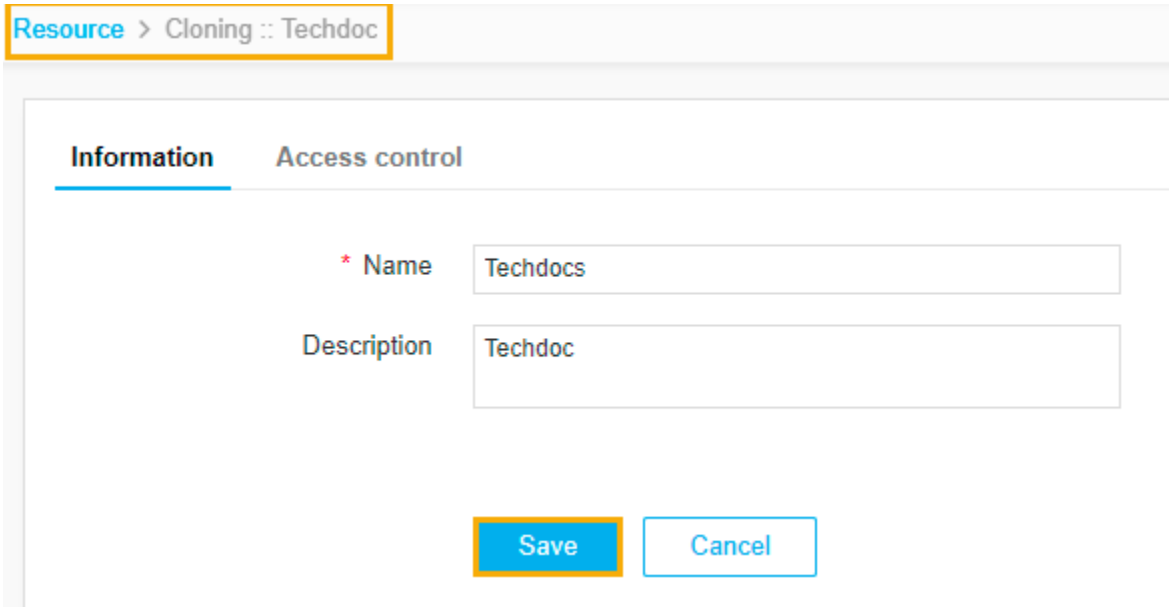


The **Resource** page appears.



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.

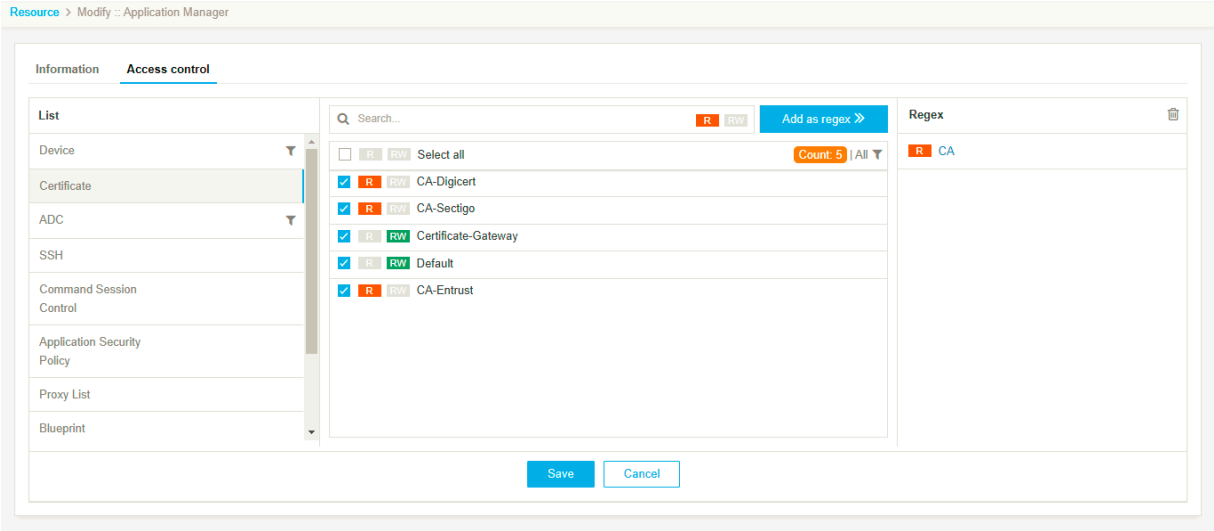


6. The following table describes the options available on the Cloning page:

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**.

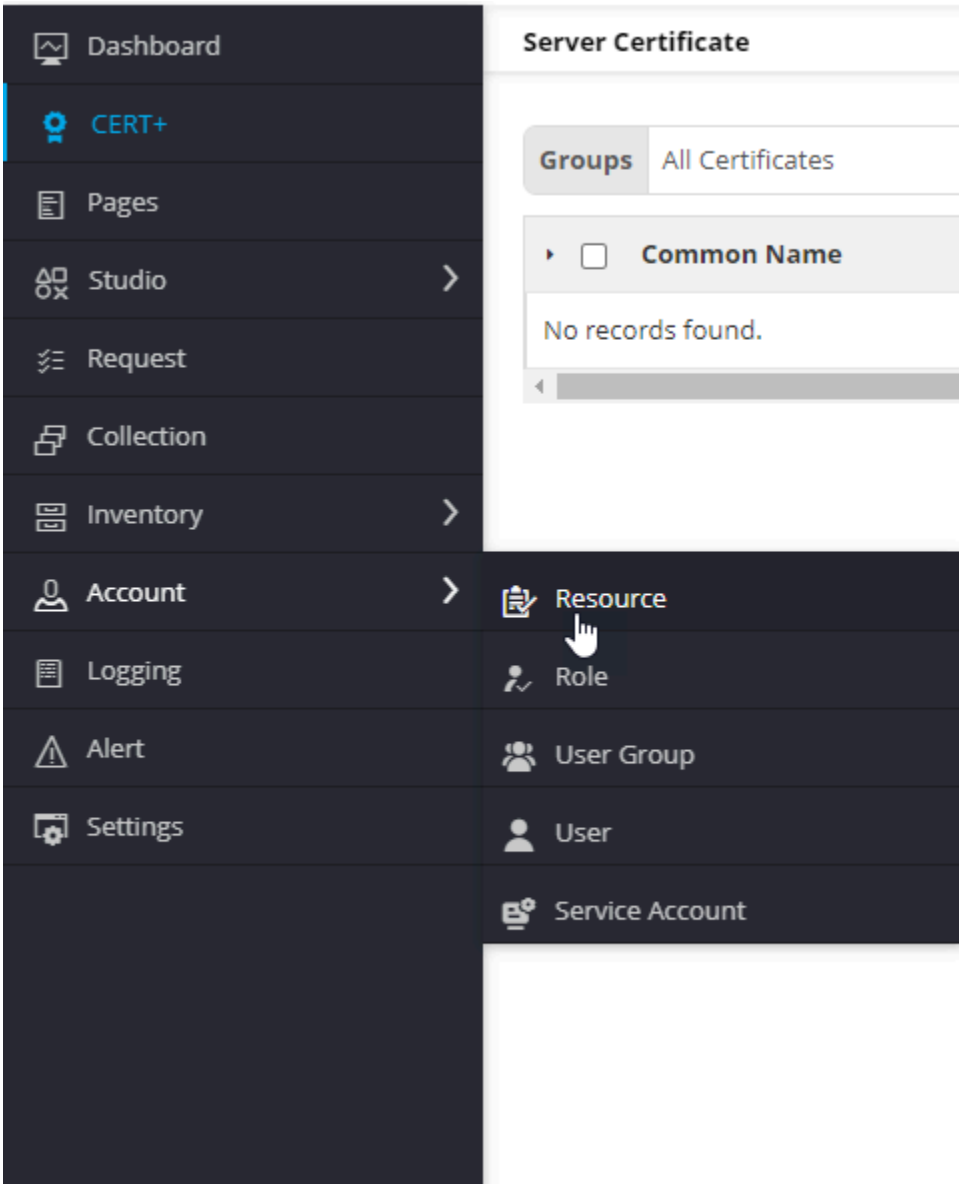
   The resource is cloned and a pop-up message displays as **Resources has been cloned successfully**.



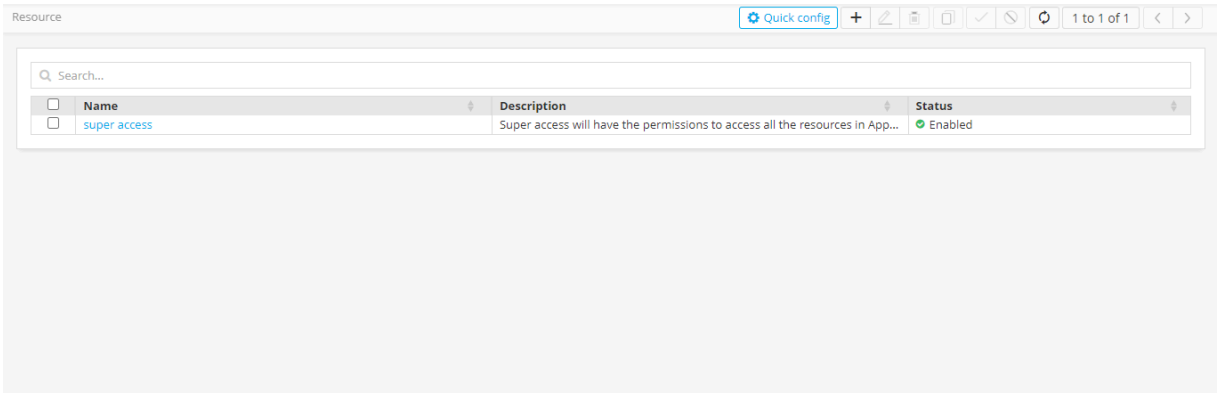
Enable a Resource

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.

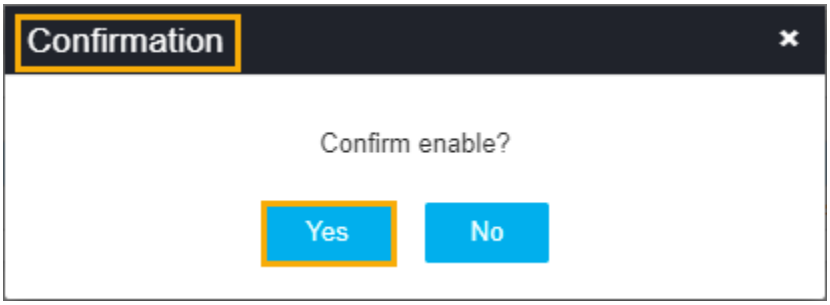


The **Resource** page appears.



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

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



7. Click **Yes**.

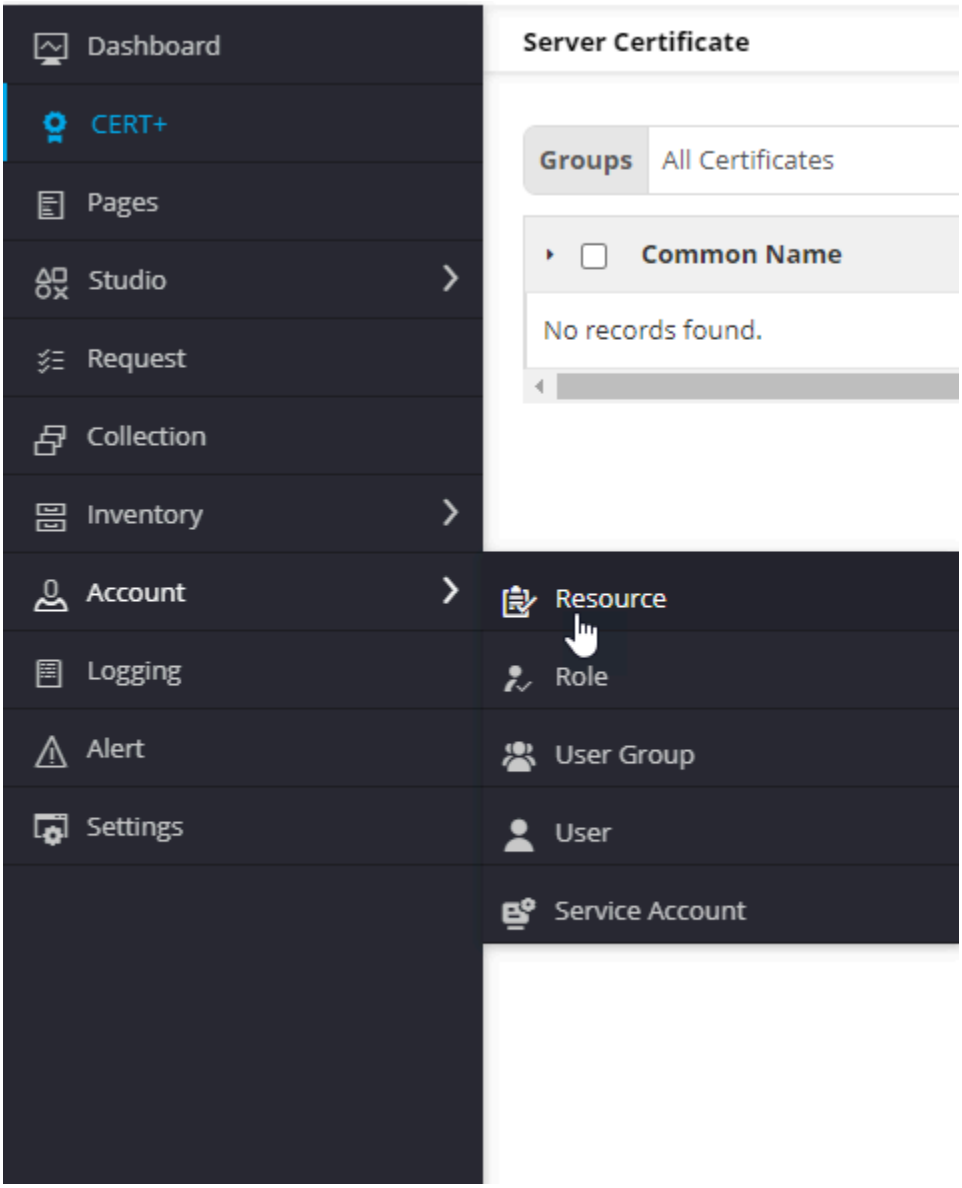
   The resource is enabled and a confirmation message displays as **Operation performed successfully**.

Disable a Resource

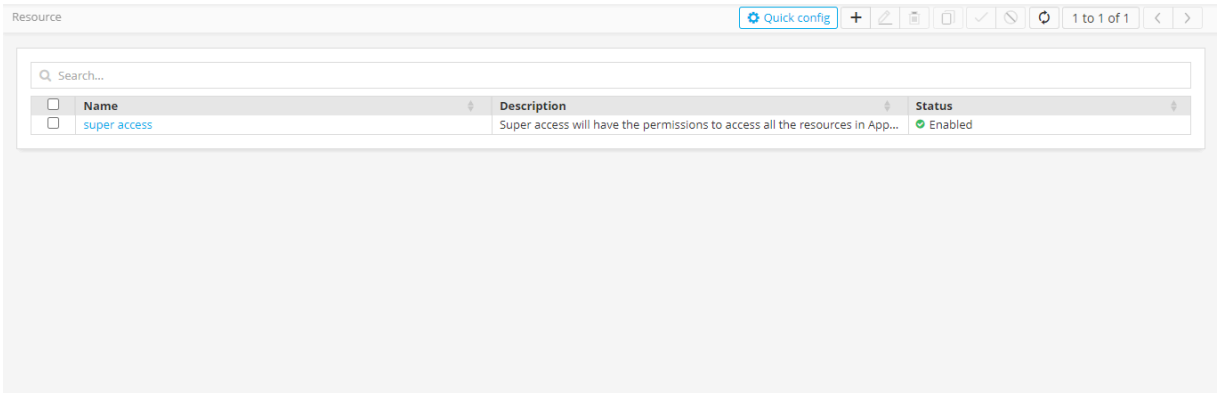
To disable a resource,

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.

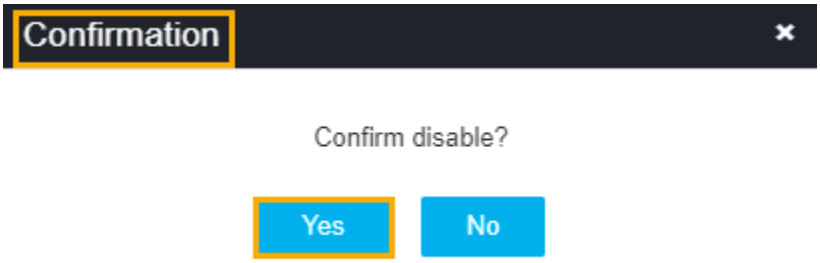


The Resource page appears.



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

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

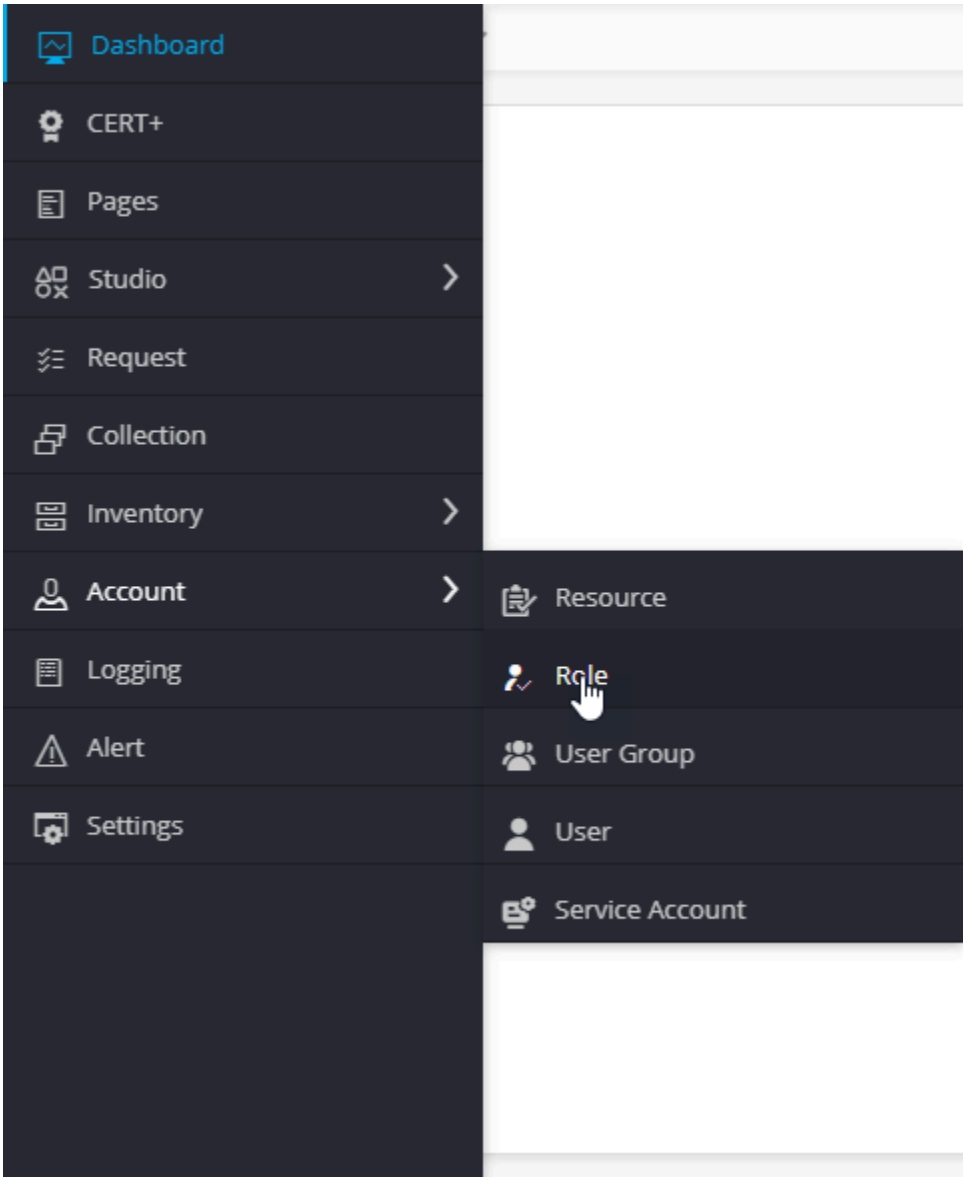
Overview

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.

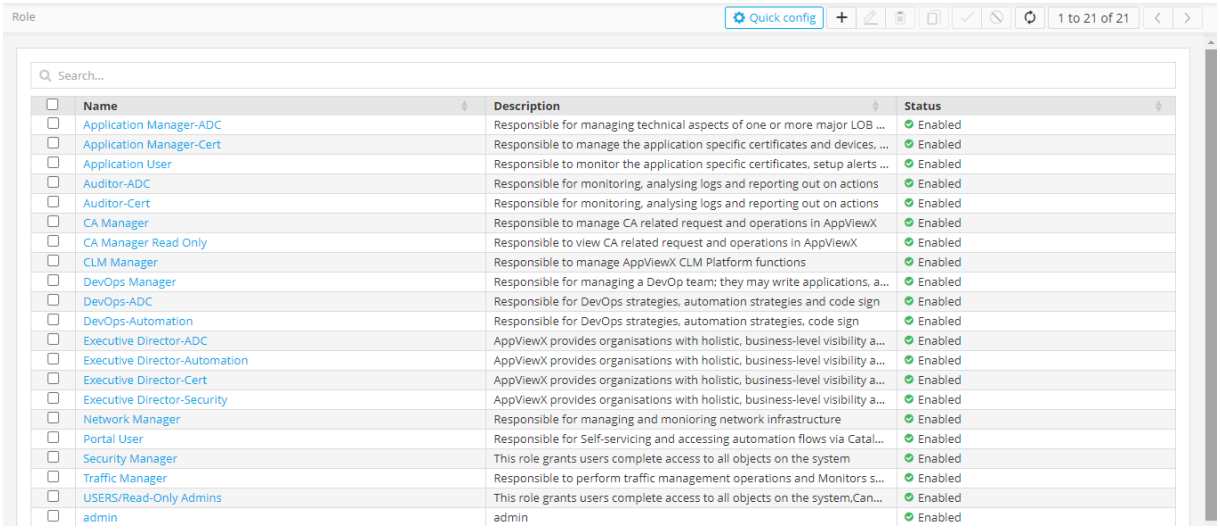
Create a Role

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.



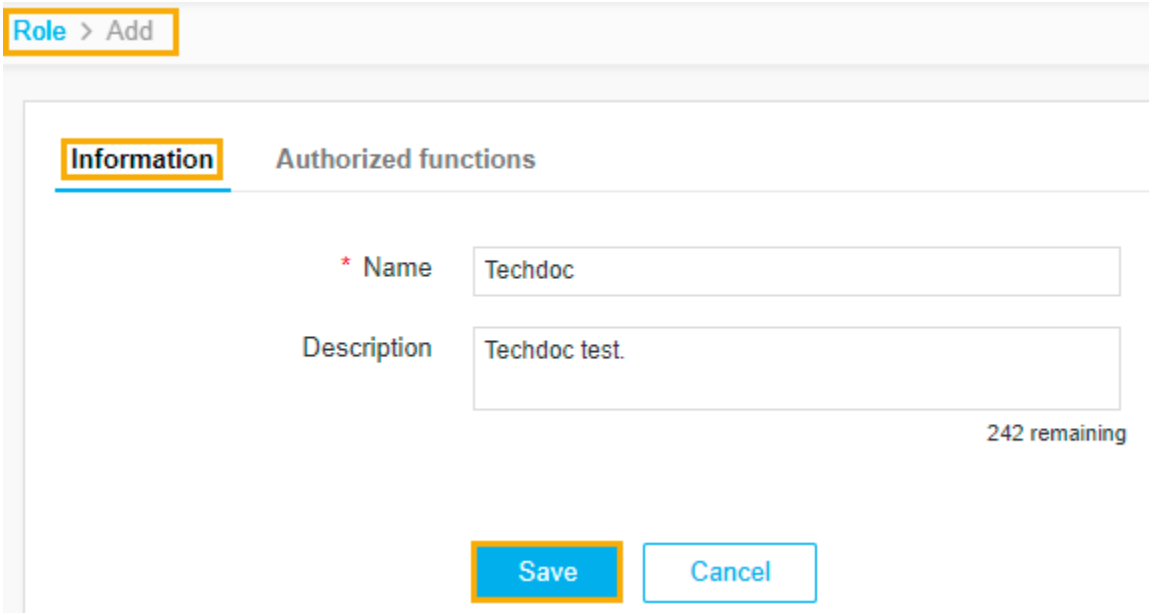
The **Role** page appears.



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.

Field	Description
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.

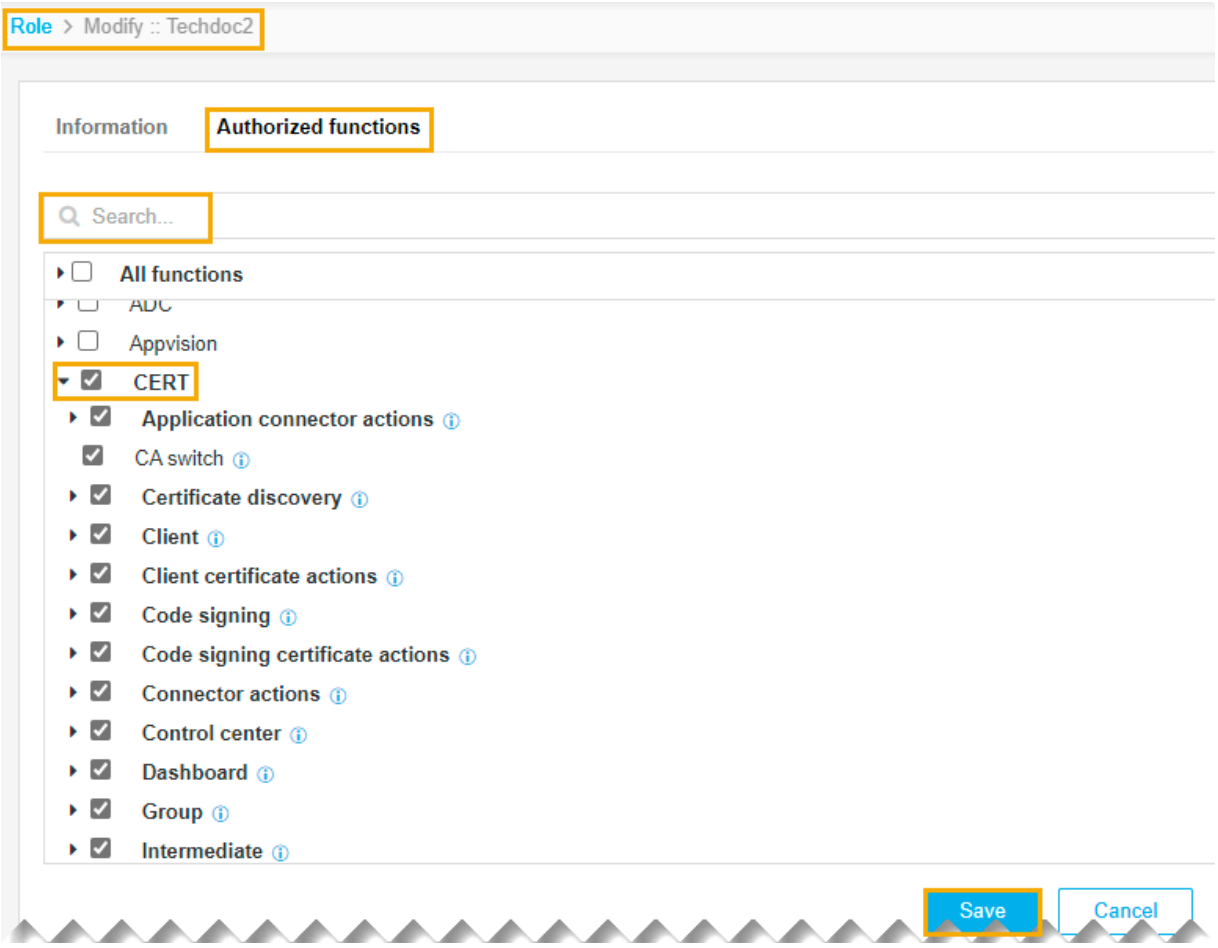
Note: The asterisk (*) symbol indicates a mandatory field.

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:

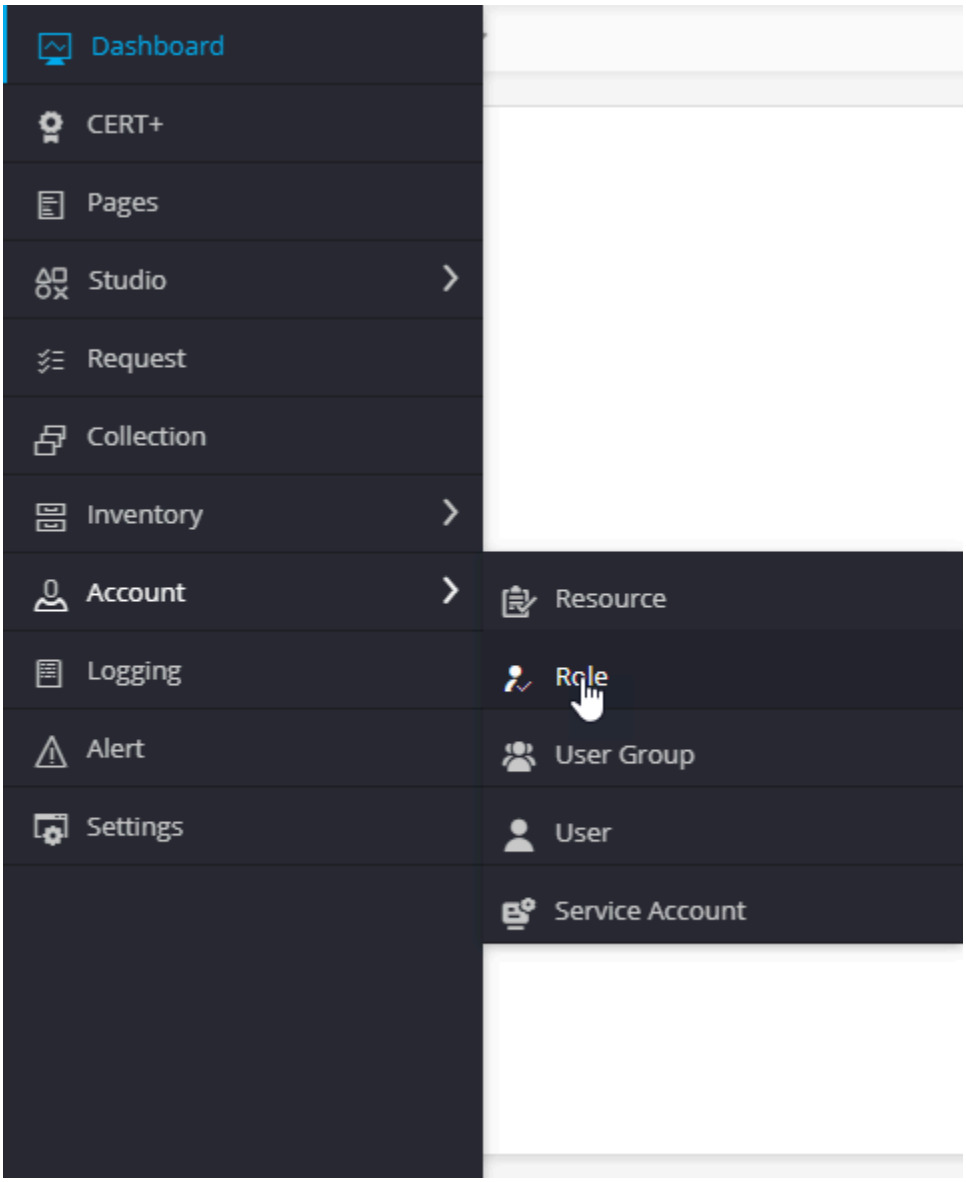
a. Click the expand icon beside a function check box.
b. Select the individual sub-options within that function.
c. You can select **CERT**, which automatically assigns all sub-options or you can expand the **CERT** function and select only the sub-options you want to assign.

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**.

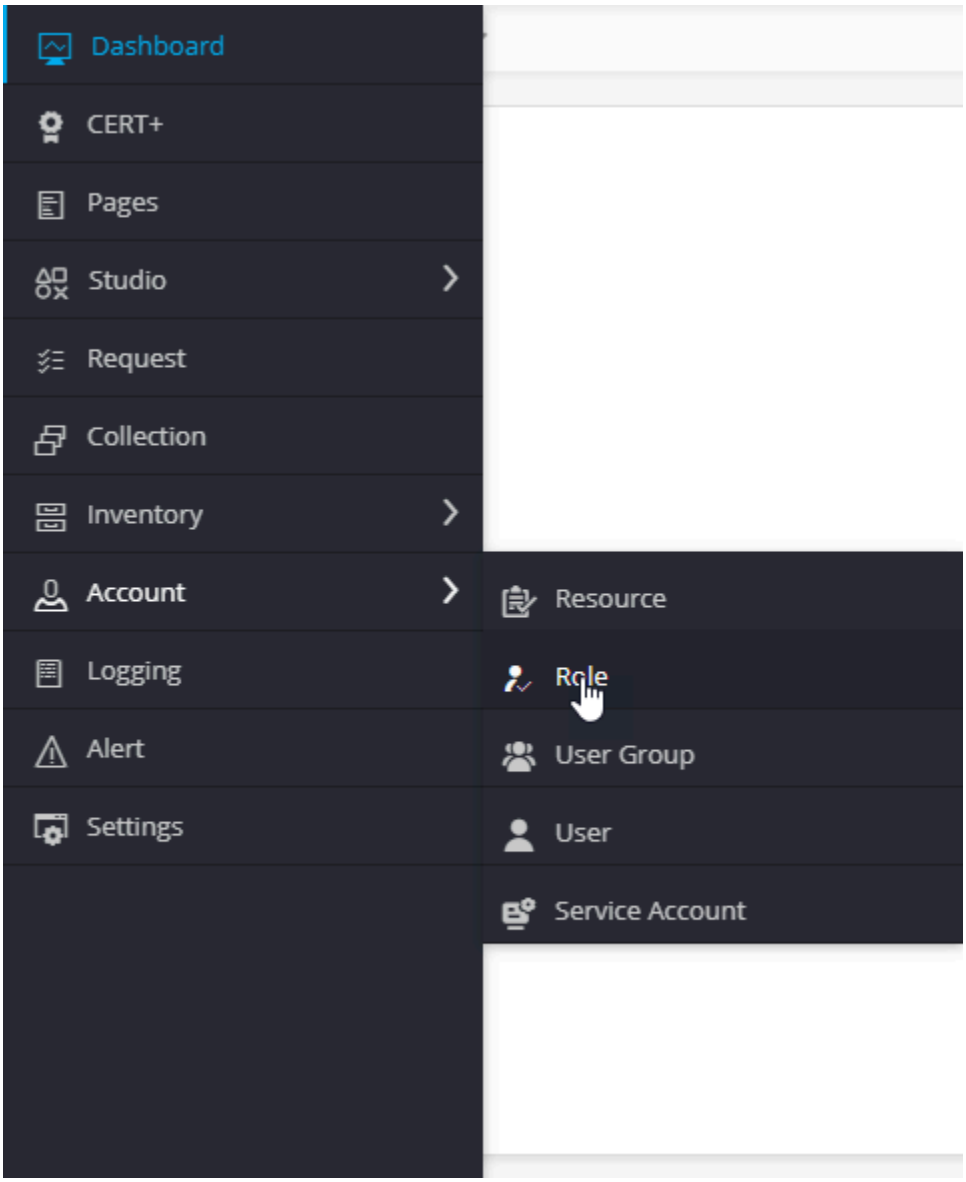
> **Note:** Fields that are grayed out, such as the Name field on the Information tab, cannot be edited.

Delete a Role

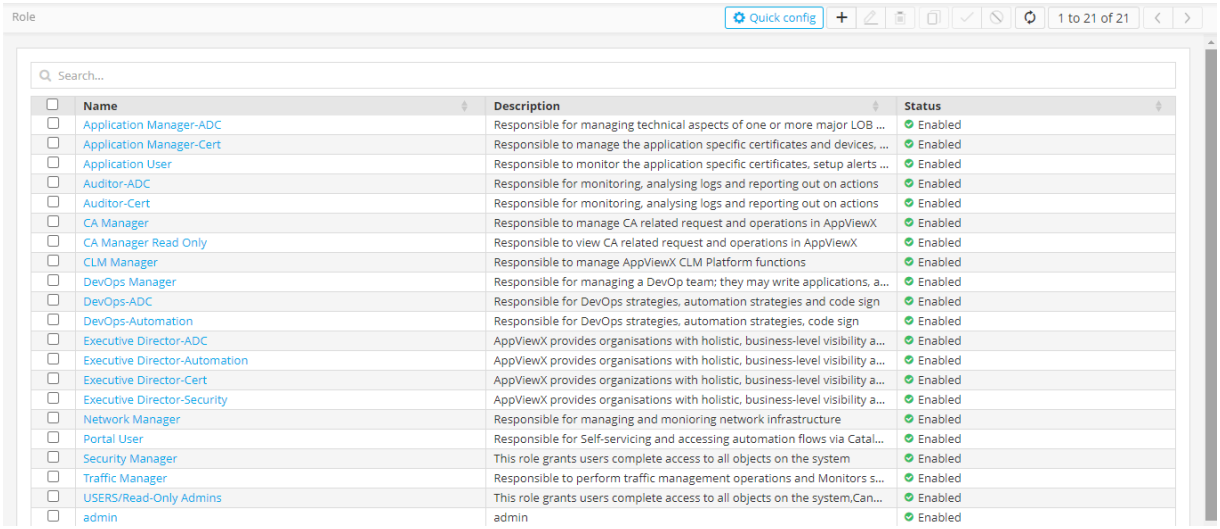
> **Note:** A role that has active users belonging to it cannot be deleted.

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.



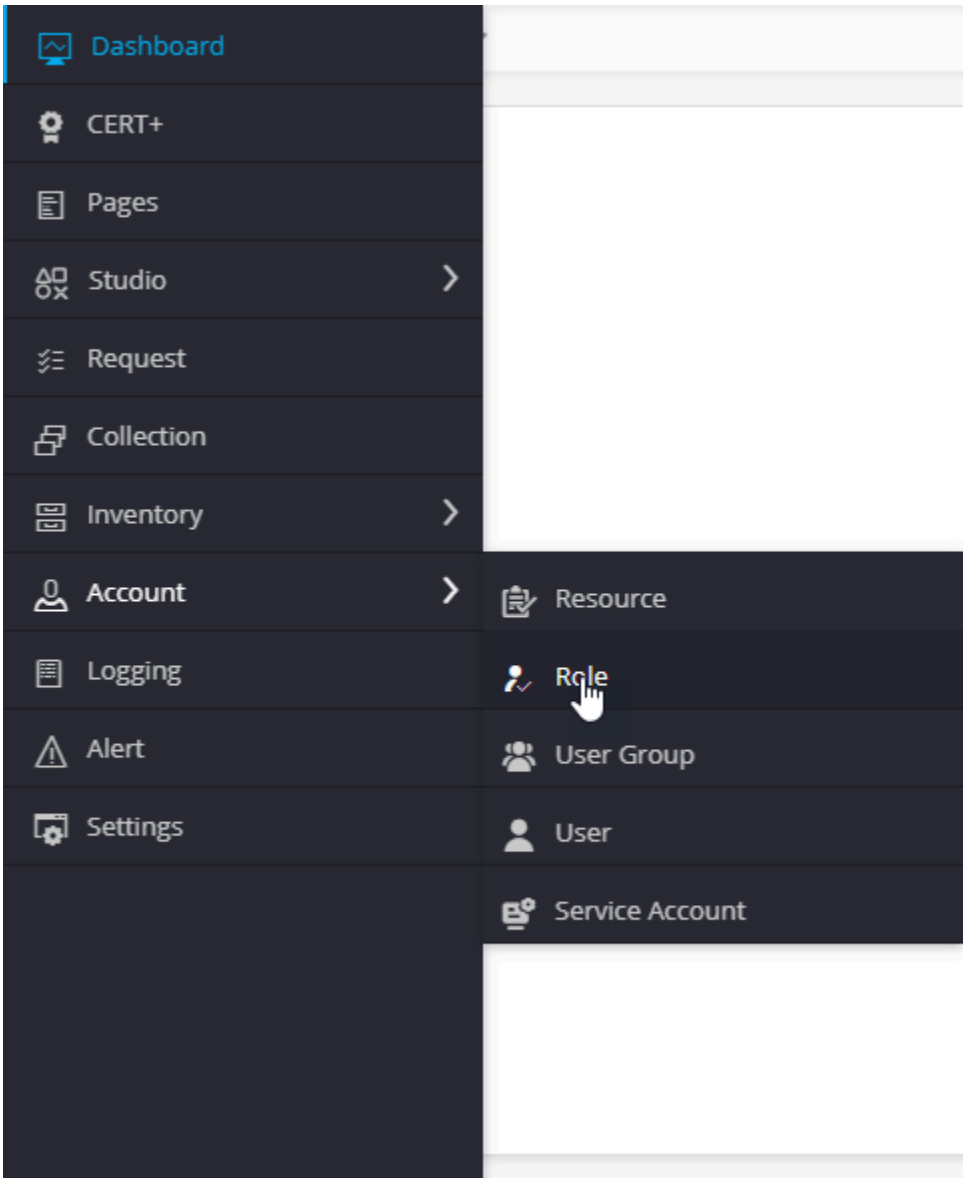
4. In the Roles list, select the check box beside the role you want to delete.
5. Click the  icon in the command bar to delete the role.
   The confirmation pop-up window appears.
6. Click **Yes**.
   The pop-up message appears as Operation performed successfully.

Clone a Role

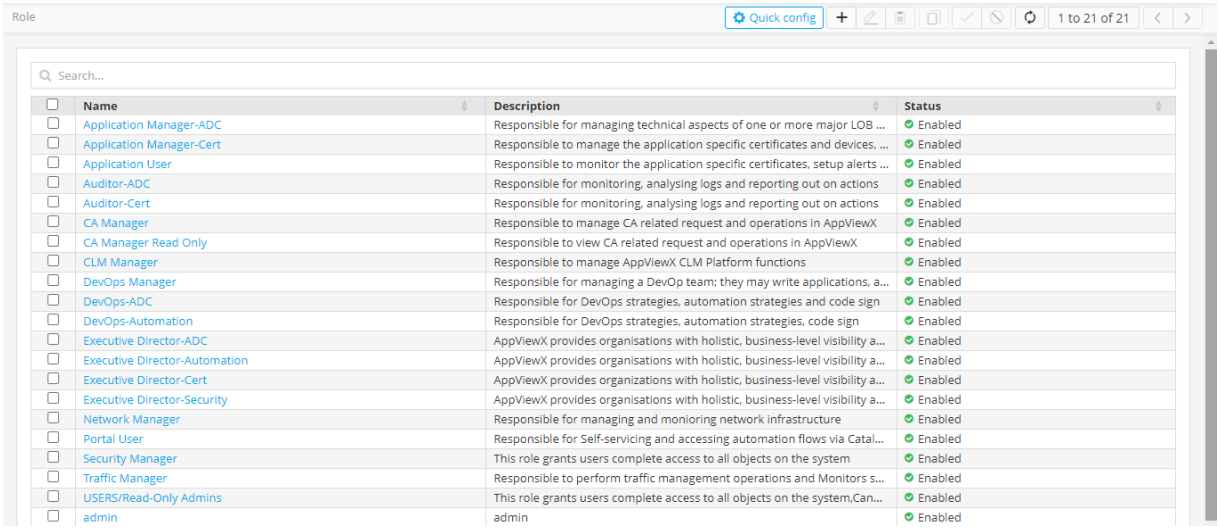
The Clone a role option allows you to create an exact copy of an existing role with a different name. The user can modify the permissions and tasks that can be performed while cloning a role.

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.

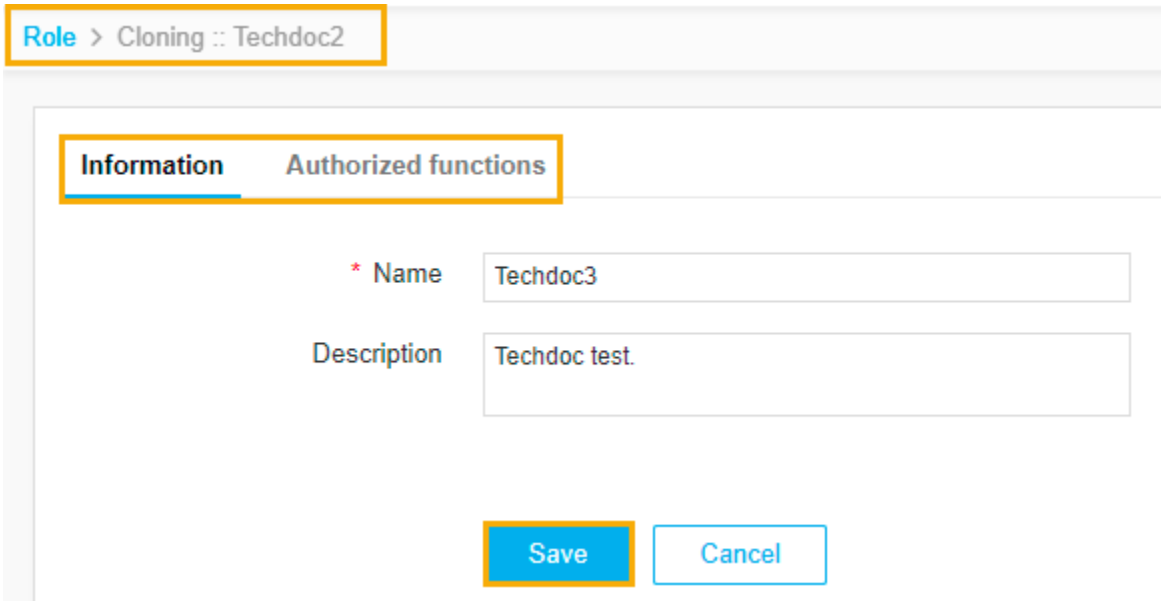


The **Role** page appears.



4. In the Roles list, select the check box beside the role you want to clone.
5. Click the  **icon** in the command bar to clone the role.

   The selected Cloning page appears.



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

Field	Description
* **Name**	Enter the name of the resource.

Field	Description
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**.

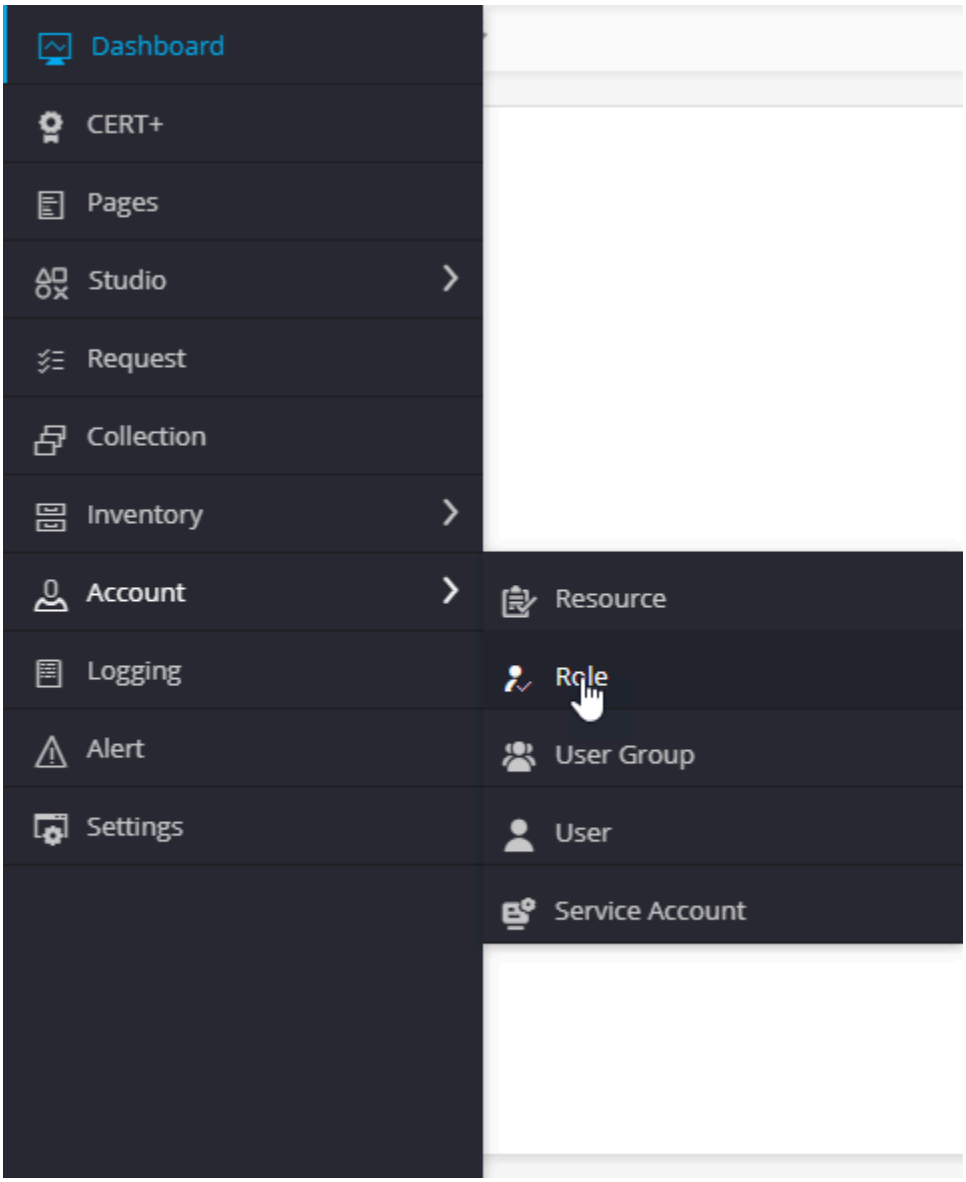
   The role is cloned and a pop-up message displays as **Role has been cloned successfully**.

Enable a Role

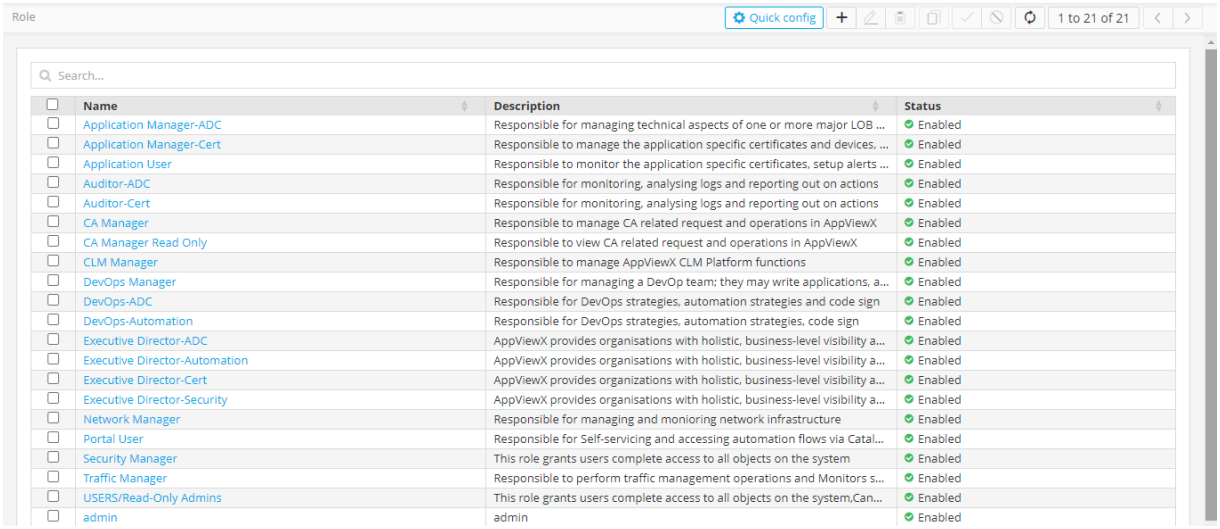
To enable a role,

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.

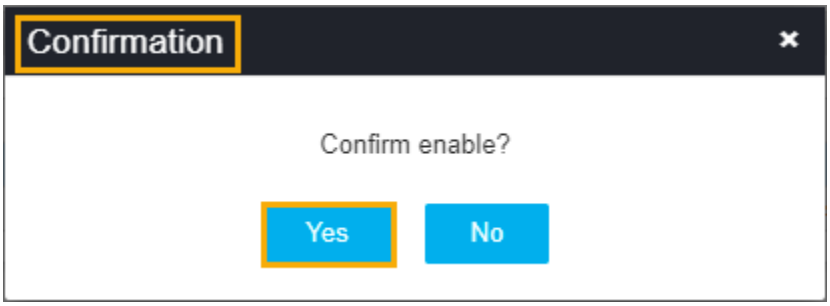


The **Role** page appears.



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

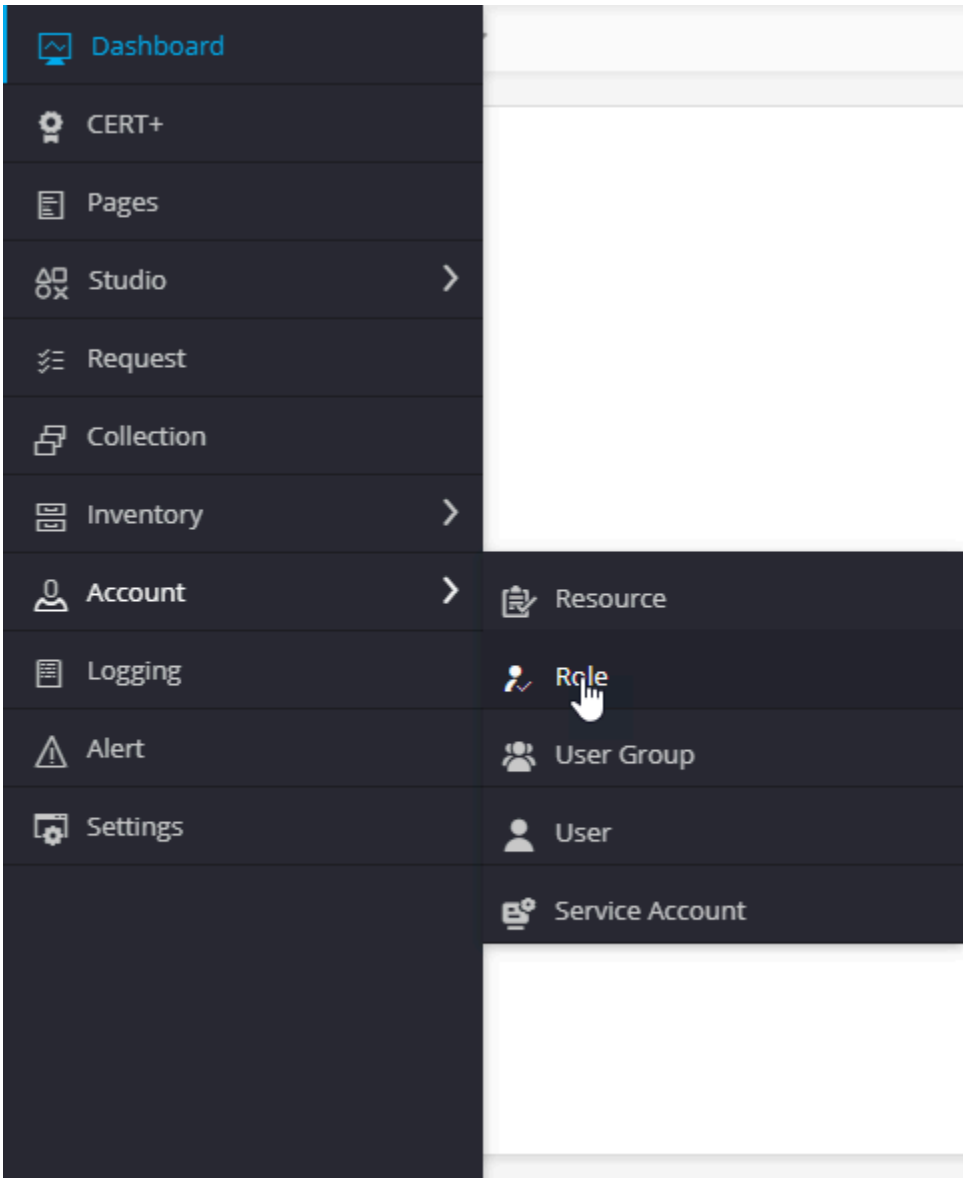
You cannot disable a role that has active users in it. The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role,

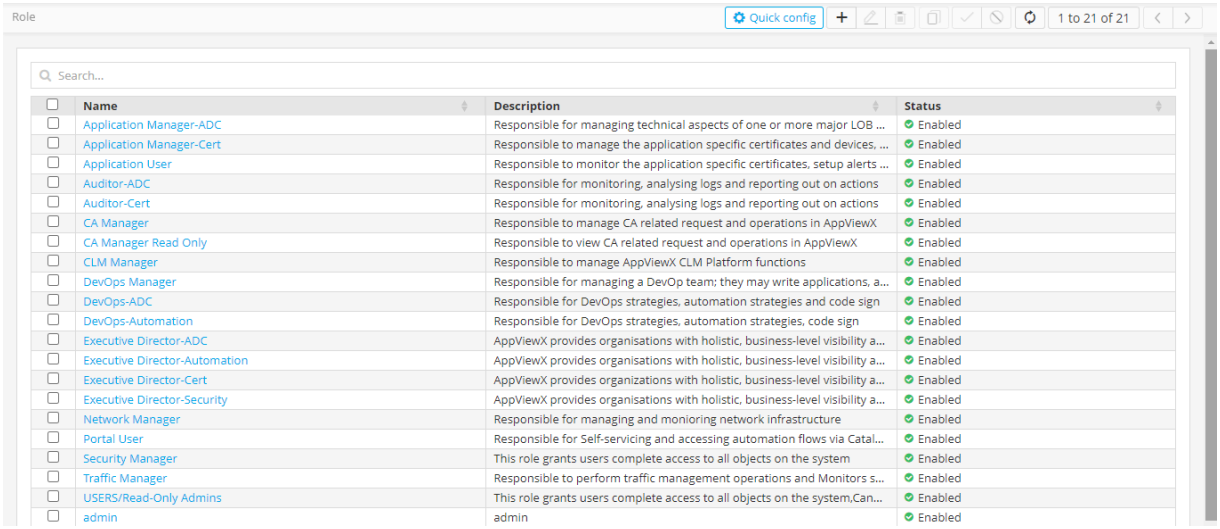
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

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

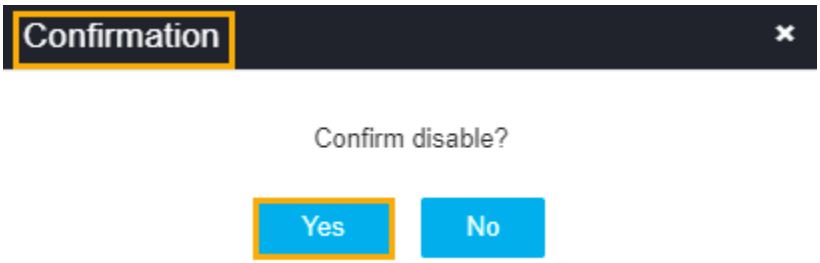


The **Role** page appears.



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

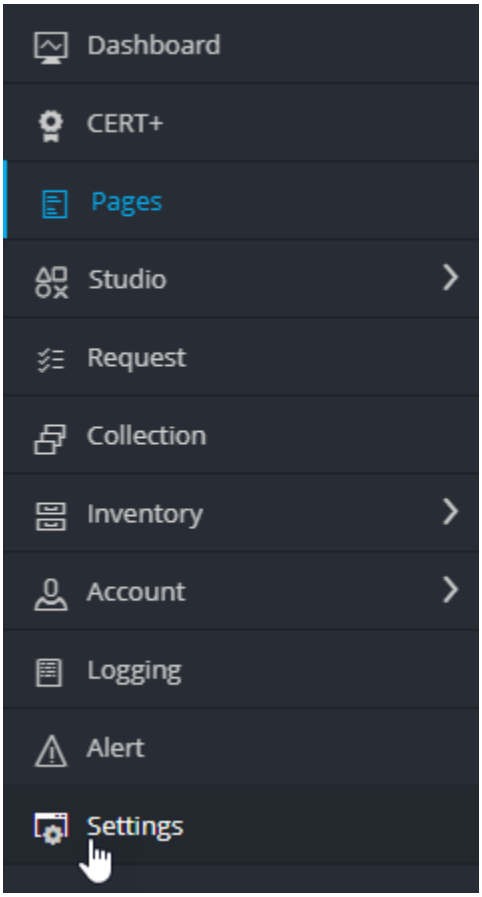
When the Admin enables the Birthright role feature, all new users who log into the product will be provided with a pre-defined set of customizable functions.

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.

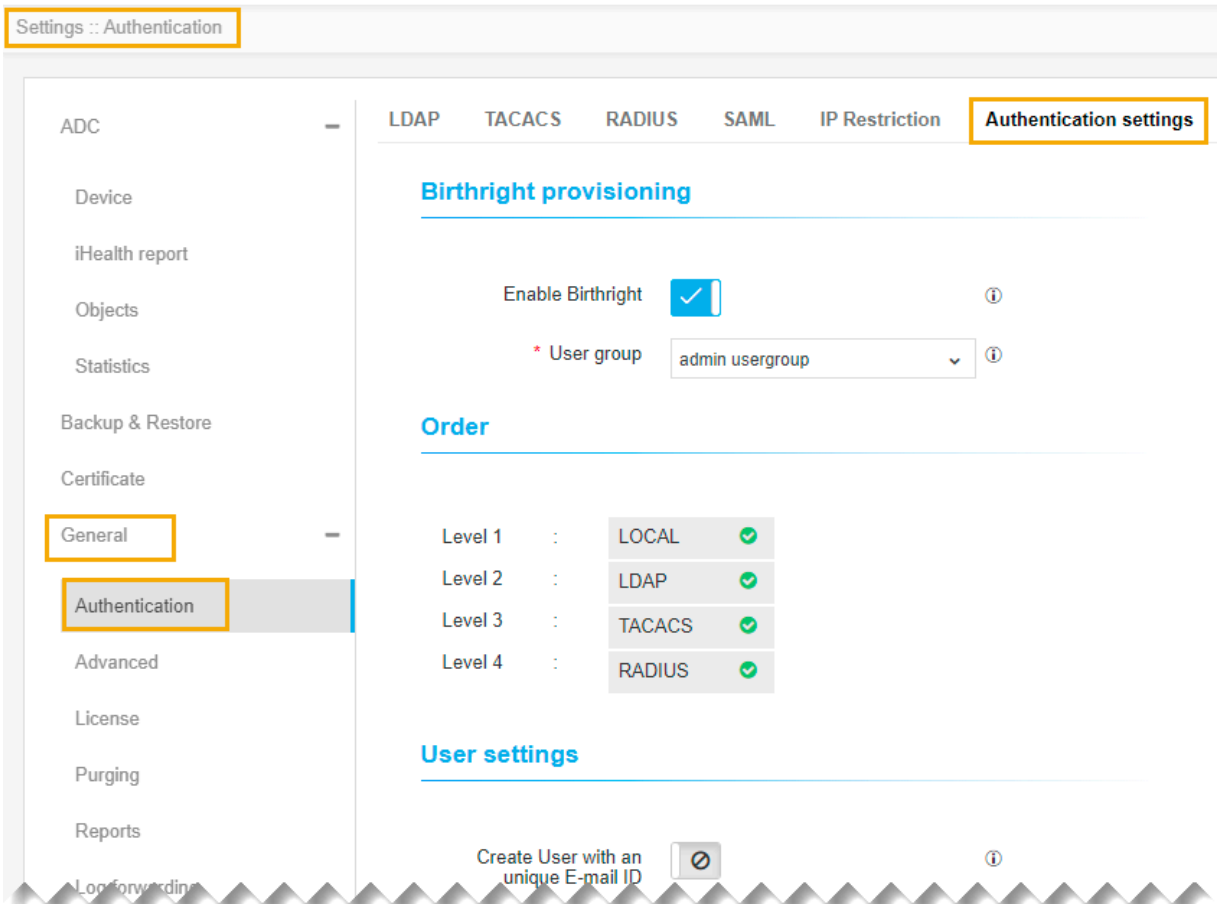
Whenever a new user logs in, the user will be mapped with roles and resources specified in that particular user group.

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 (associated with the user group), enable the **Enable Birthright** toggle key. • * **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: **Options** / **Description** **Create a User with a unique E-mail ID** – Enable the toggle key, to ensure that all the users have a unique email ID.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Create User on Authorization Failure</td><td>Enable the toggle key, to create a user even if authorization fails but authenticated successfully.</td></tr>
<tr><td>Session Timeout</td><td>Allows users to set the idle web session timeout limit between 2 to 480 minutes.
Note: The idle web session timeout is calculated in minutes.</td></tr>
</table>
</td></tr>
<tr><td>Node settings</td><td>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. Restart the avx-config-server pod in every data center.</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

7. Click **Save**.

User Group

Overview

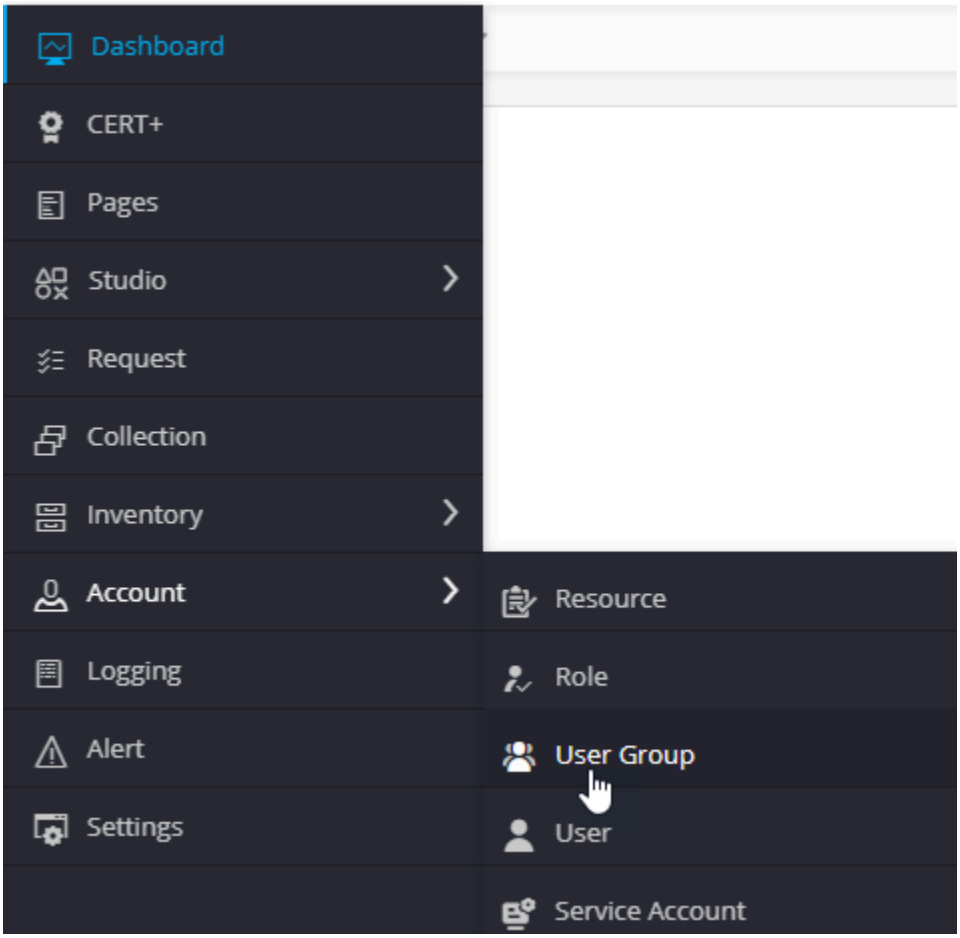
A user group is a group of individuals that have access to the same roles and resources. When you associate a role and resource with a user group, the users within that user group are granted all of the role's and resource's corresponding privileges and permissions.

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

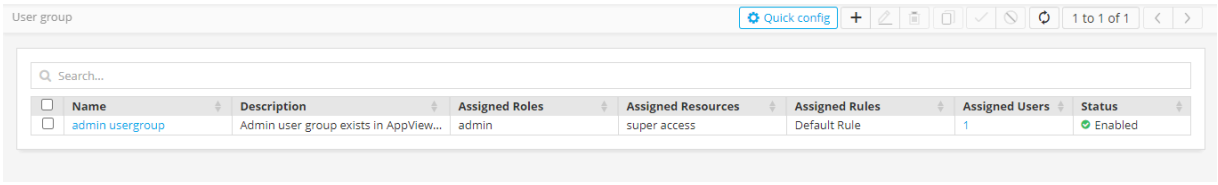
Create a User Group

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.



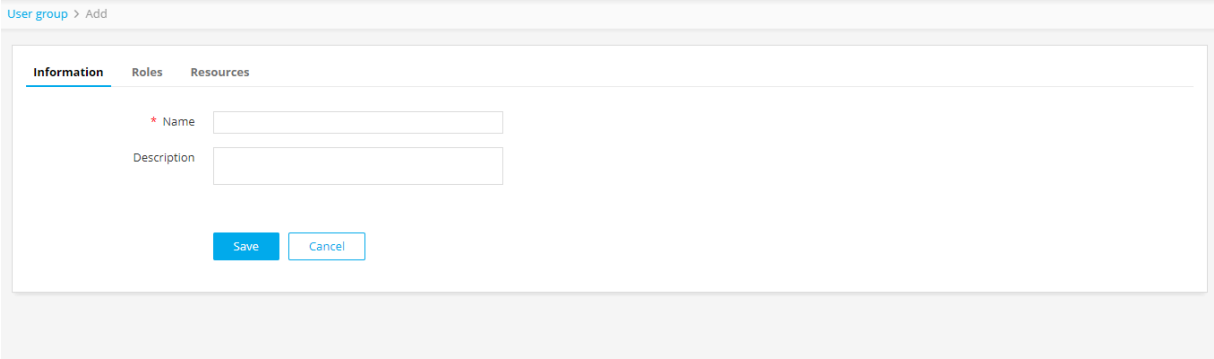
The **User Group** page appears.



4. Click the 

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

   The **Add** page appears.



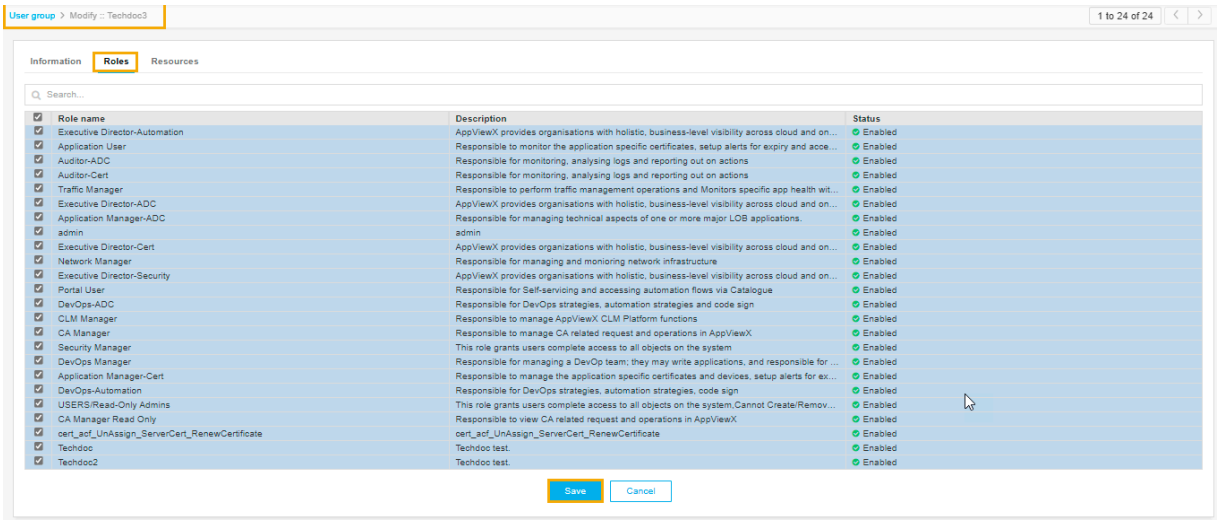
   The following table describes the options available on the User Group page:

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**.

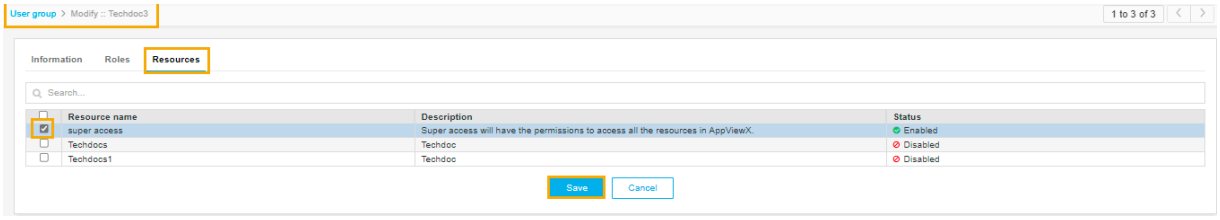
   The pop-up message appears as **the User group added successfully. Please associate the roles and resources to perform the concerned operations**.

6. Click the **Roles** tab.



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.



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.

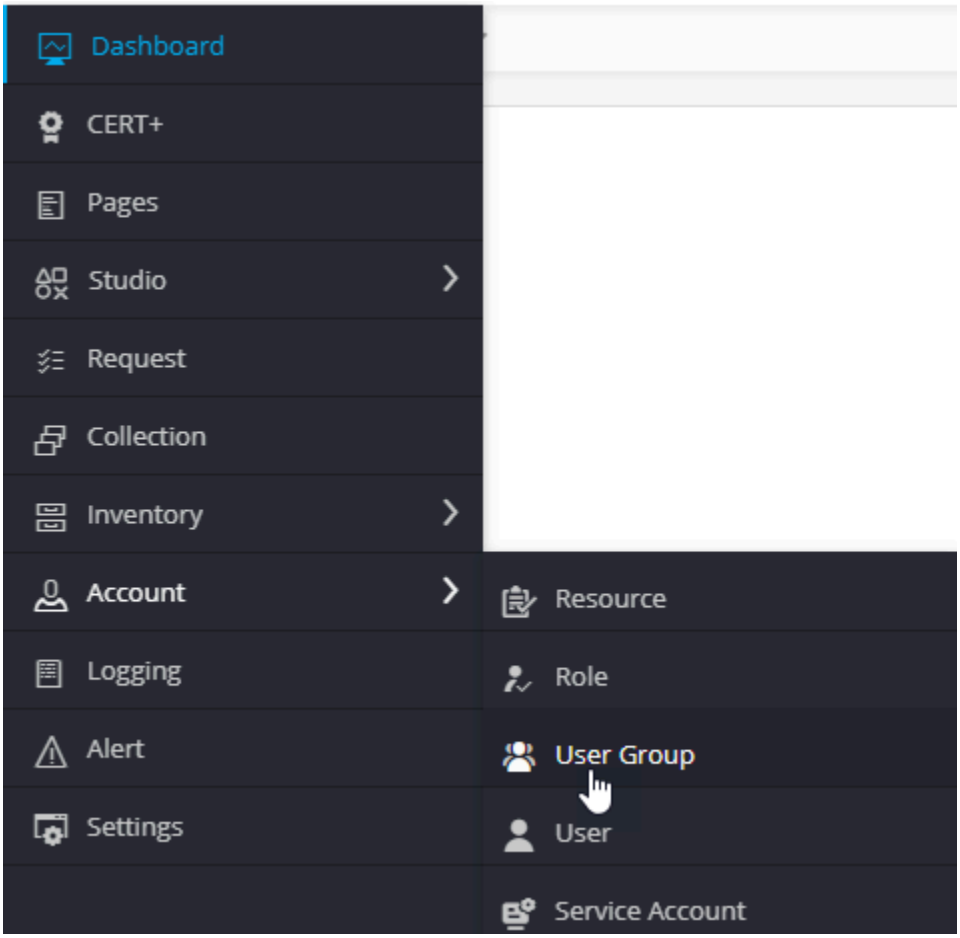
11. Click **Save**.

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

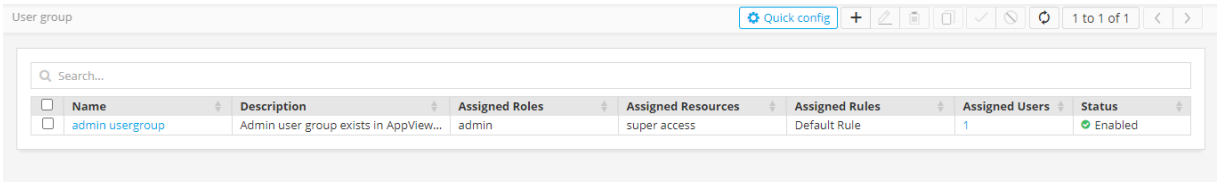
Modify a User Group

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.

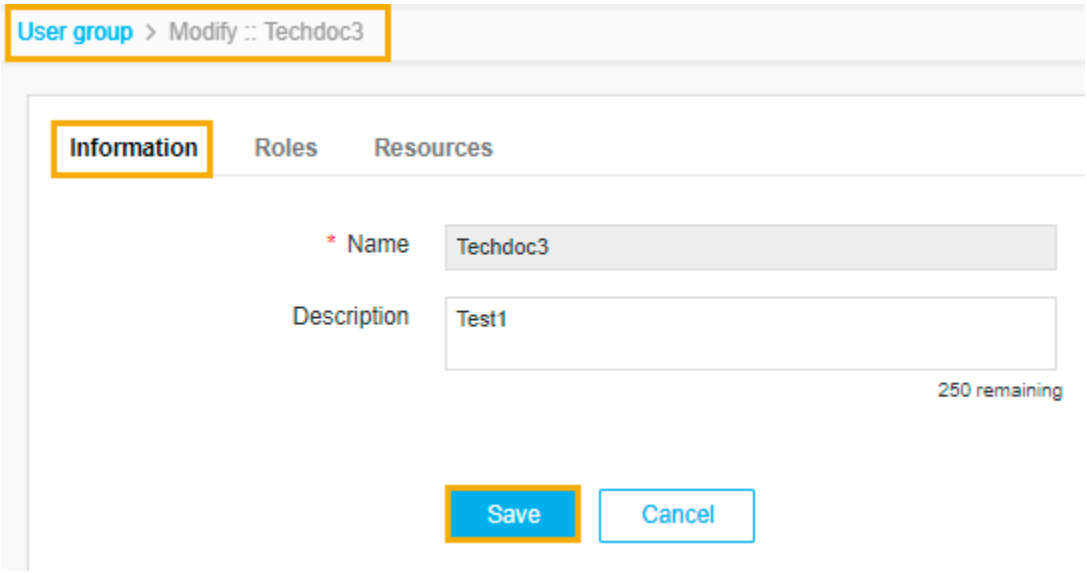


The **User Group** page appears.



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

   The **Modify** page appears.



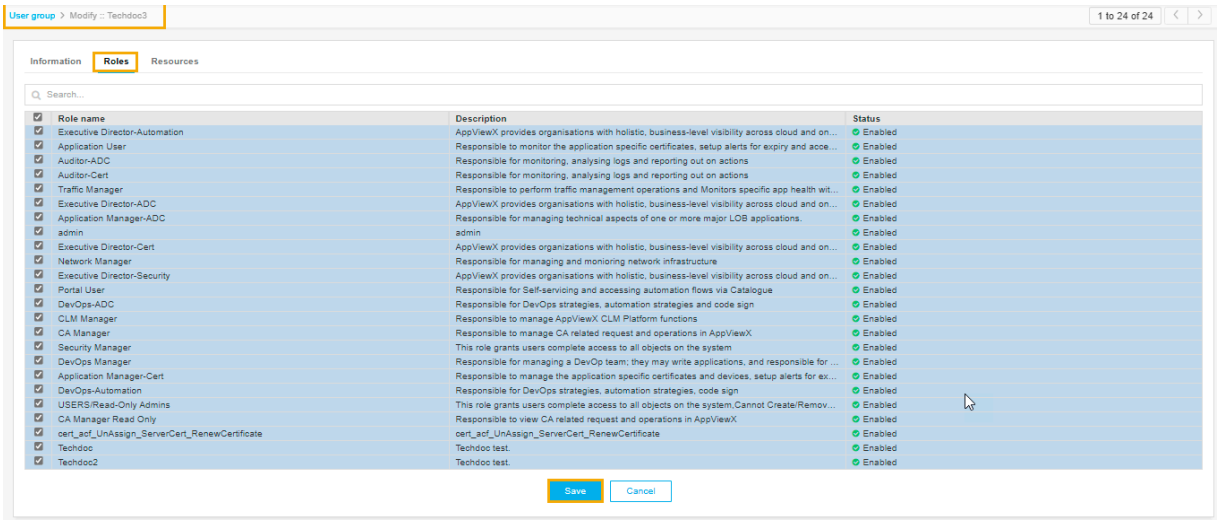
   The following table describes the options available on the User Group page:

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

5. Click **Save**.

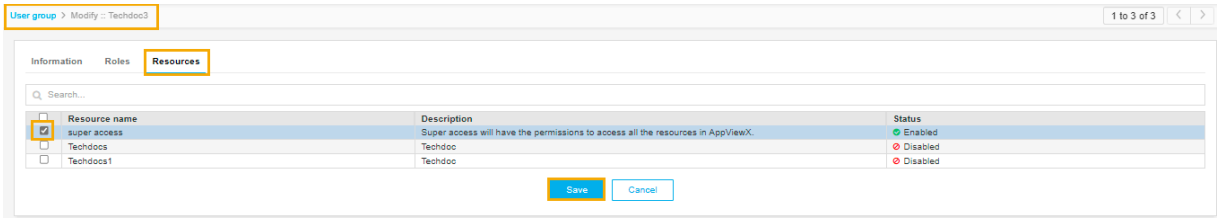
   The pop-up message appears as **User group information updated successfully.**

6. Click the **Roles** tab.



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.



10. Select additional resources or unselect existing resources for the User group.
11. Click **Save**.

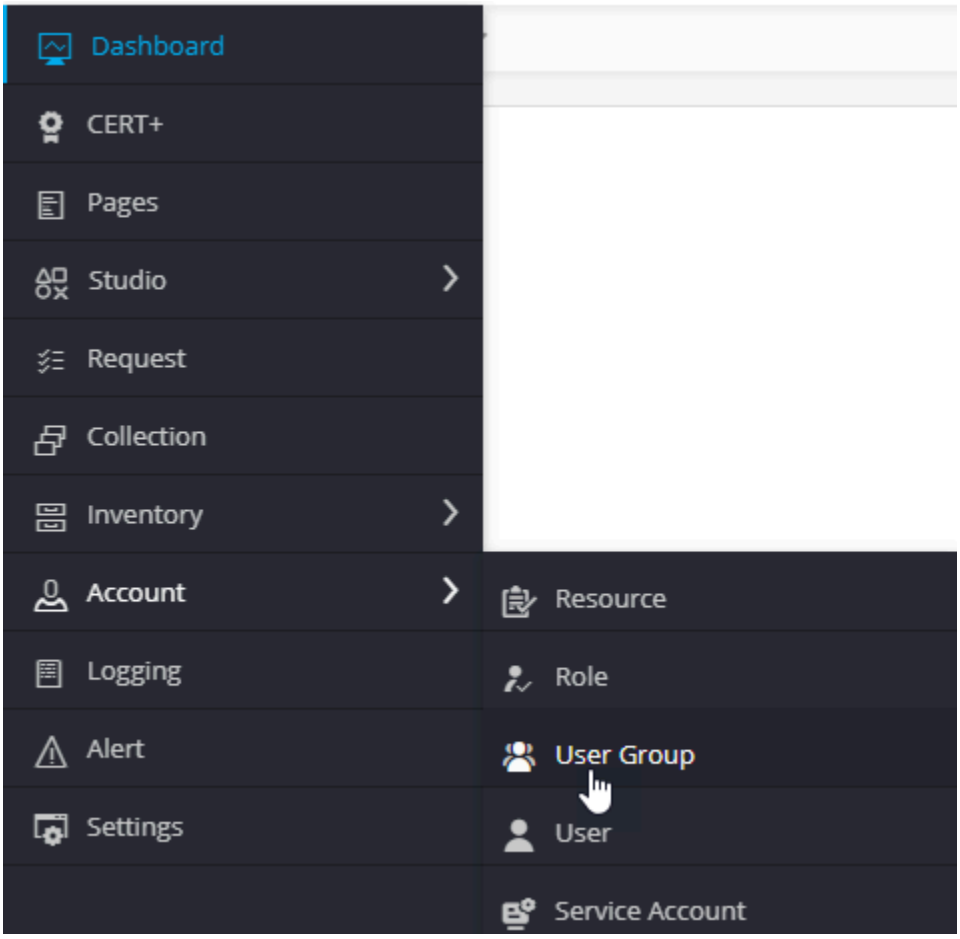
    The pop-up message appears as **Operation performed successfully**.

Delete a User Group

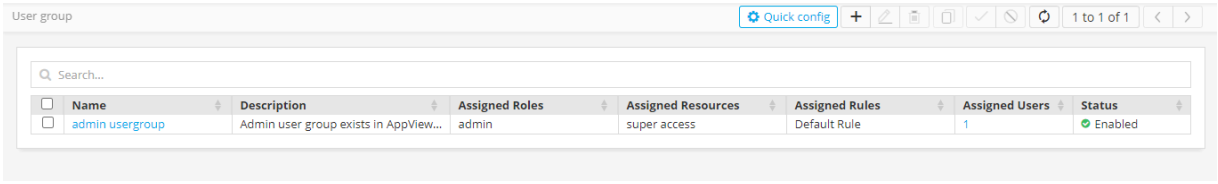
To delete a user group,

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.



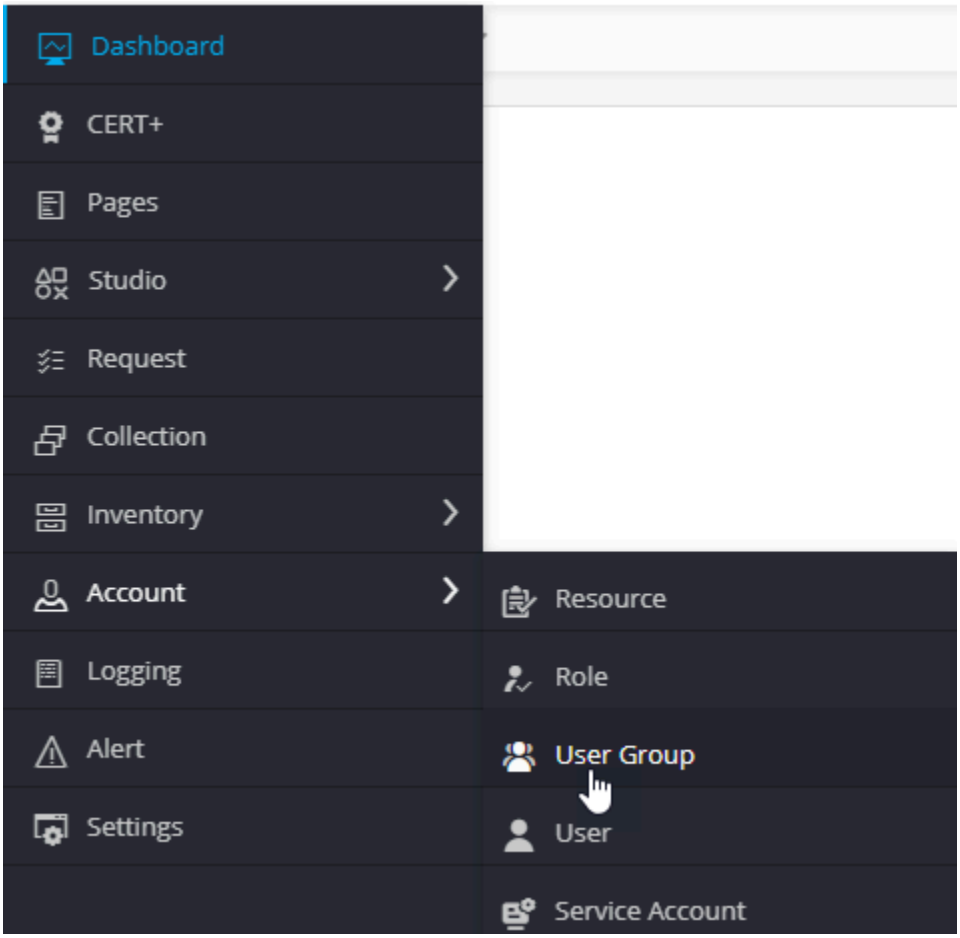
4. In the **User Group** list, select the check box beside the role you want to delete.
5. Click the  icon in the command bar to delete the User Group.
   The confirmation pop-up window appears.
6. Click **Yes**.
   The pop-up message appears as Operation performed successfully.

Clone a User Group

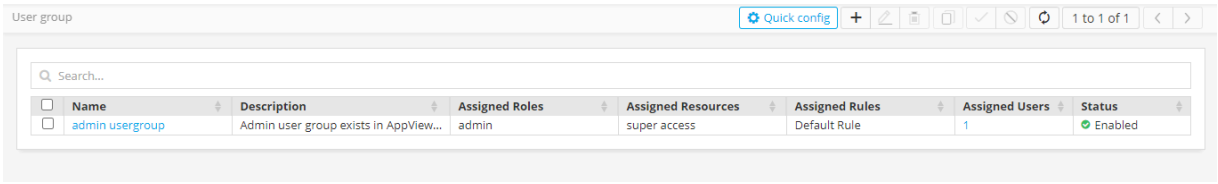
The Clone a user group option allows you to create an exact copy of an existing user group with a different name. You can modify the roles and resources association while cloning a role.

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.

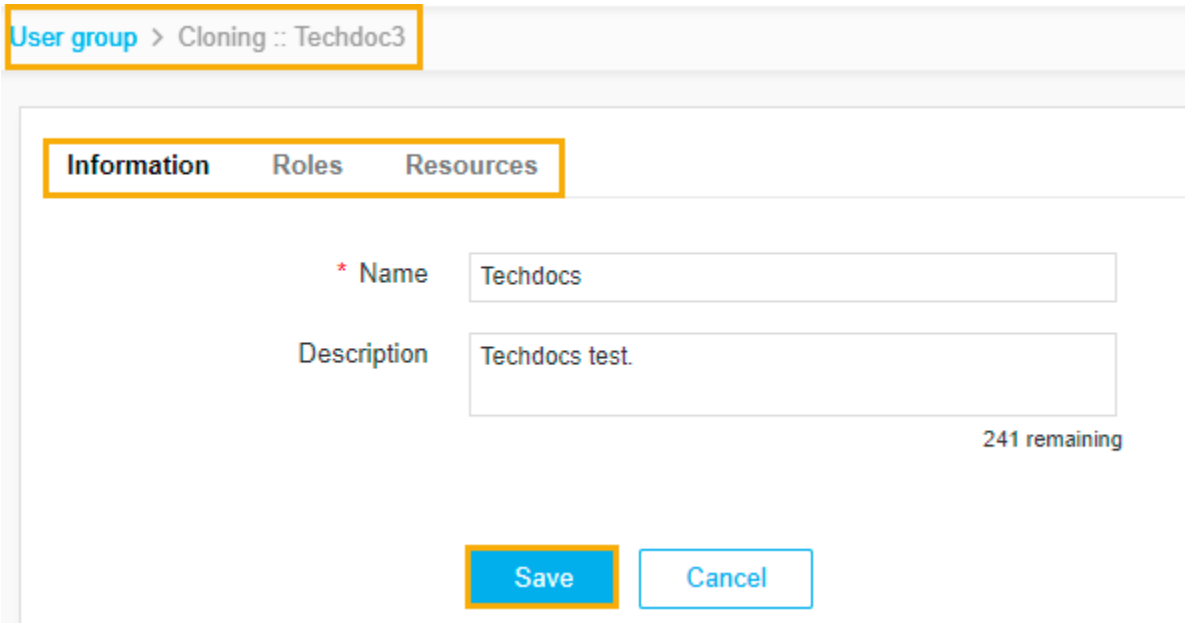


The **User Group** page appears.



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.



   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.	

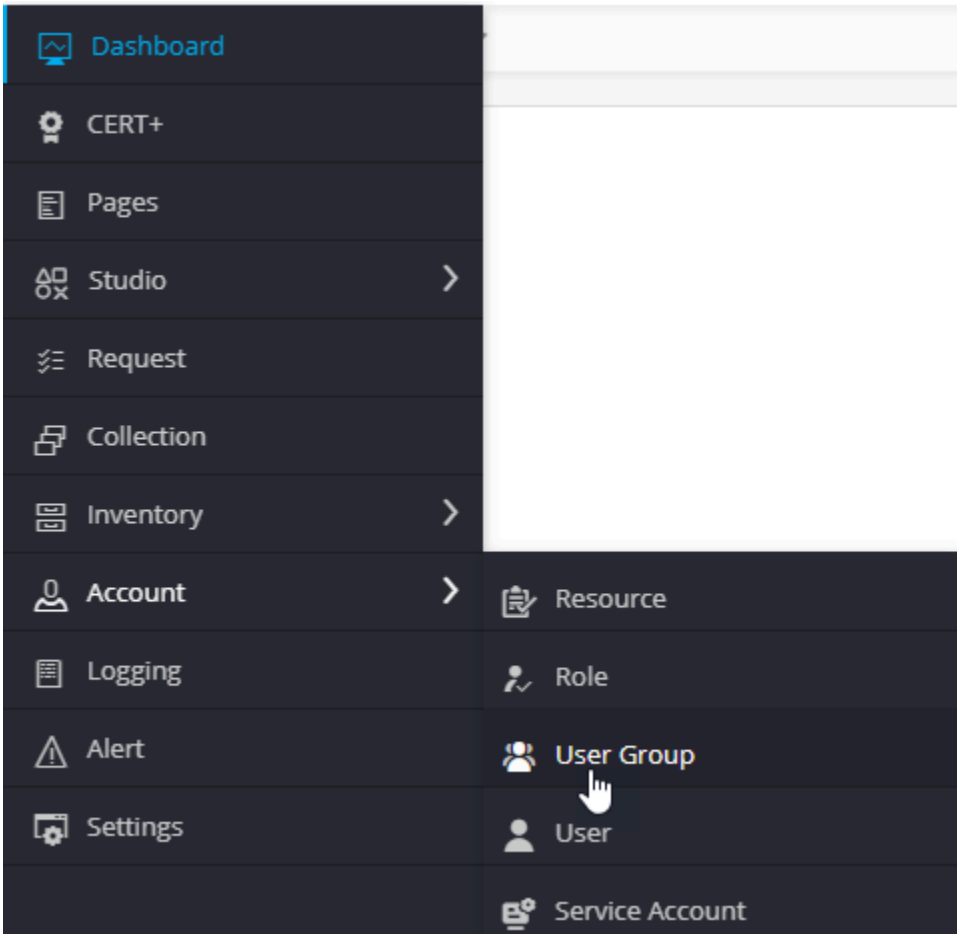
6. Click **Save.**

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

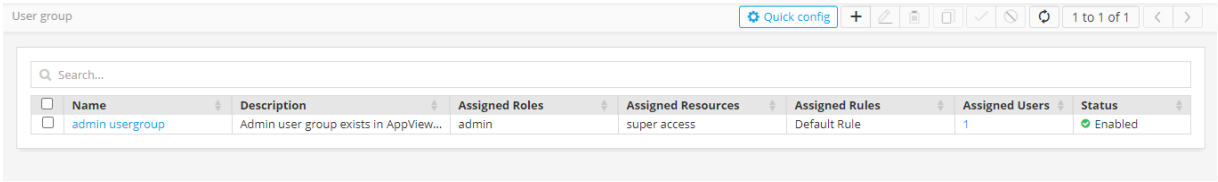
Enable a User Group

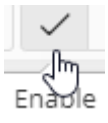
To enable a user,

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.

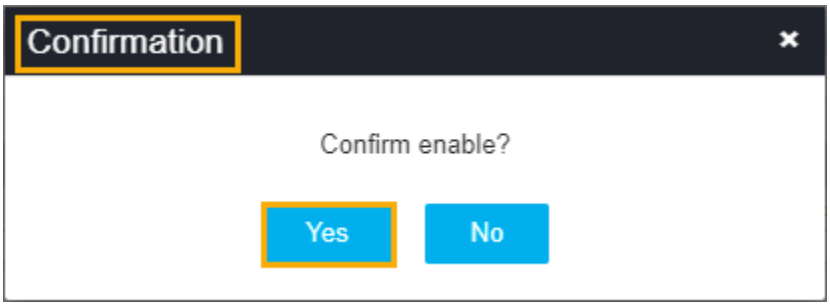


The **User Group** page appears.



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.

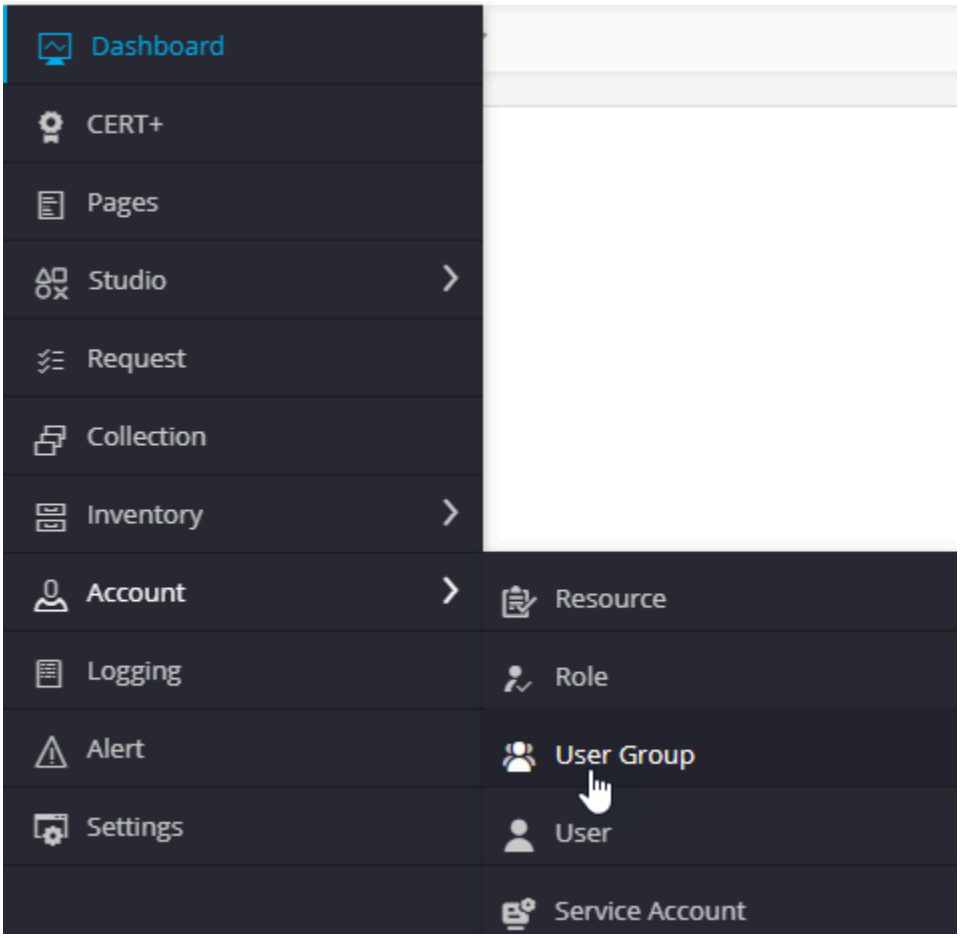


7. Click **Yes.**
   The role is enabled and a confirmation message displays as **Operation performed successfully**.

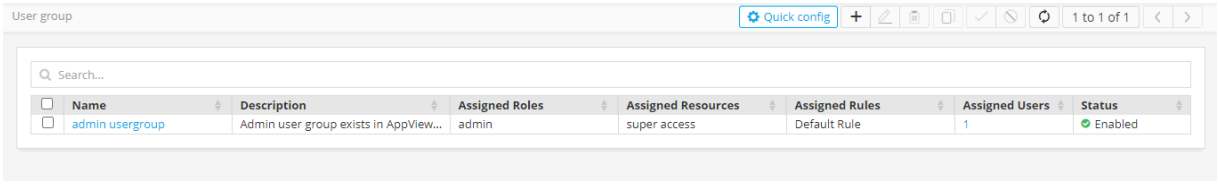
Disable a User Group

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.

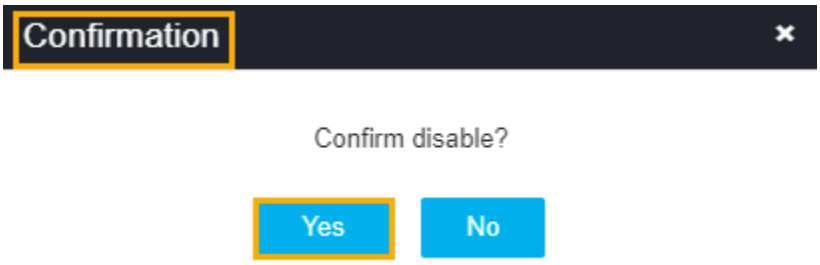


The **User Group** page appears.



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

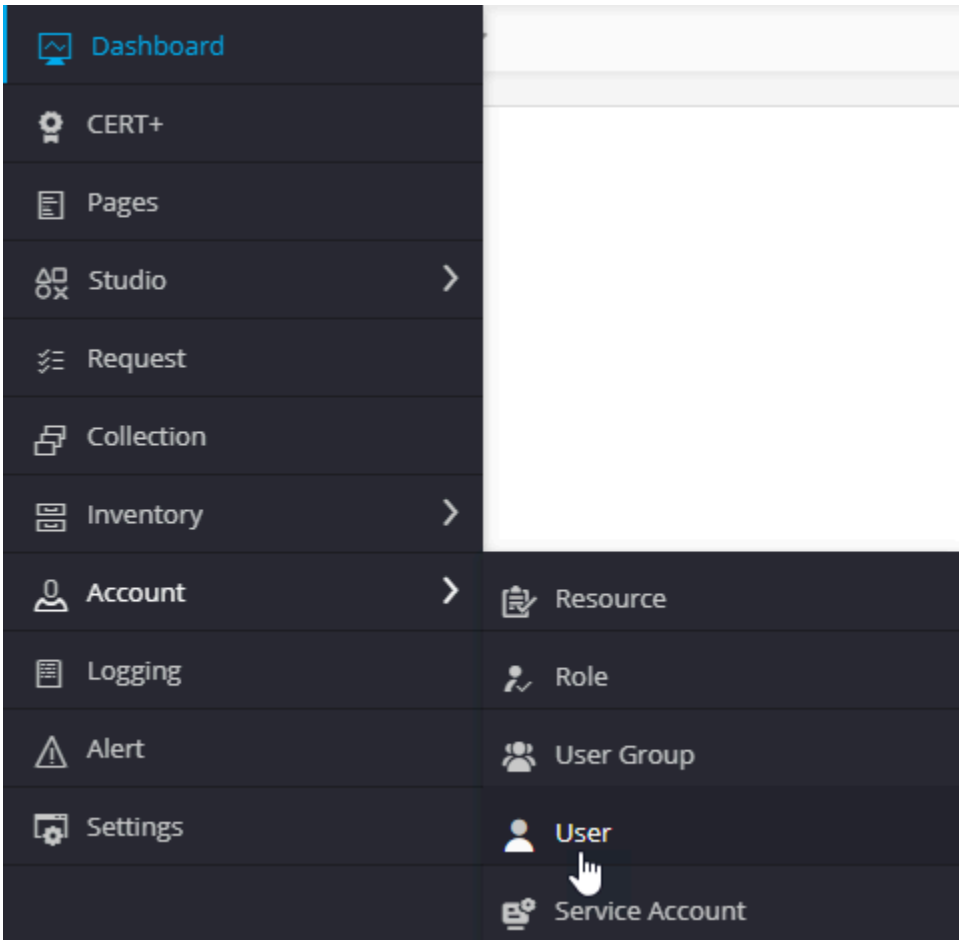
A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directory (AD). A user account is used for authentication, access, accounting, security, logging, and resource management. To create user accounts,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

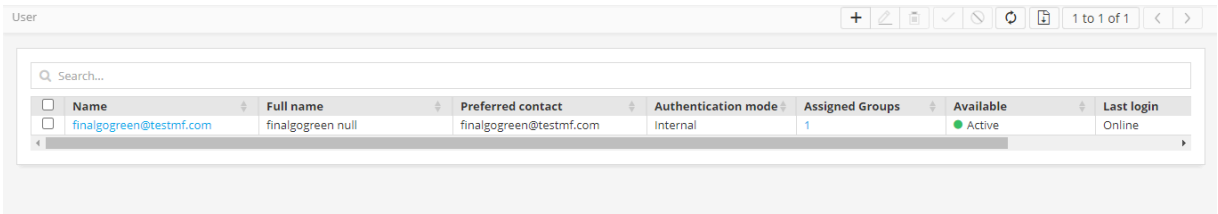
Create a User

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.

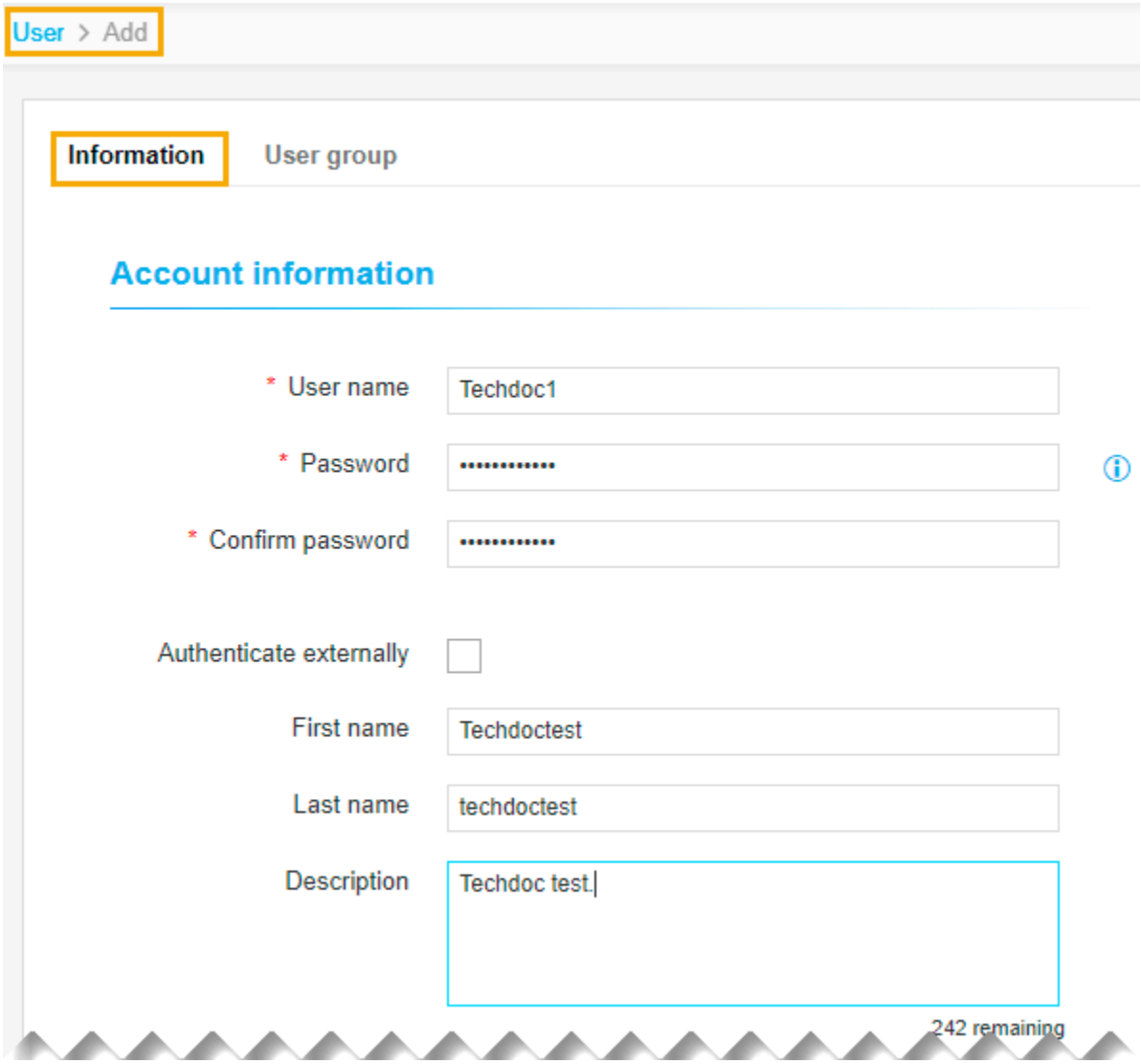


The **User** page appears.



4. Click the 

icon in the command bar to create a new user.
   The **User Add** page appears.



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

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>• Have at least one special character ~!@#$^&*_-+=|().
• Must have 6 to 24 characters long
• Not contain the user name
• Not contain the same character more than three times in a row (for example, aaaaL1$)
• Not contain blank spaces.</td></tr>
<tr><td>*Confirm password</td><td>The password to confirm the entered Password field and match with it.</td></tr>
<tr><td>(Optional) Authenticate externally</td><td>Select the Authenticate externally checkbox if you want authentication handled by an external enterprise server, such as LDAP, RADIUS, or TACACS, that is configured with AppViewX.</td></tr>
<tr><td>First name</td><td>Enter the first name of the user.</td></tr>
<tr><td>Last name</td><td>Enter the last name of the user.</td></tr>
<tr><td>Description</td><td>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.</td></tr>
</table>
</td></tr>
<tr><td>Contact information</td><td>Enter the following account details as described below:
<table>
<tr><th>Options</th><th>Description</th></tr>
<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 select the mode of contact as Phone number, phone number is mandatory to update.</td></tr>
</table>
</td></tr>
</table>

Options	Description
	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.

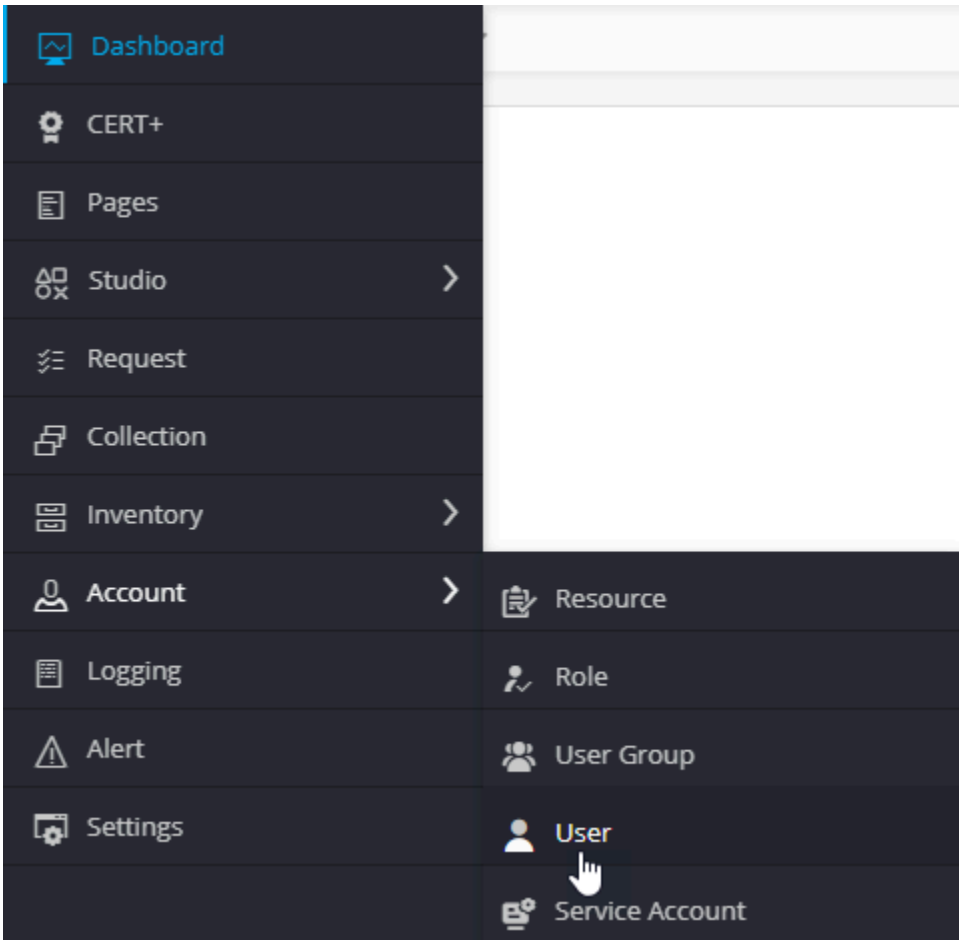
> **Note:** A user can be assigned to more than one group in the system. A user assigned to more than one group inherits all of the permissions of all of the groups to which he or she is added.

10. Click **Save**.
    The pop-up message appears as **Updated successfully.**

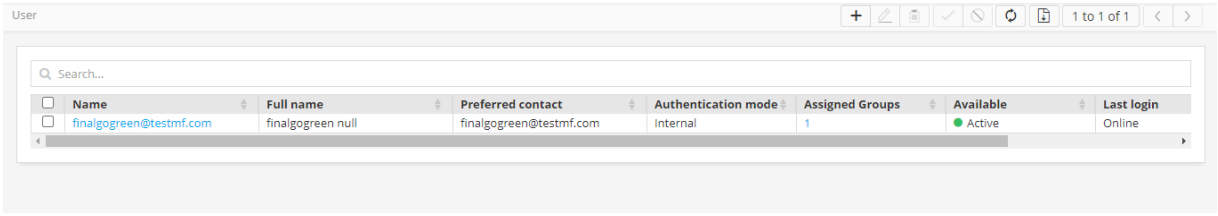
Modify a User

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.

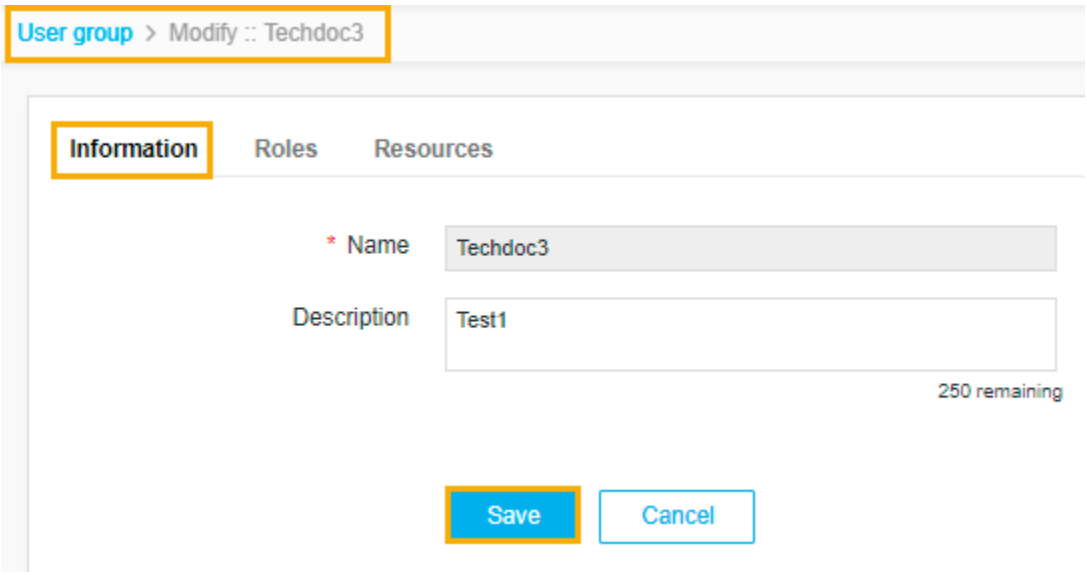


The **User** page appears.



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

   The **User > Modify** page appears.



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

Options	Description
***User name**	You cannot modify the user name.
***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 handled by an external enterprise server, such as LDAP, RADIUS, or TACACS, that is configured with AppViewX.
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 associated with the user group. **Note:** You can enter a maximum of 255 words in the field.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Contact information</td><td>Enter the following account details as described below:
<table>
<tr><th>Options</th><th>Description</th></tr>
<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.</td></tr>
<tr><td colspan="2">Note: If you have the select mode of contact as Phone number, phone number is mandatory to update.</td></tr>
</table></td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

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.

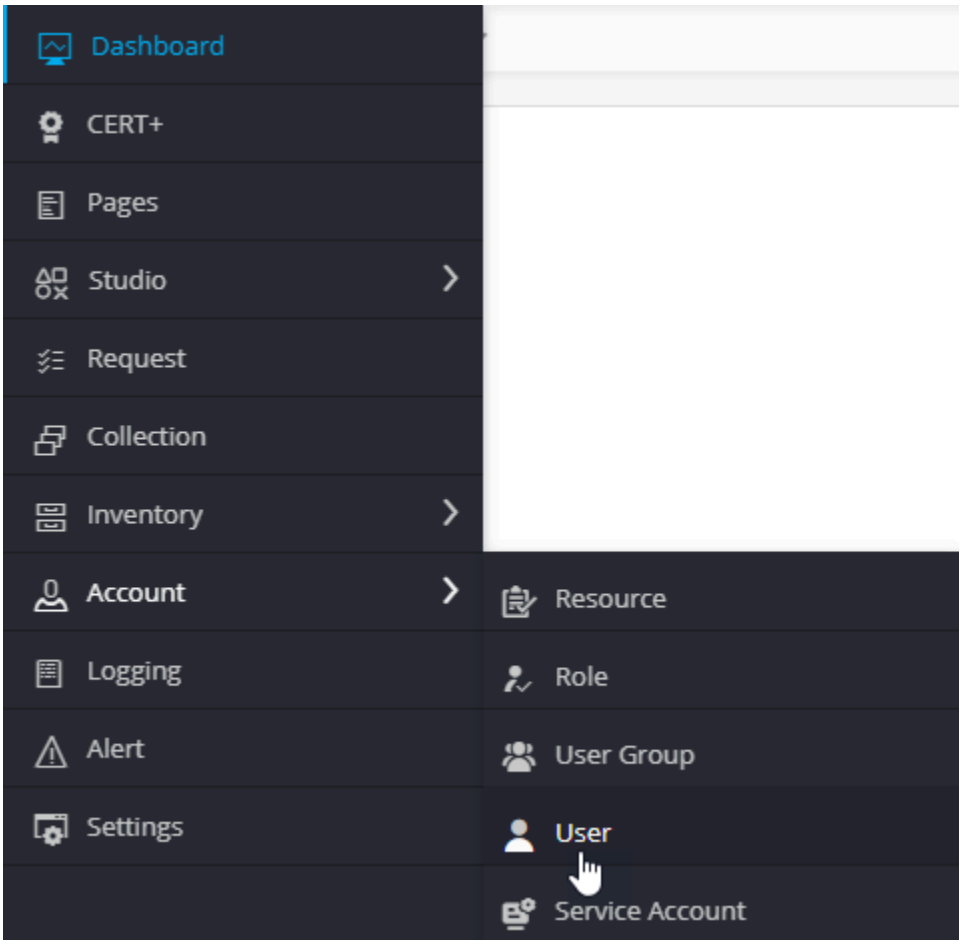
Note: A user can be assigned to more than one group in the system. A user assigned to more than one group inherits all of the permissions of all of the groups to which he or she is added.

9. Click **Save**.
   The pop-up message appears as **Updated successfully.**

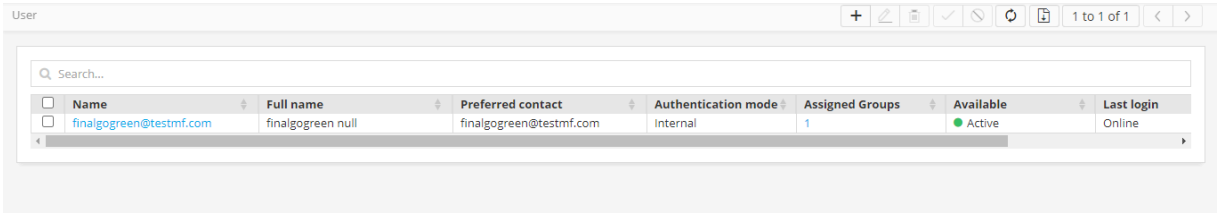
Delete a User

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.



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

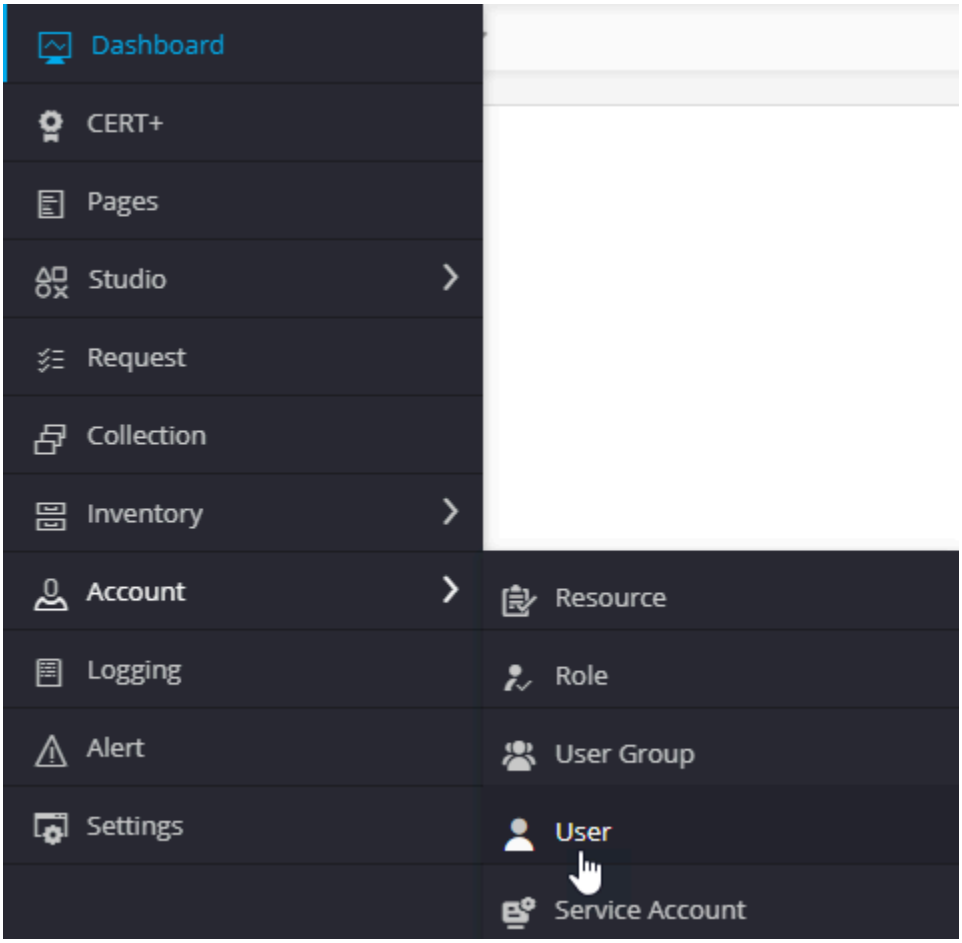
   The confirmation pop-up window appears.
6. Click **Yes**.

   The pop-up message appears as Operation performed successfully.

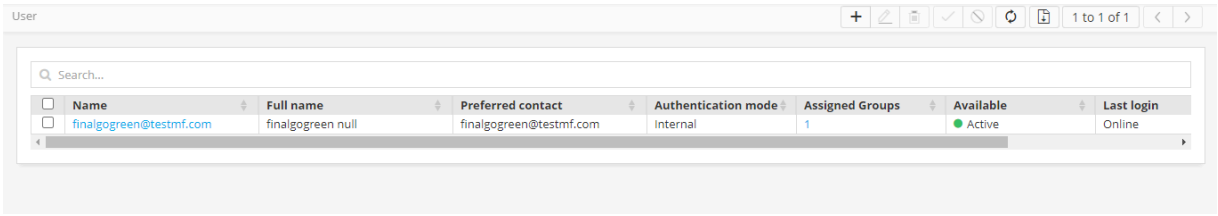
Enable a User

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.



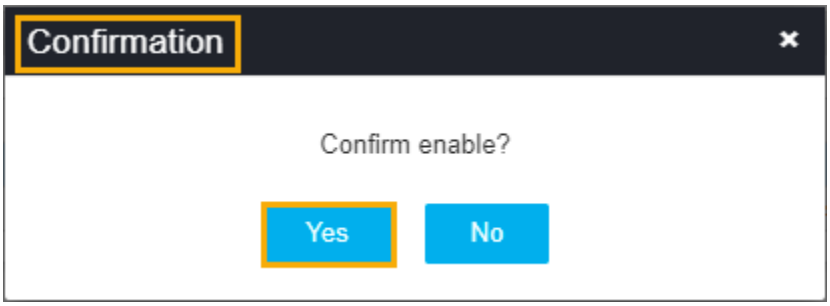
The **User** page appears.



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

5. Click the 

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

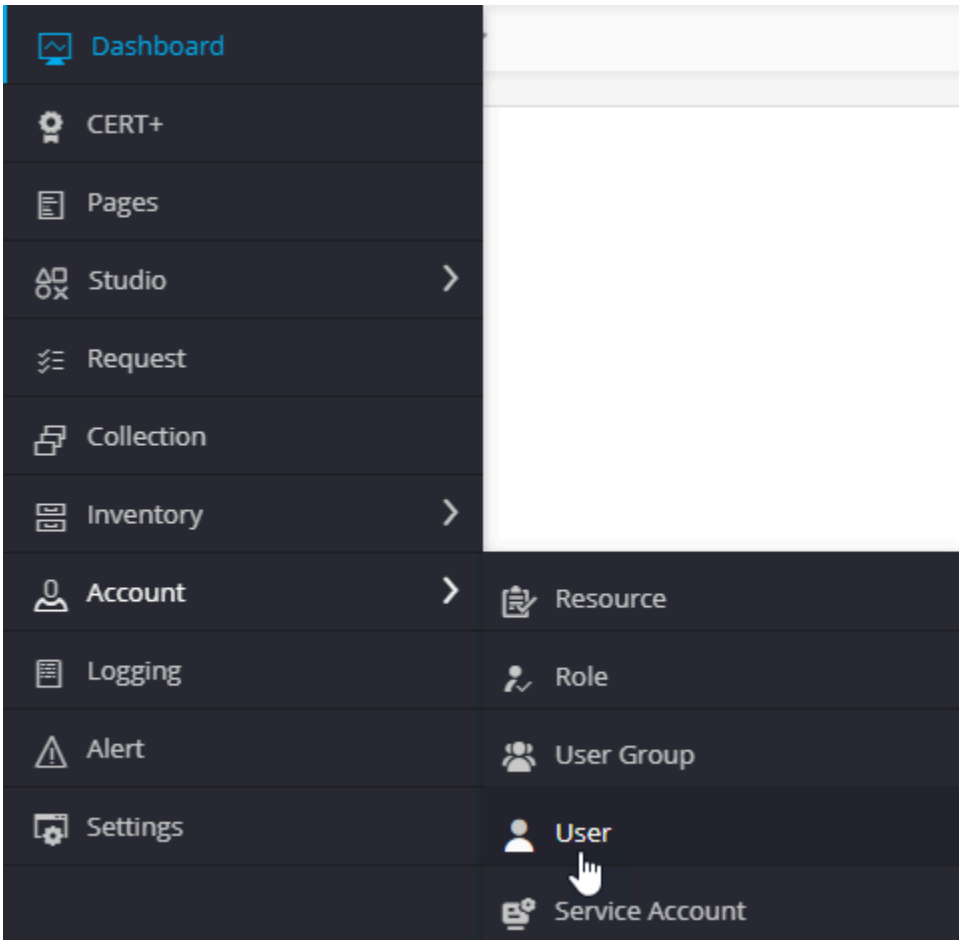


7. Click **Yes**. The role is enabled and a confirmation message displays as **Operation performed successfully**.

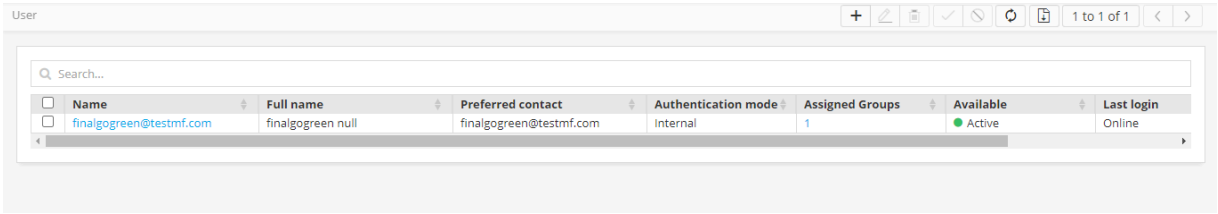
Disable a User

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** from the list.

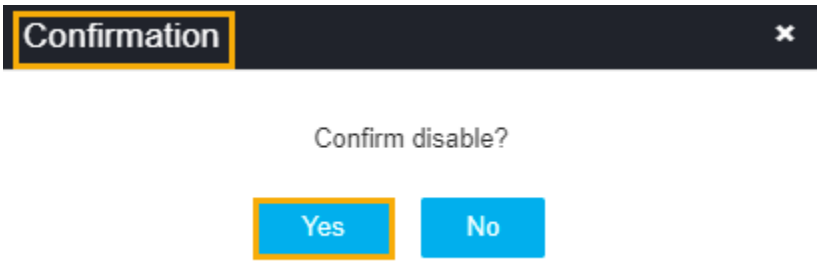


The **User** page appears.



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.

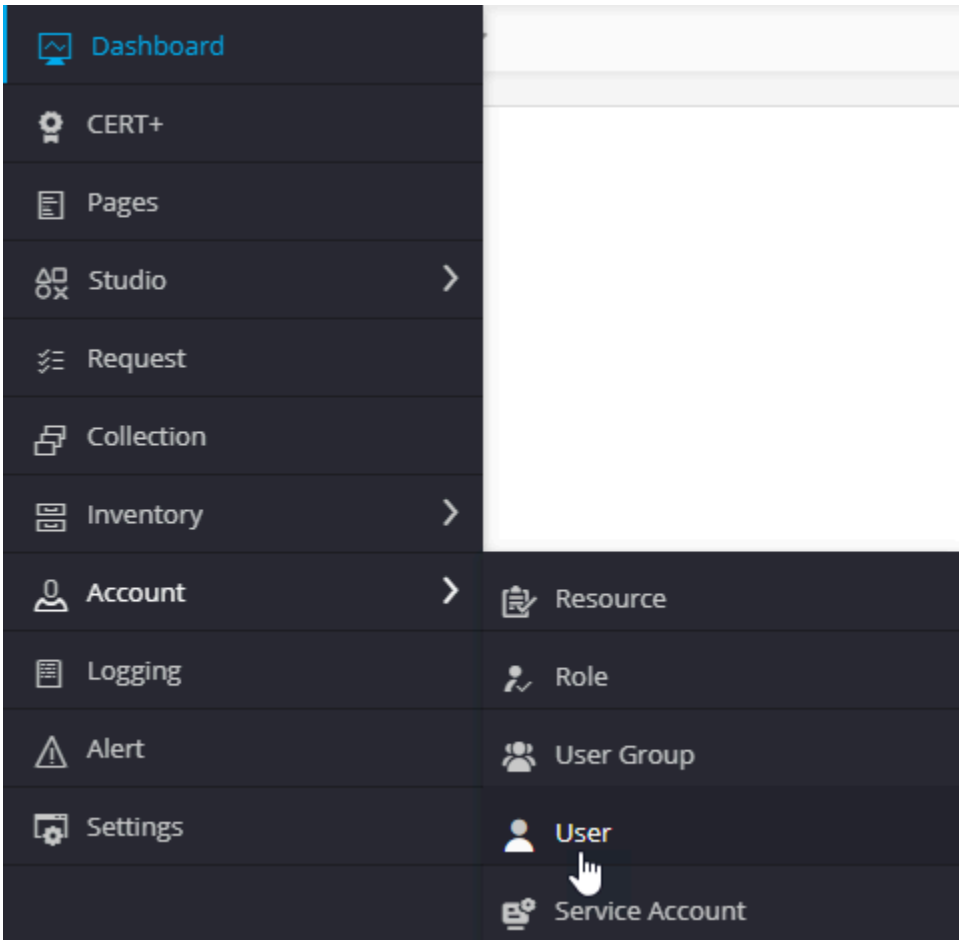


7. Click **Yes.**
   The role is disabled and a confirmation message displays as **Operation performed successfully**.

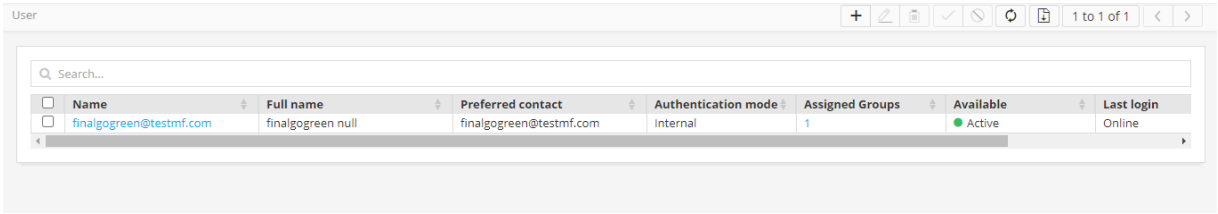
Import Users

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.



4. Click the  icon in the command bar to import the file.
   The import page appears.
5. 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

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

Accessing 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
- EJBCA CA
- Entrust MPKI
- GoDaddy CA
- Google CA
- InCommon CA
- Let’s Encrypt CA
- Microsoft Enterprise CA
- Microsoft Standalone CA
- Symantec CA
- Trustwave CA

Amazon and Amazon Private CA

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

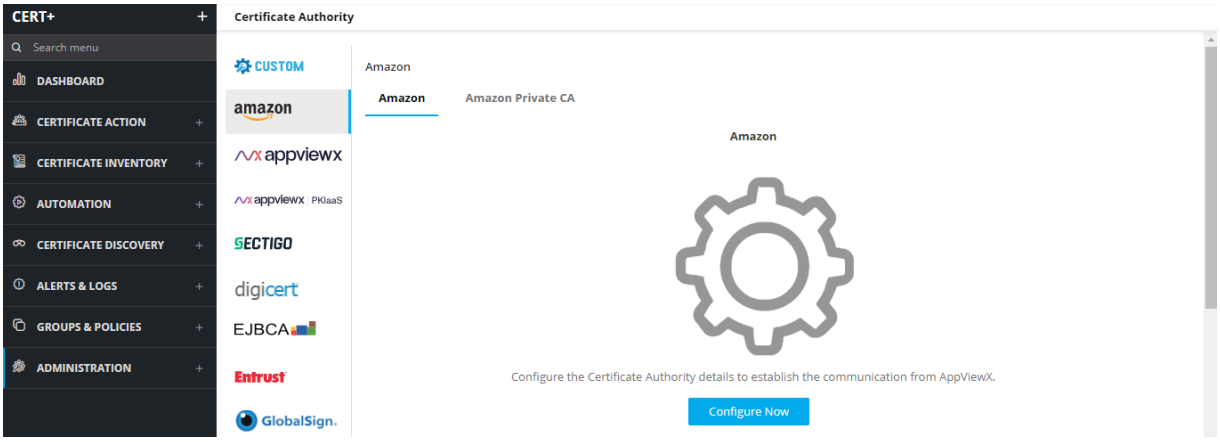
To configure the Amazon CA,

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 appears.



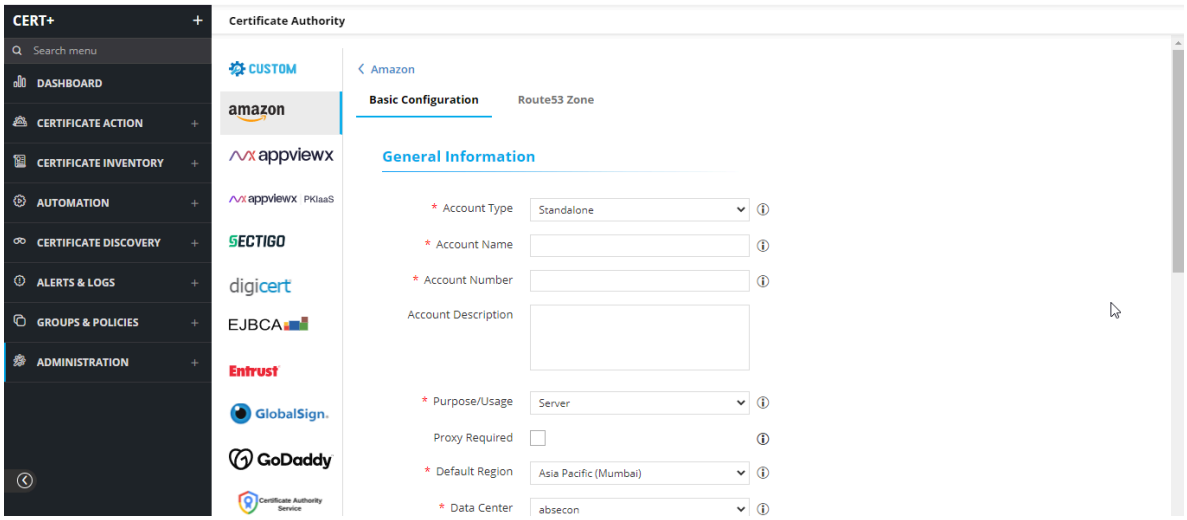
6. Click **Amazon** or **Amazon Private CA** from the home page.

   The respective CA home page appears.

7. 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.



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.

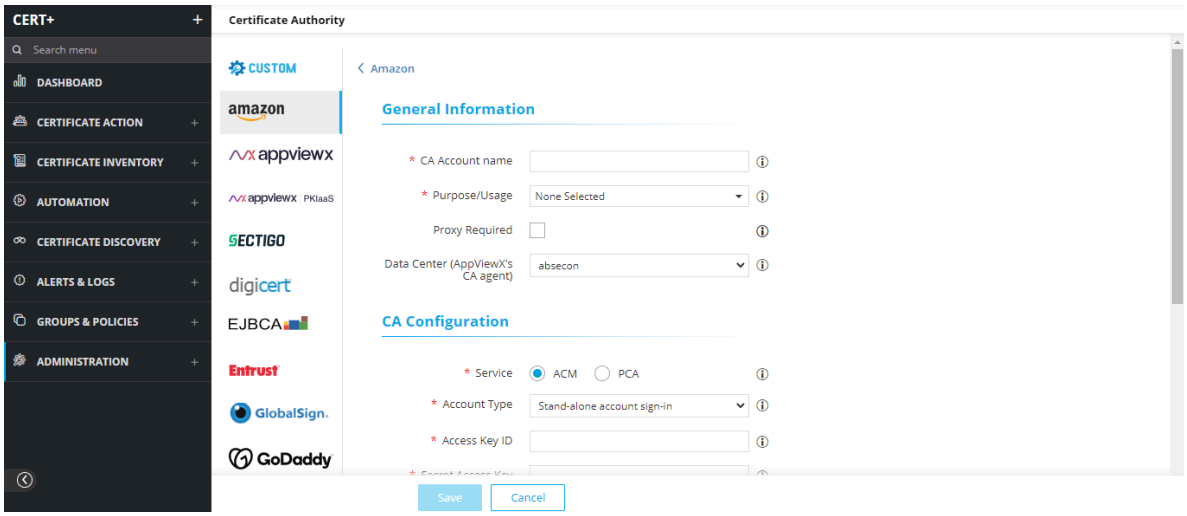
Section	Field	Description
		Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
	* **Purpose/ Usage**	Certificate Type for which CLM actions will be enabled. The available options are, • Server • Client.
	Proxy Required	Enable this field if 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**.

8. To configure Amazon Private CA, click **Amazon Private CA** on the home page.

a. Click the **Configure Now** or **+Add** icon from the middle or top-right of the page respectively.

The **Amazon** Private CA configuration page appears.



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	***Service**	Based on the permissions assigned on AWS, select the service. The possible services are,

Section	Field	Description
		• ACM • PCA. **Note**: By default, ACM is selected.
	***Account Type**	Select the account type from the dropdown list. The possible options are, • **Stand-alone account sign-in** - User account and resource available within the same account. • **Cross account sign-in** - Resource available in the different account and accessed via role.
	***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.
	***Default region**	Select the Fetch region where the user has access.
	***Service Region**	• Click the Fetch regions button. • **To enable Fetch regions,** enter the Access Key ID and Secret Access Key. • On Providing **valid** details, AppViewX must fetch the region associated with the account. • On successful operation, enabled regions are listed in the multi-select dropdown list. **Note:** You can select one (or) more regions from the dropdown list. • If provide **invalid** details, an error message appears as **Incorrect Credentials, provide valid credentials to fetch regions. Users can not complete the submission of the account details in AppViewX**.

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

b. On selecting the region from the dropdown list, the Fetch Issuer Details button enables.
   i. Enter the access key and secret key details, it fetches all the ACM Private CA account names corresponding to the selected regions.
   ii. Lists the CA names along with the Regions and their validity.
      1. Select the PCA account required to be configured.
      2. Enable and Disable option should be available for all the PCA account. By default, the PCA account will be enabled.
      3. Click **Enable** to configure the PCA account.

c. Click **Save**.

Validating Amazon

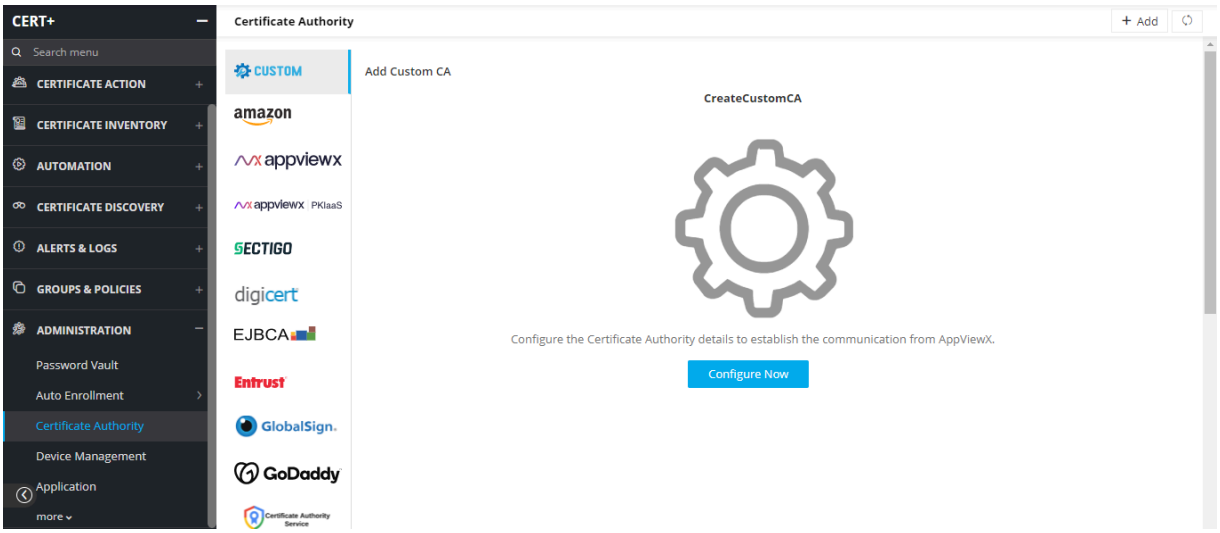
Once the Amazon settings are added, you need to validate the connection between AppViewX and Amazon, to make sure that the connection is properly configured.

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+**.

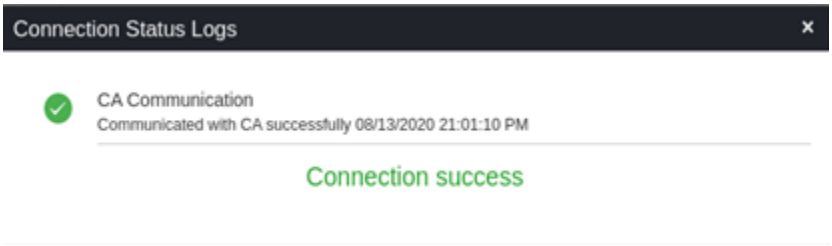
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Amazon**.

   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

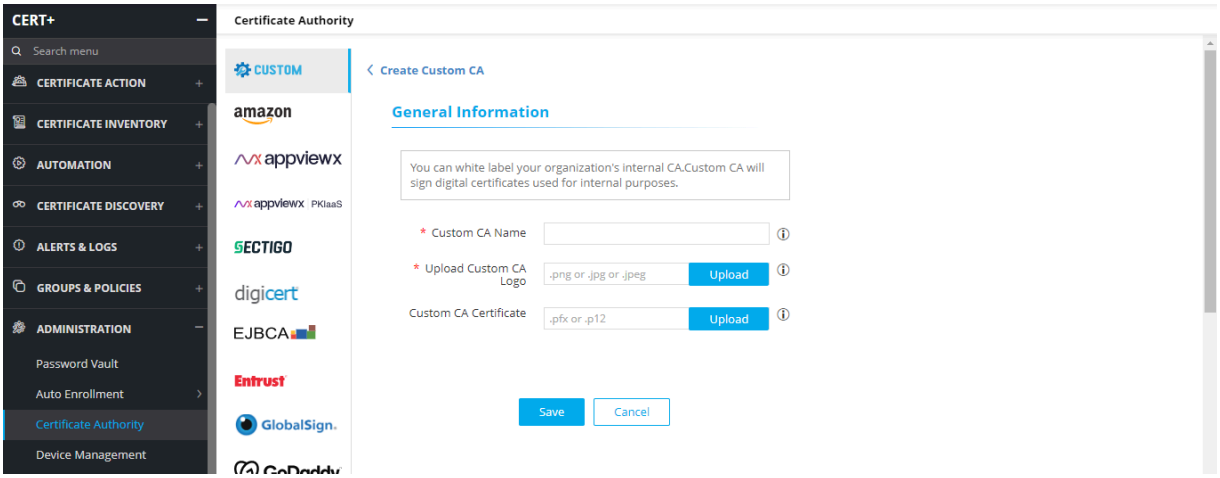
Following are the prerequisites for configuring Custom CA account in AppViewX:

- 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,

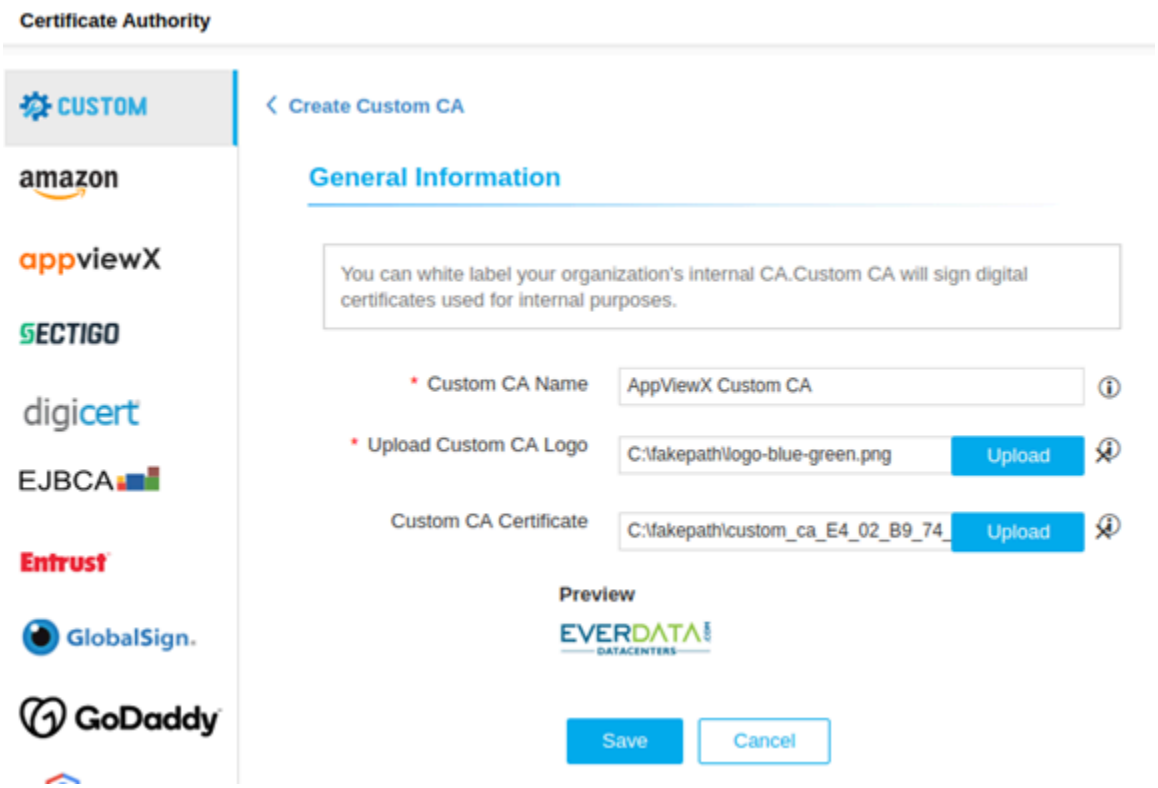
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Custom**.
   The **Certificate Authority** home page appears.



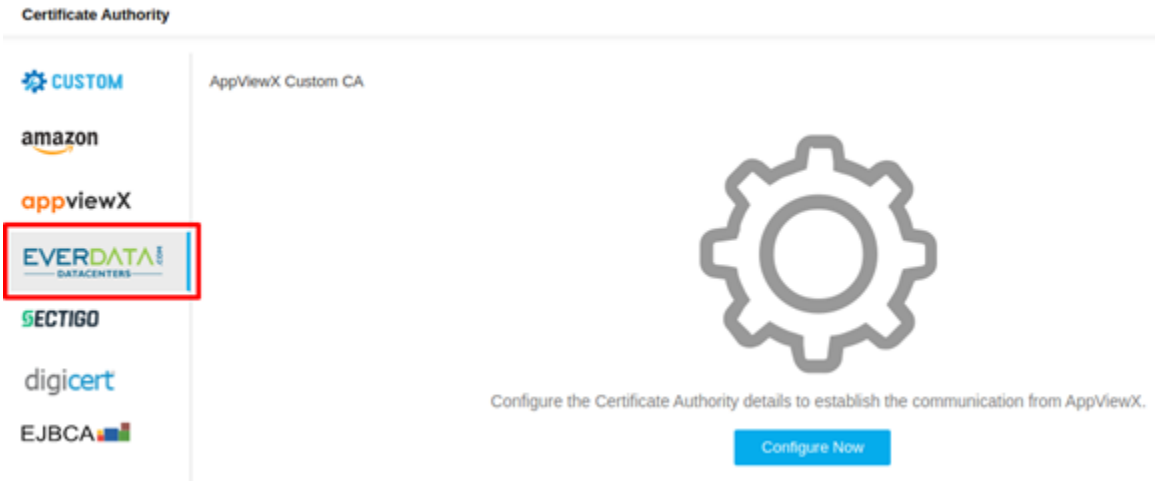
6. Update the following details in the **General Information** section as described in the table:

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

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



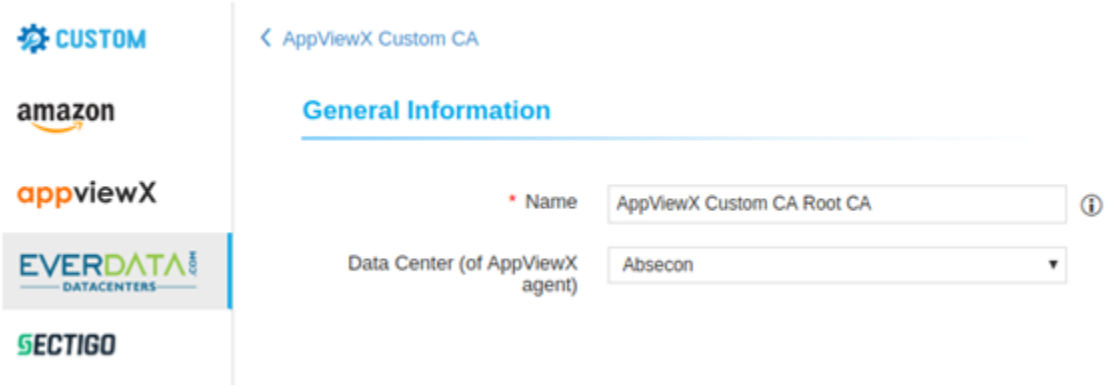
7. Once the logo and certificate are uploaded, the entered CA will appear in the CA list with the logo presented.



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.

Name	Description
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.

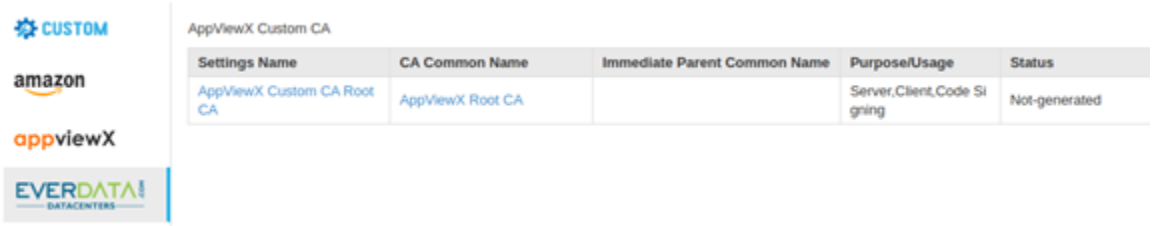
Name	Description
***Start Date**	Start date of the certificate issuance.
***End Date**	End date of the certificate issuance.

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.



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,

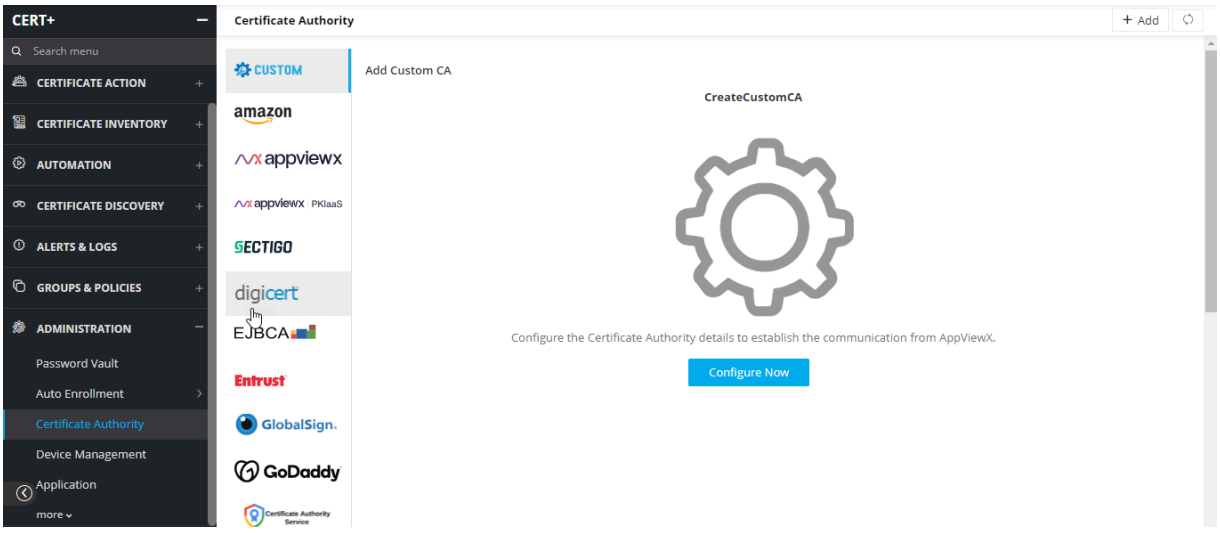
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

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

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

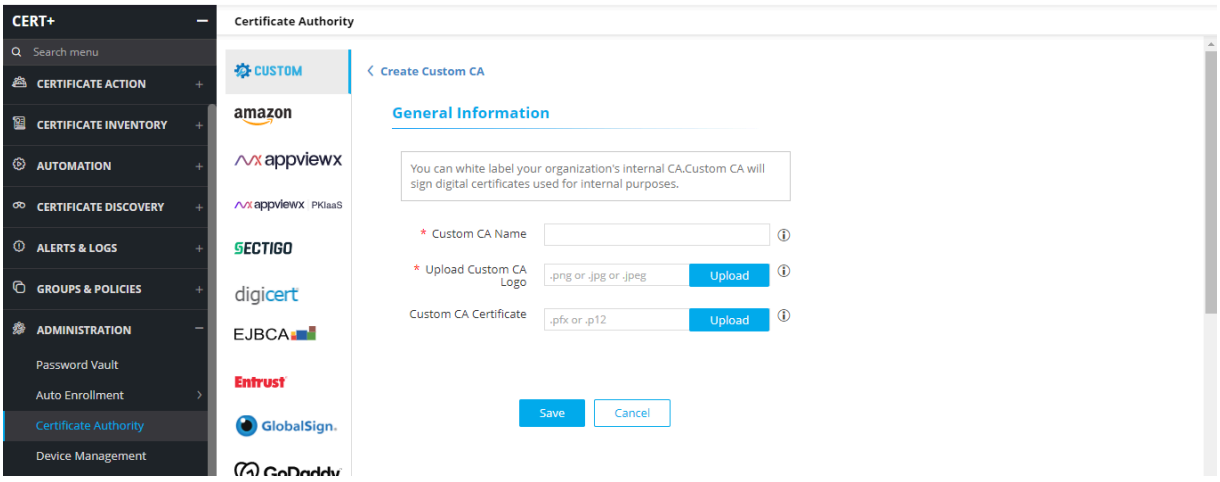
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **digicert**.

   The **Certificate Authority** home page appears.



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

   The **DigiCert** configuration page appears.



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
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.

Name	Description
Account ID	Account id details of Digicert CA Account, which can be found under account manager details in Digicert CertCentral Account.
***API Key**	API key specific to the CA account. This API key should have required permission to make API Calls. Space is not allowed.
Auto Approve	Enable **the Auto Approve** option if all CLM requests from AppViewX do not need to be approved from Digicert CA Account.

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.

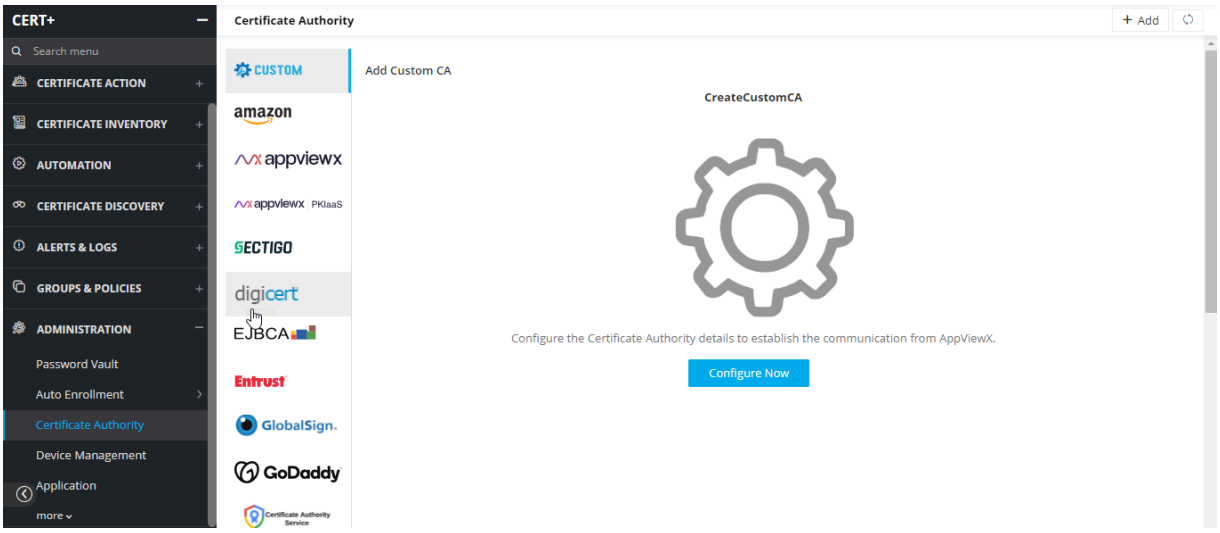
   The left navigation pane appears.

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**.

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

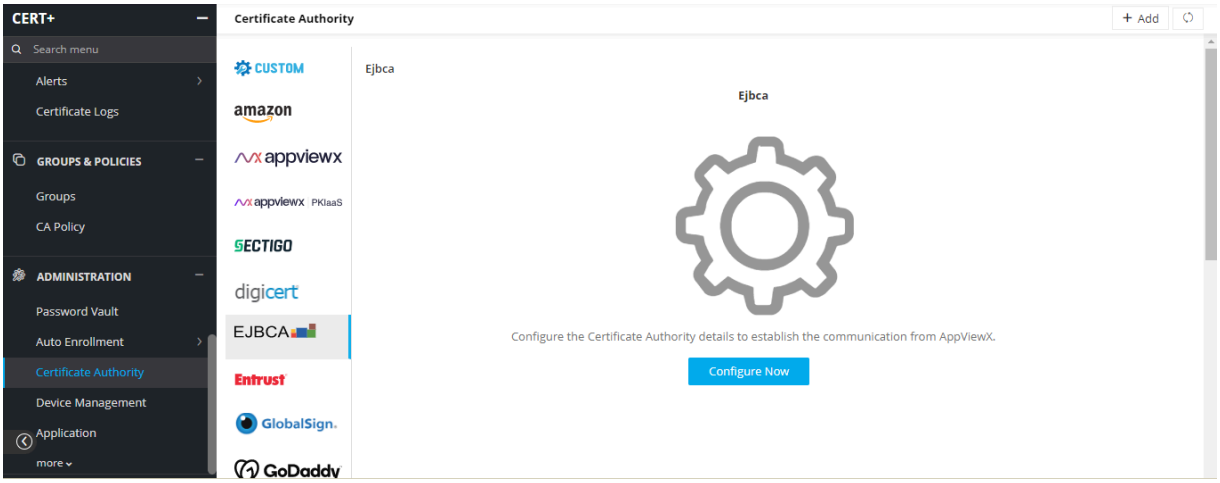
To configure the EJBCA CA,

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+**.

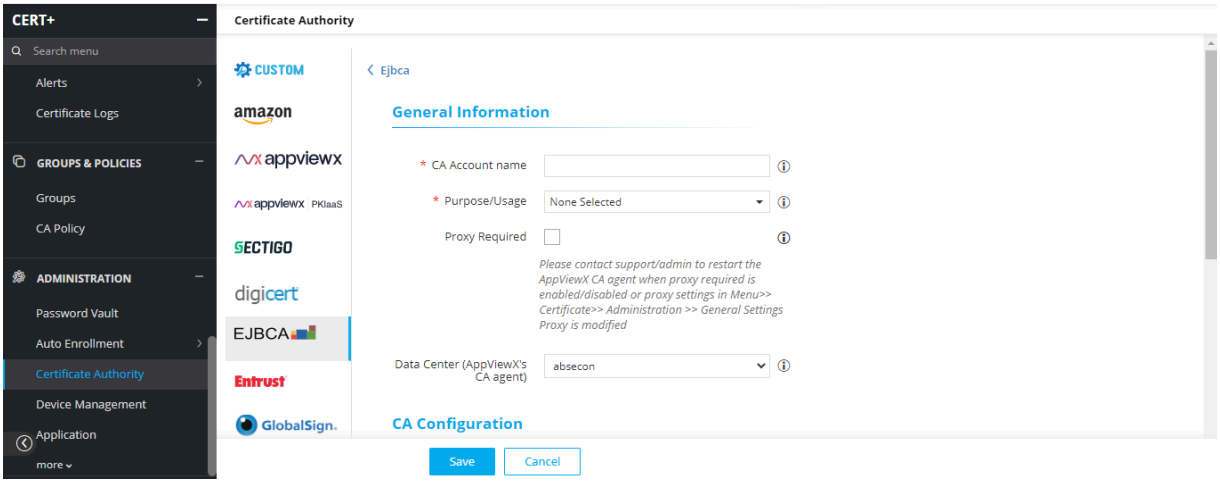
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **EJBCA**.

   The **Certificate Authority** home page appears.



6. Click **Add** from the top right corner of the page.

   The **Ejbca** configuration page appears.



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.
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**.

Options	Description
	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.

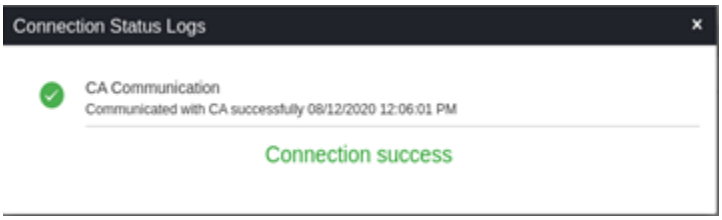
1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

   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.

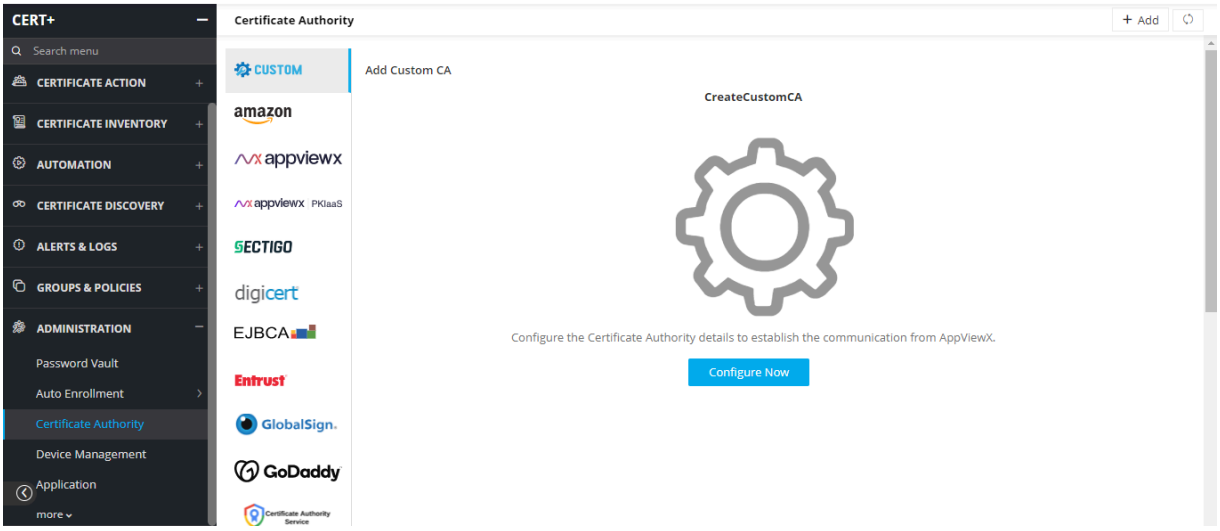
Configuring Entrust MPKI

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.

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 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 Authorityalong 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,

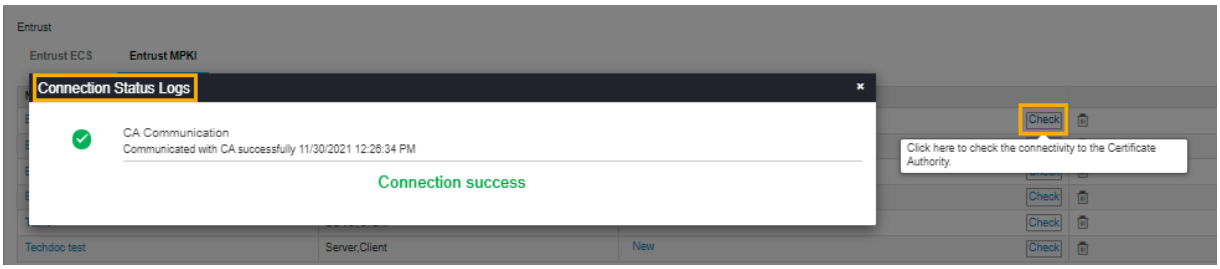
1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   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

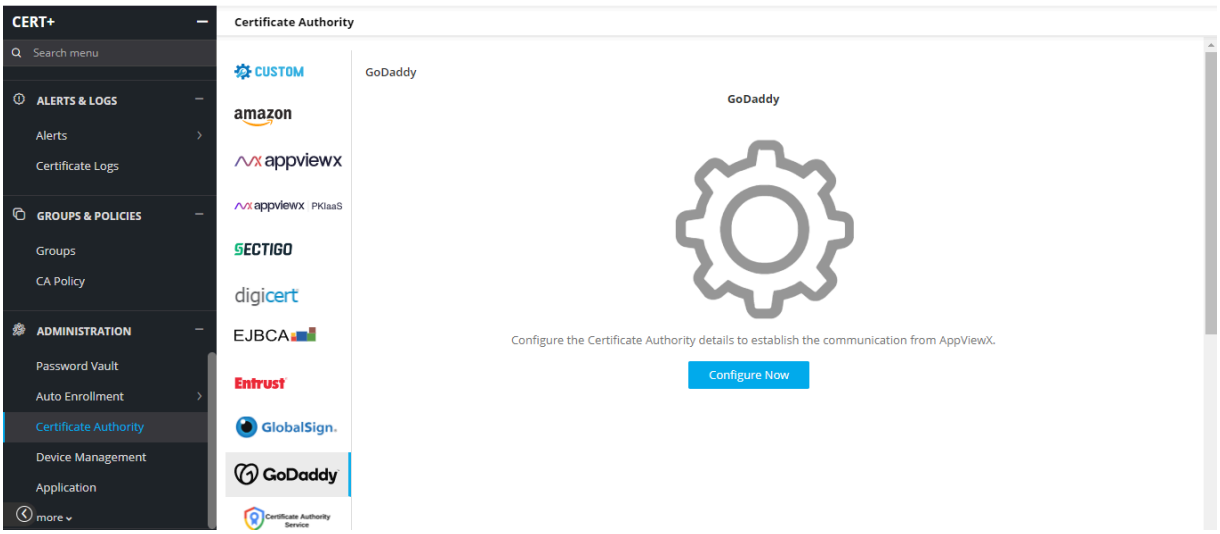
To configure the GoDaddy CA,

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+**.

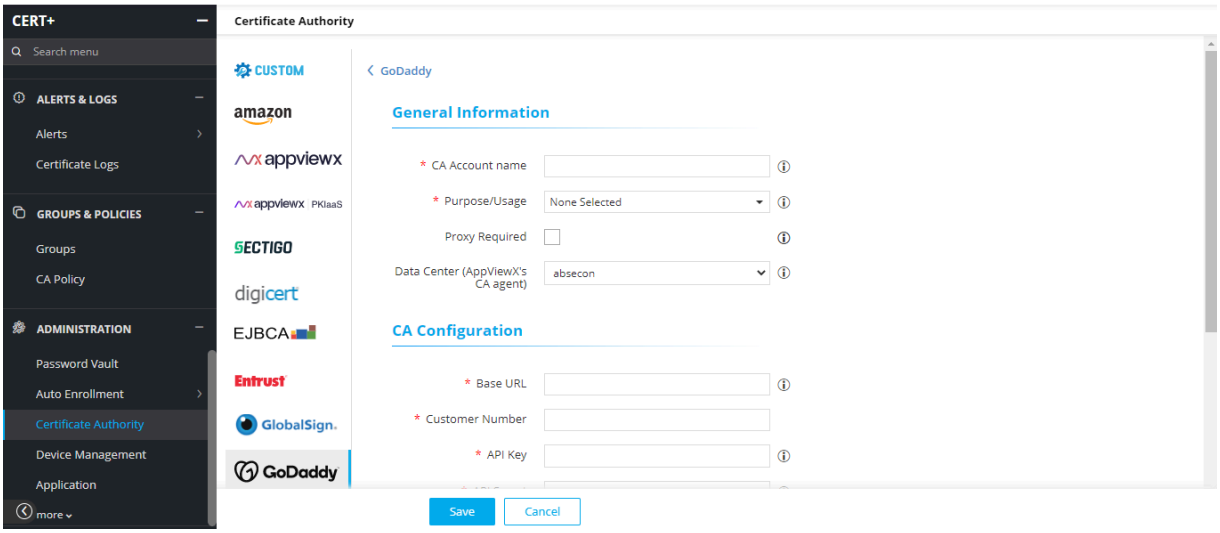
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **GoDaddy**.

   The **Certificate Authority** home page appears.



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

   The GoDaddy configuration page appears.



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.

Name	Description
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
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.
Phone Number	Phone number of the GoDaddy Account user as provided in the portal to be used for certificate creation purposes.

Name	Description
	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,

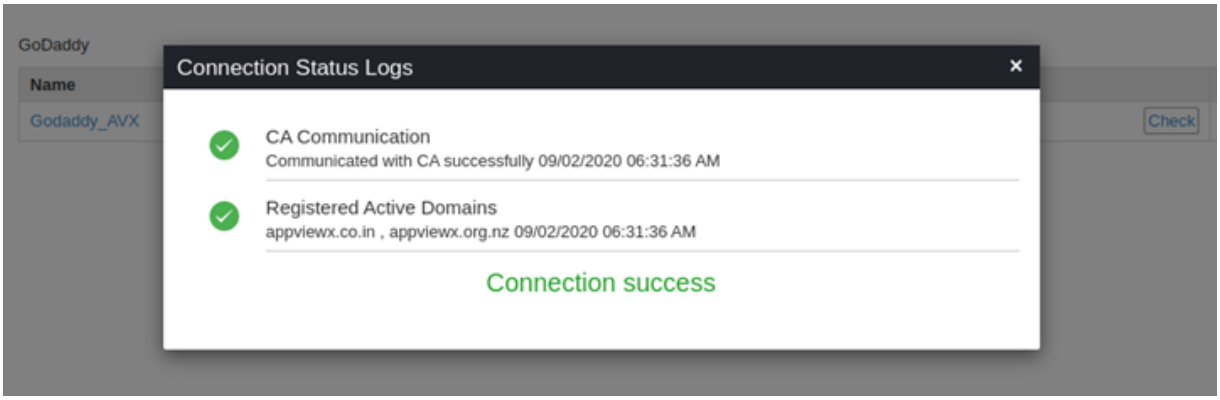
1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

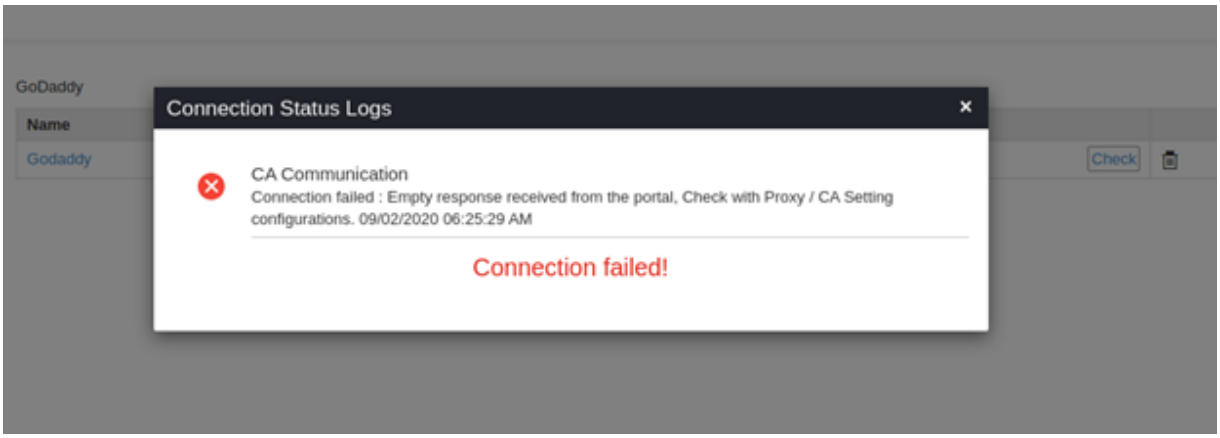
   The left navigation pane appears.
3. Click **CERT+**.

   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.

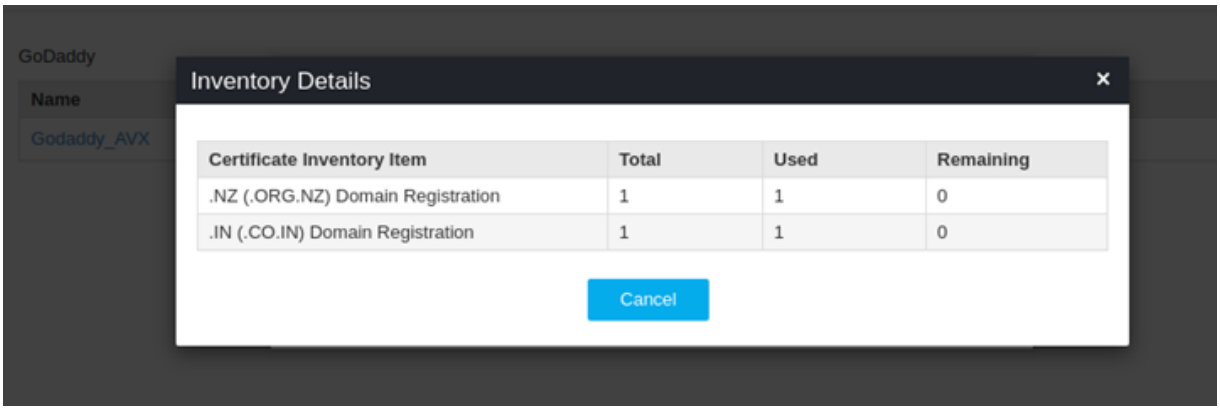
To view the GoDaddy product units,

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.
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

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+**.

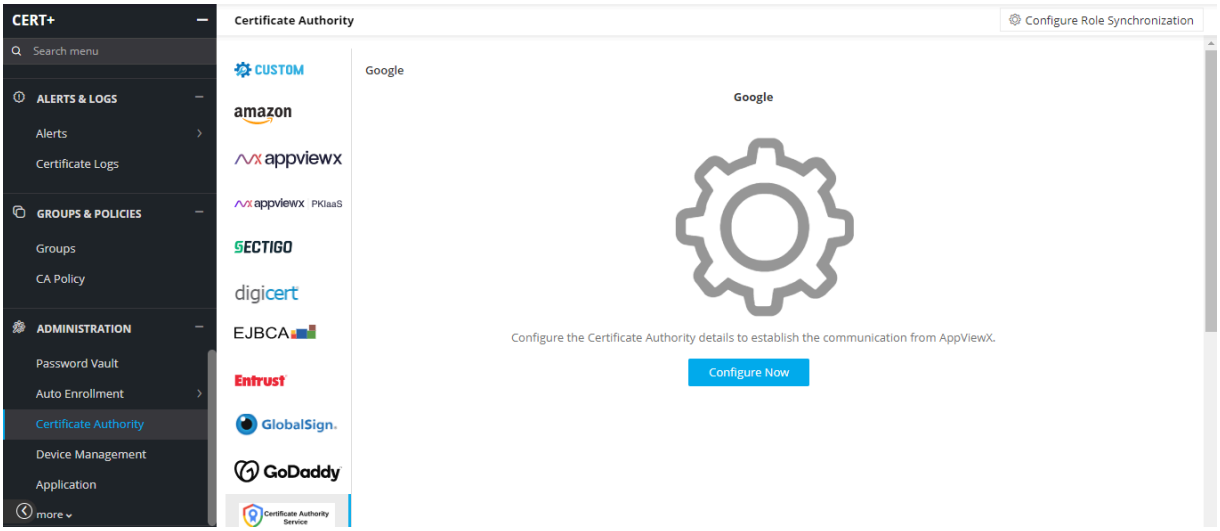
The **CERT+** left navigation pane appears.

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.



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.
*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.

Name	Description
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

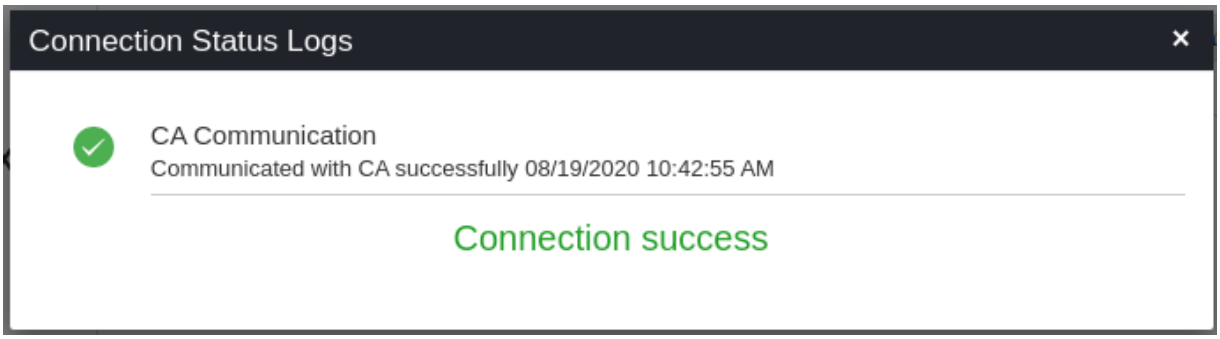
Once the Google settings are added validation needs to be done to check whether the connection between AppViewX and Google is properly configured. To validate the Google CA,

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

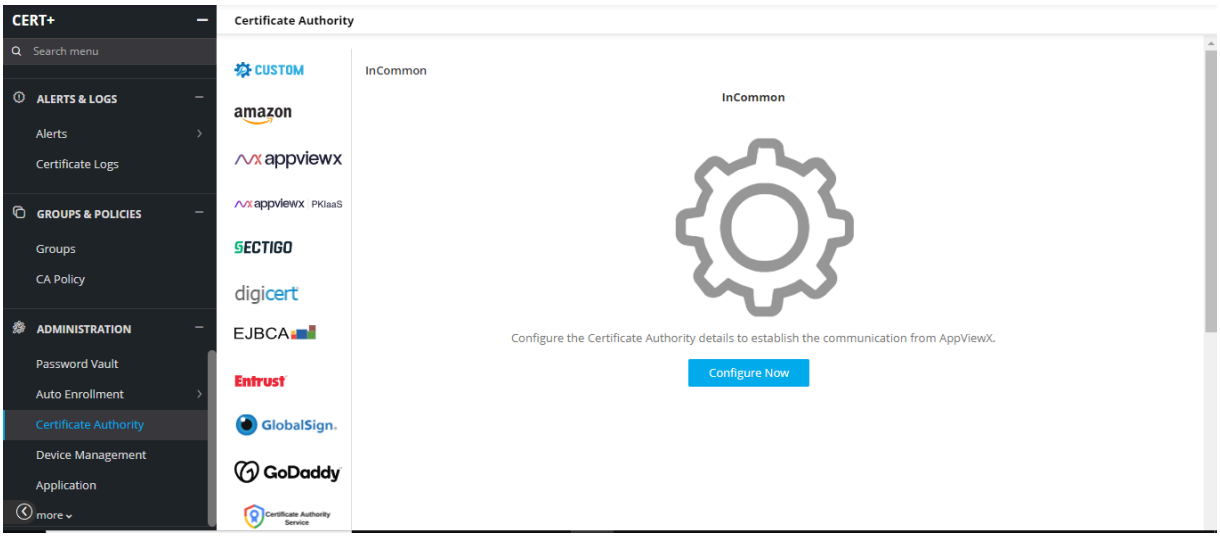
To configure the InCommon CA,

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

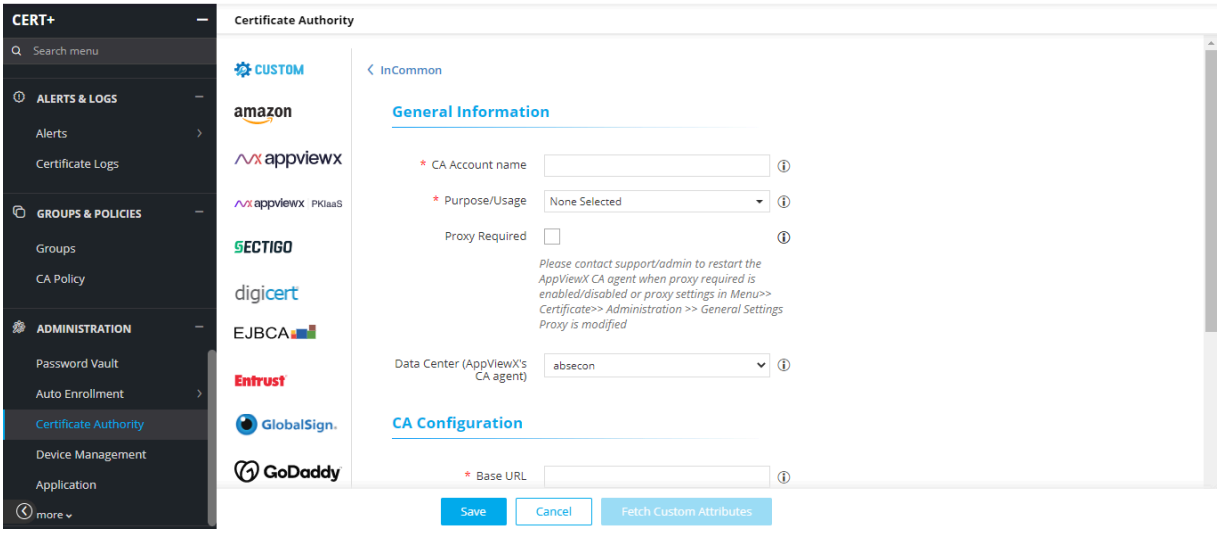
   The left navigation pane appears.
3. Click **CERT+**.

   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.



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 - https://cert-manager.com/customer/<<customer_uri>>/ssl- here base URL is **https://cert-manager.com.** **Note:** No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Login URL**	URI specific to the InCommon CA Customer Account. Eg https://cert-manager.com/customer/<<customer_uri>>/ssl- here URI is **customer_uri**.
***User Name**	User name for the account created with InCommon CA.
***Password**	Password for the account created with InCommon CA.
***Organization ID**	InCommon supports organization hierarchy. Id of the **Organization Unit/ Department** in which Certificates need to be managed has to be specified here. **CLM** actions done using this CA account will be specific to this particular organization's id/department.
Note: The asterisk (*) symbol indicates a mandatory field.**Note:** If the certificates from multiple organization's units/departments need to be managed, then a separate CA has to be configured for each organization unit/department in the Incommon CA setting page.	

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

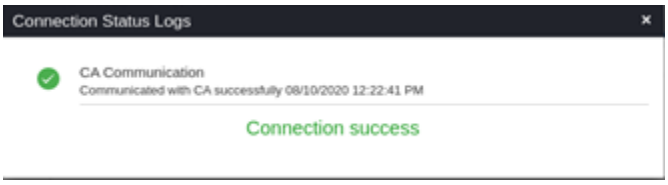
Once the InCommon settings are added validation needs to be done to check whether the connection between AppViewX and InCommon is properly configured. To validate the InCommon CA,

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.orgfor **staging**.
2. https://acme-v02.api.letsencrypt.org for **production**.

Configuring Let's Encrypt CA

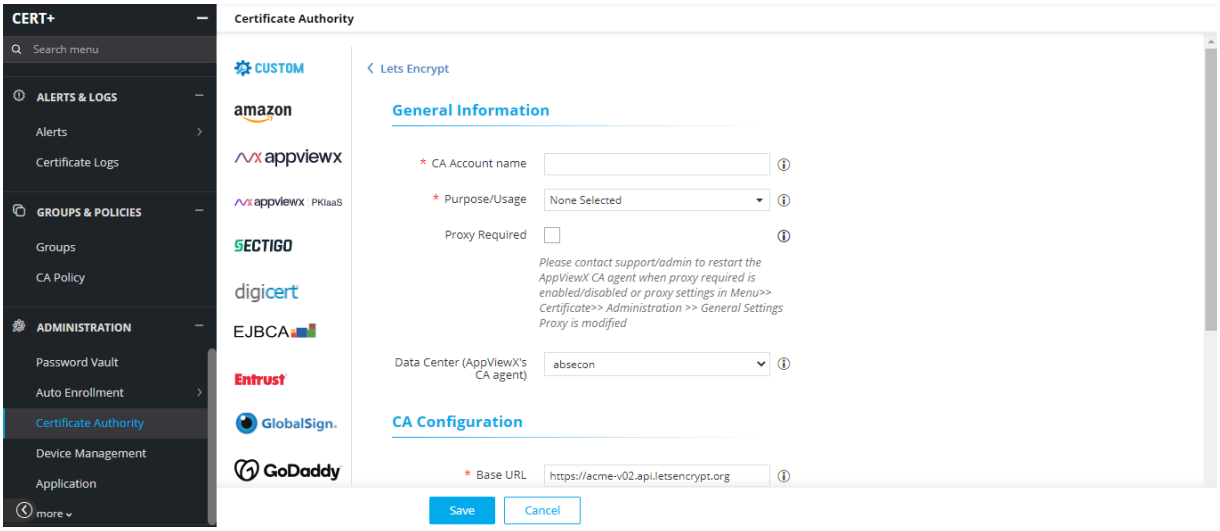
To configure the Let's Encrypt CA,

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

   The Let's Encrypt configuration page appears.



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.

Name	Description
	Note: No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Purpose/Usage**	The certificate types will be managed by these settings. For now, Let's Encrypt is having only one purpose **Server**.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
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

Communication mode	Category	Windows gateway machine	Microsoft 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 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

Communication mode	Category	Windows gateway machine	Microsoft CA
			level for the service account or the service account group or authenticated users
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	NA.	135, 445 or 139

Configuring Microsoft Enterprise CA

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
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.

Name	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.

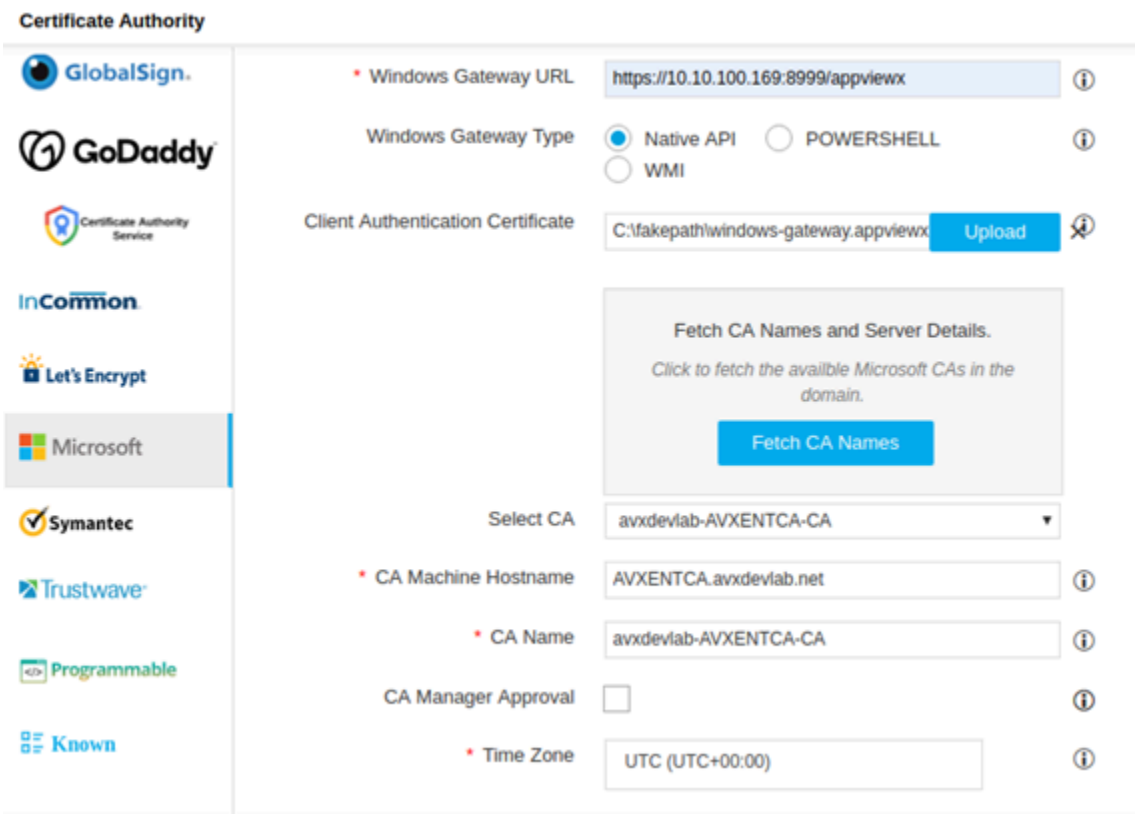
Name	Description
***Windows Gateway URL**	Enter the URL where the AppViewX agent is running.
***Windows Gateway Type**	The mode of communication types from Windows Gateway machine to CA machine. Available types are **NATIVE API, POWERSHELL, WMI.** Refer **Communication Mode**
Client Authentication Certificate	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**.

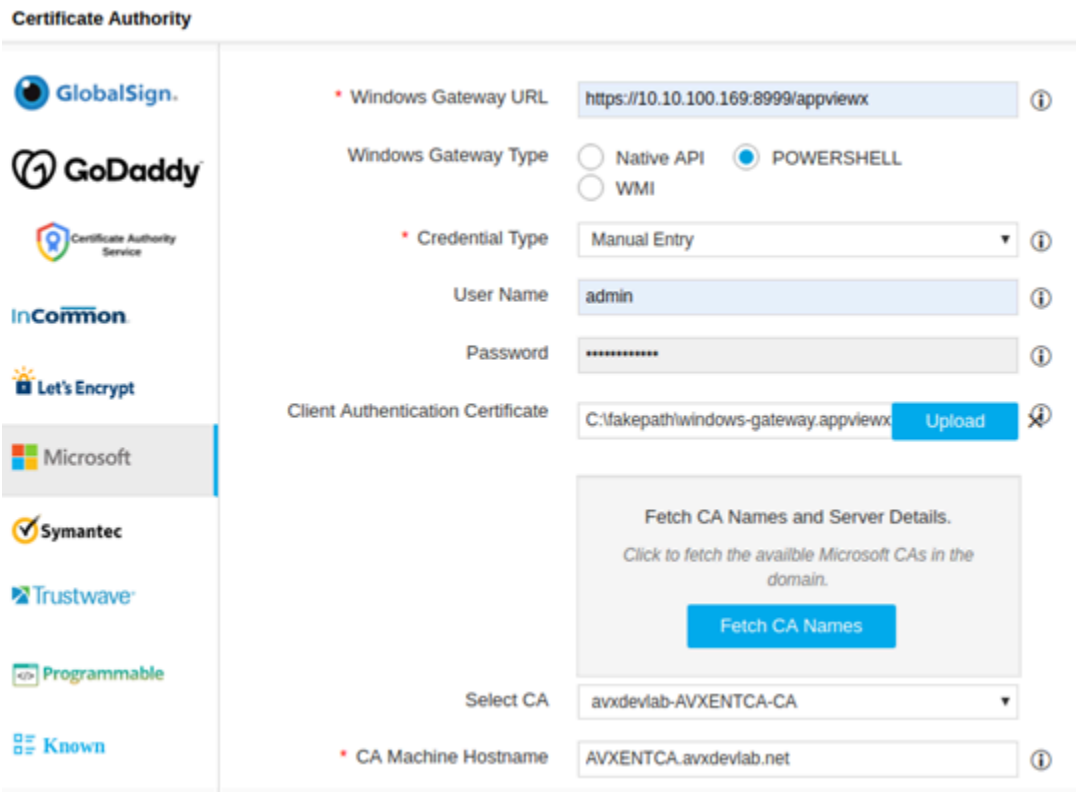
10. Click on one specific CA and proceed.



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



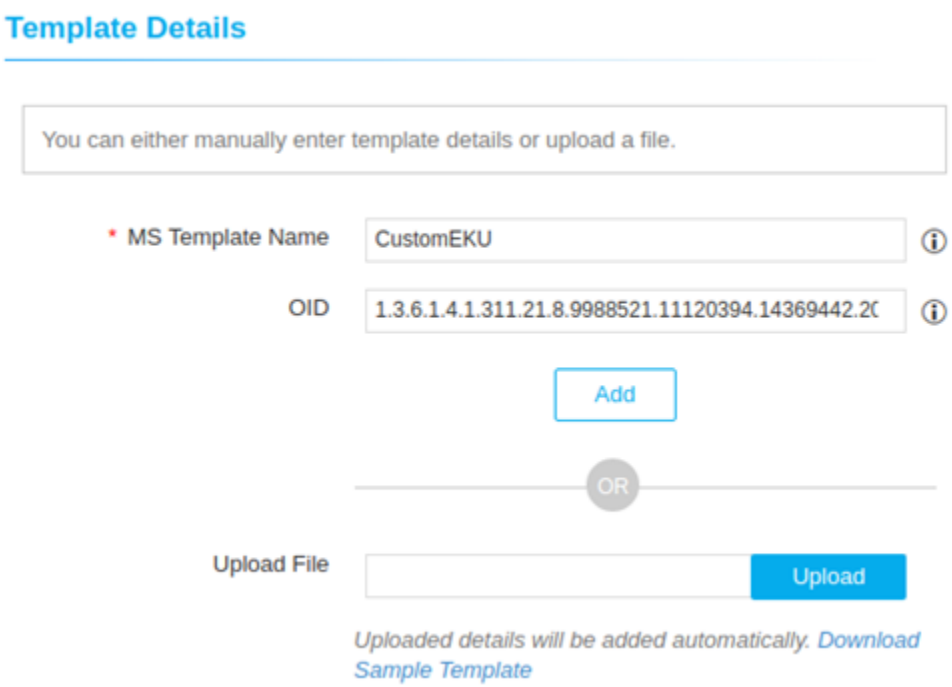
Using Powershell and WMI

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.



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,

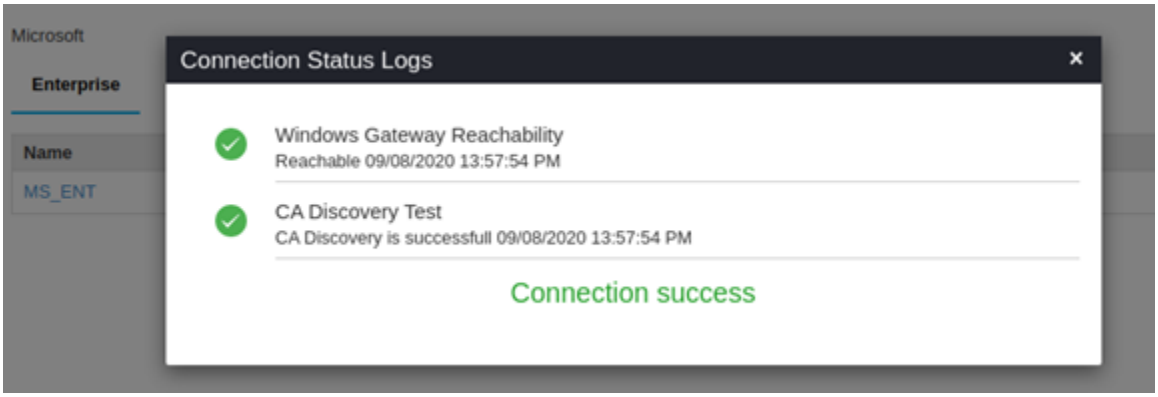
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

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

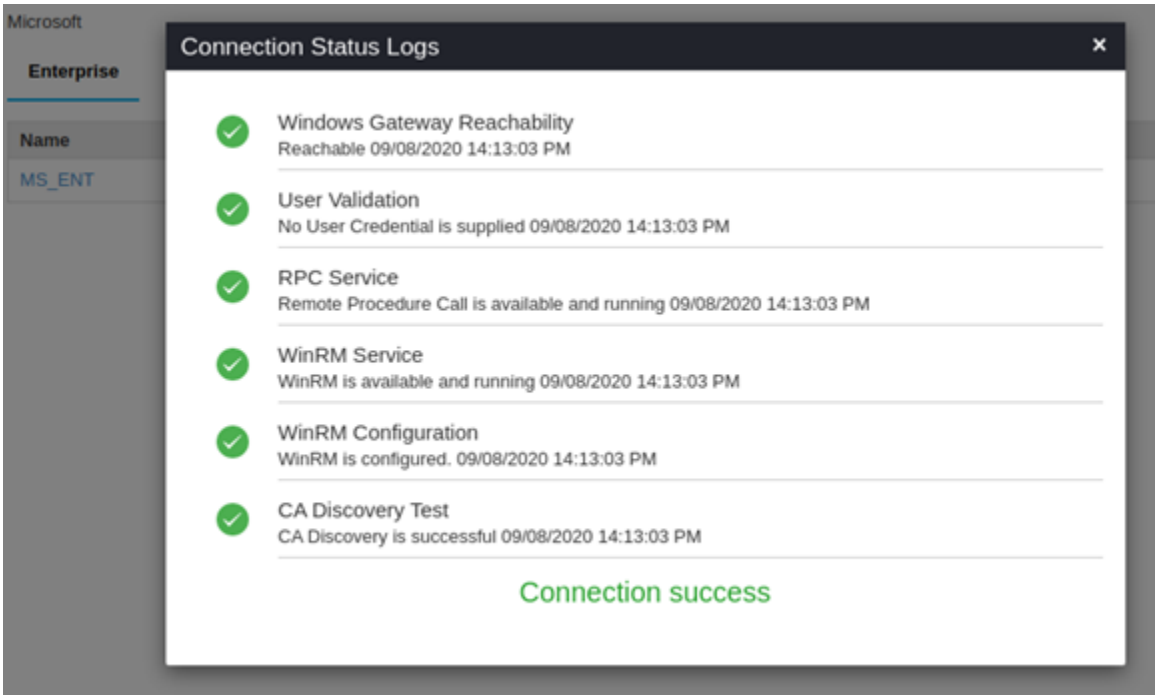
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Microsoft Enterprise**.
6. Click **Check** to validate the CA setting that has been created.

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

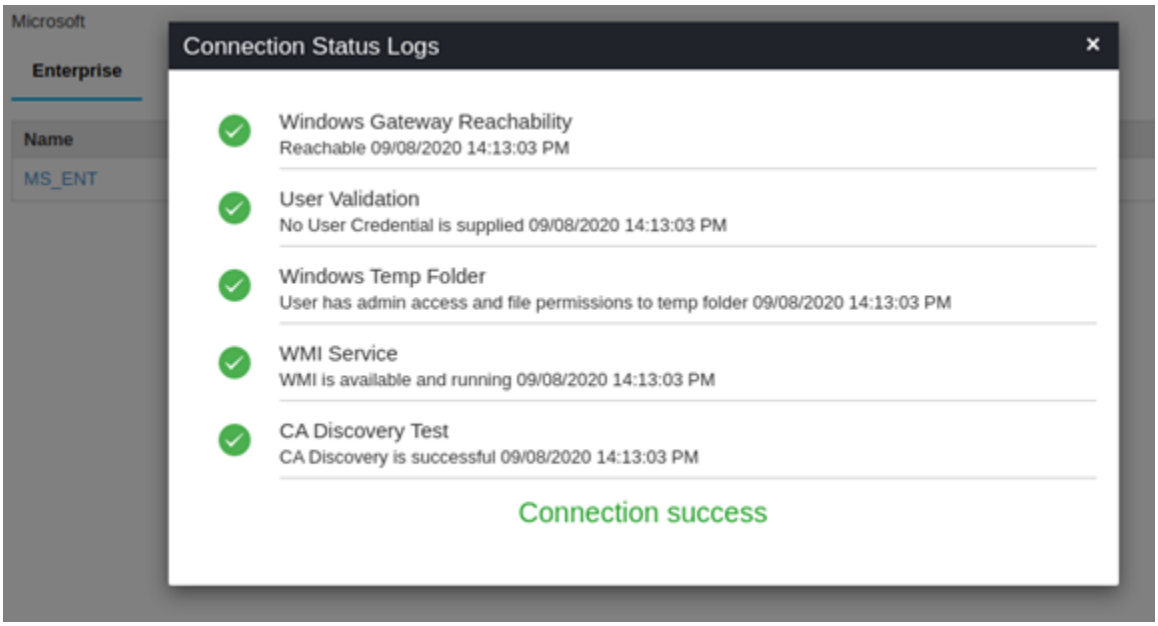
Success Message.



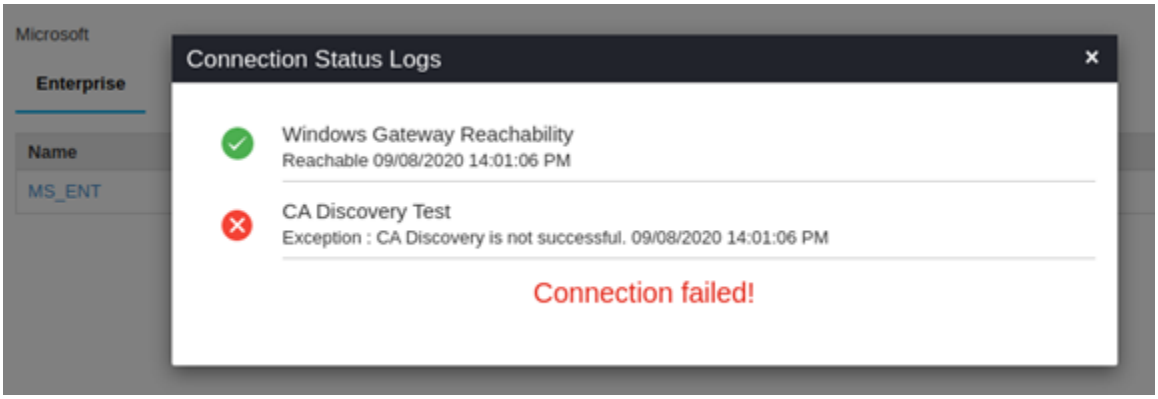
Success Scenario for Native API



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
	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

Communication mode	Category	Windows gateway machine	Microsoft CA
	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.

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, 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 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 APISuccess scenario for PowershellSuccess scenario for WMI

Symantec CA

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,

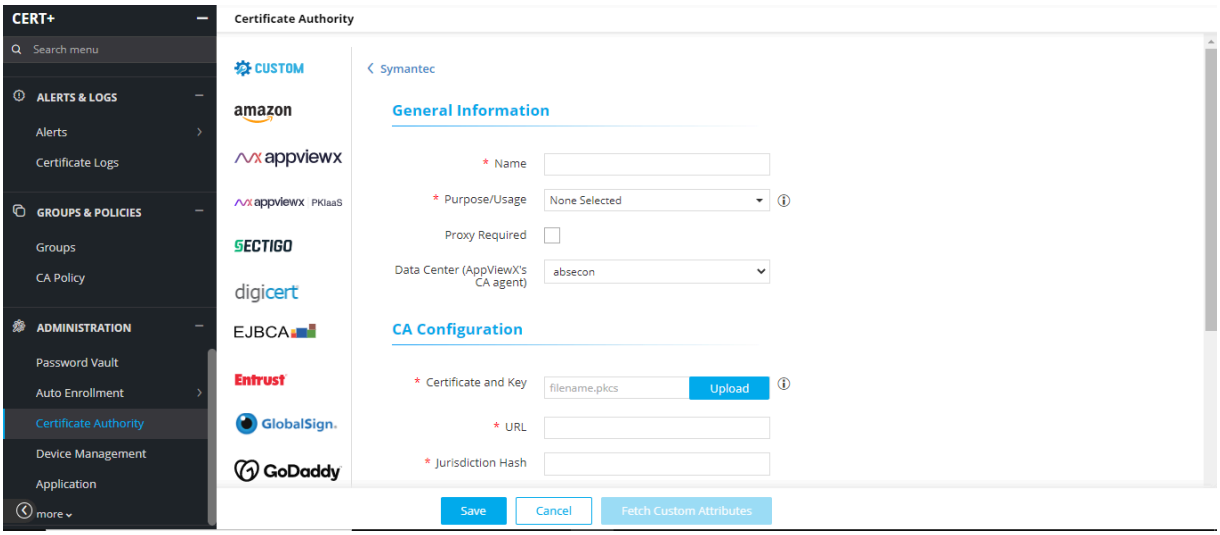
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   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.



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. 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.

Name	Description
	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,

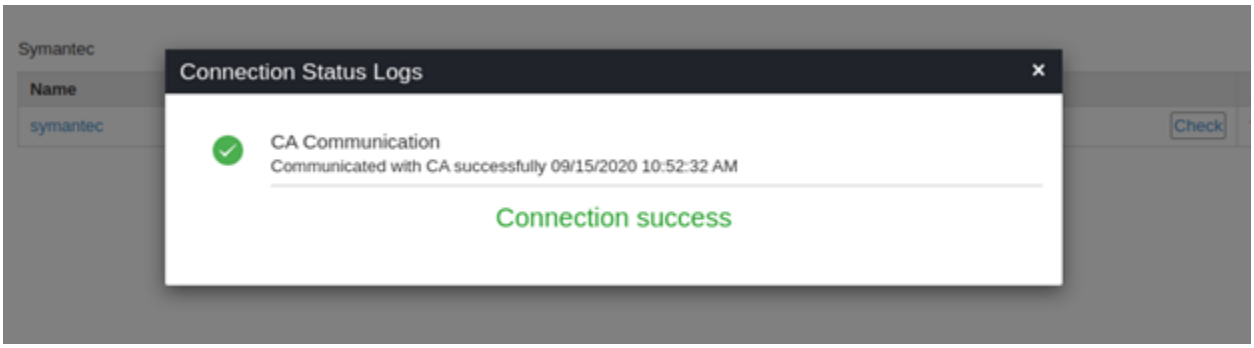
1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

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

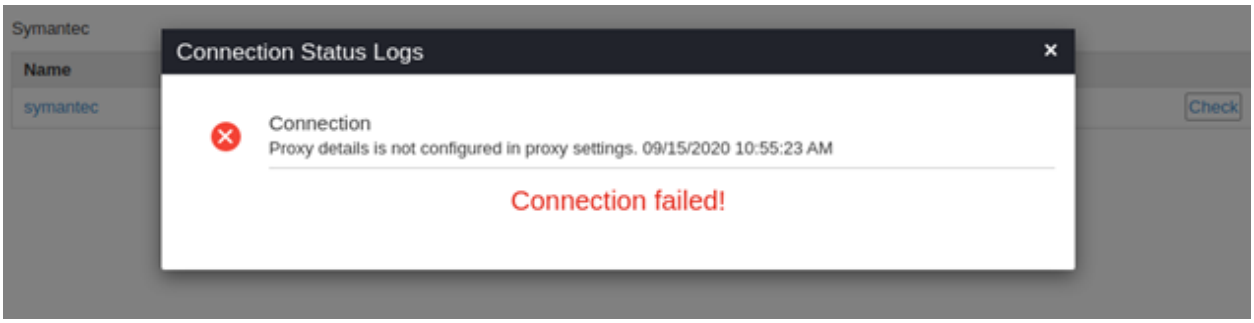
   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION**.
5. Click **Certificate Authority**, and then select **Symantec**.
6. Click **Check** to validate the CA setting that has been created.

   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 inTrustwave account such as Organization Name, Email address, Organization Address, City, State, Zip code, Country, Phone number
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Check Proxy Setup for the steps to configure the proxy. https://adminguide.appviewx.com/proxy-4

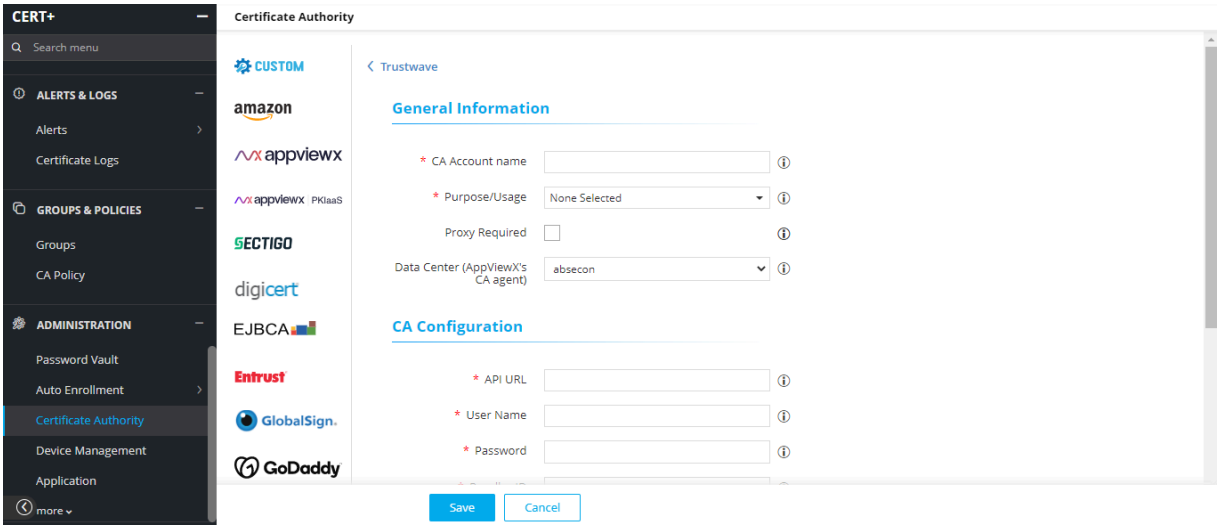
Configuring Trustwave CA

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



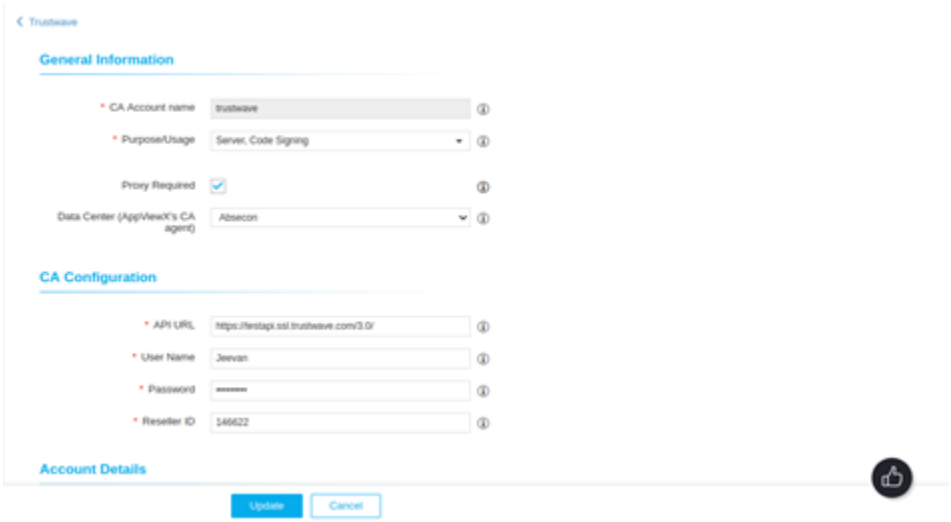
7. Configure the **General Information** details as follows:
   a. **CA Account name** - Provide an account name for the CA setting.
   b. **Purpose/Usage** - Choose the certificate categories that will be managed by this setting. Possible certificate categories could be:

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**.

Certificate Policy

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

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)*

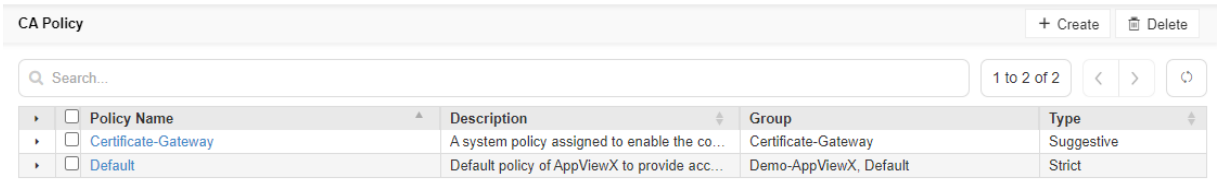
CERT > Policy > View Policy - To view the policy.

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

Configuring Policy Details

To configure policy:

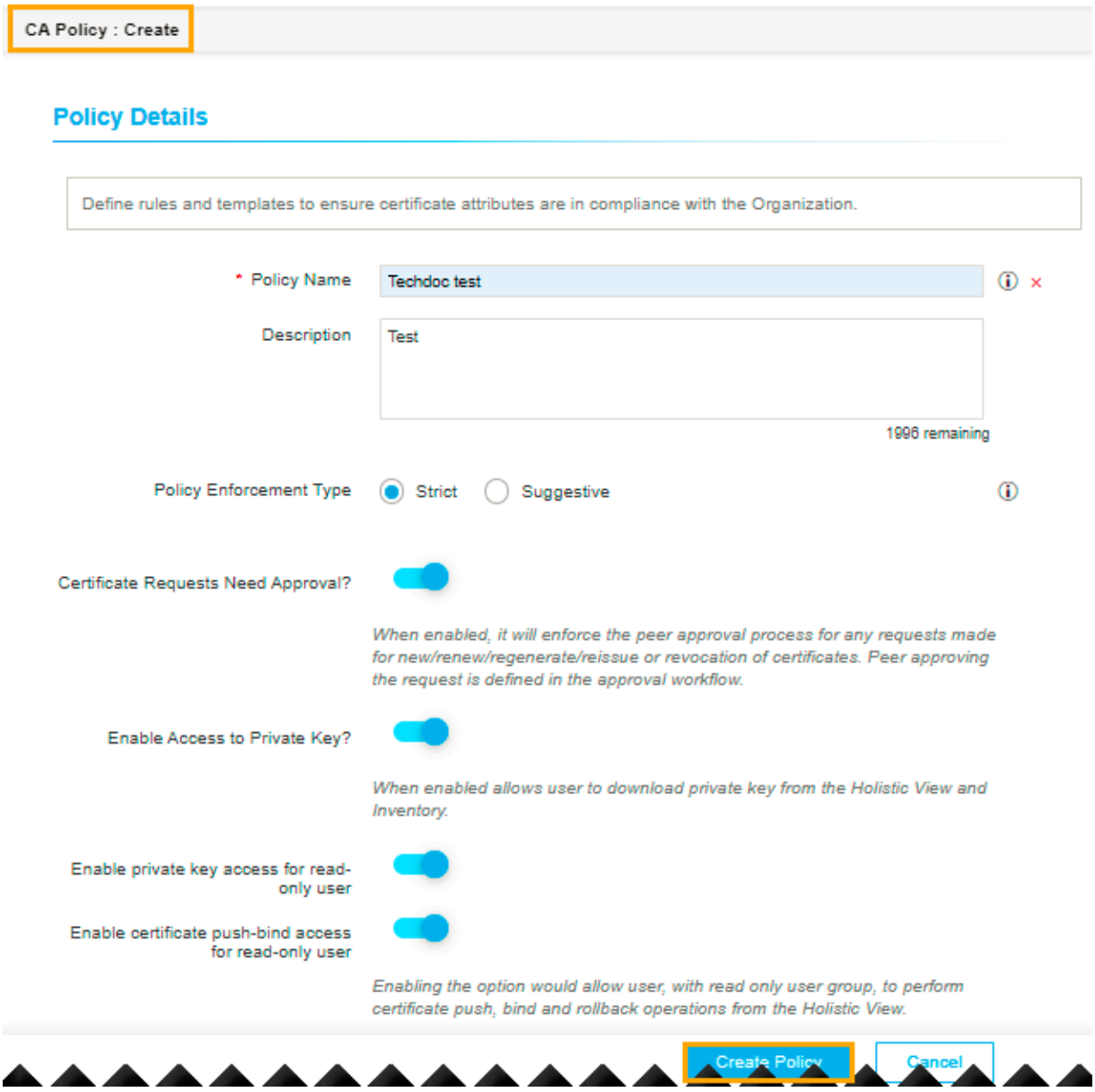
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**
   The CA Policy home page appears.



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

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

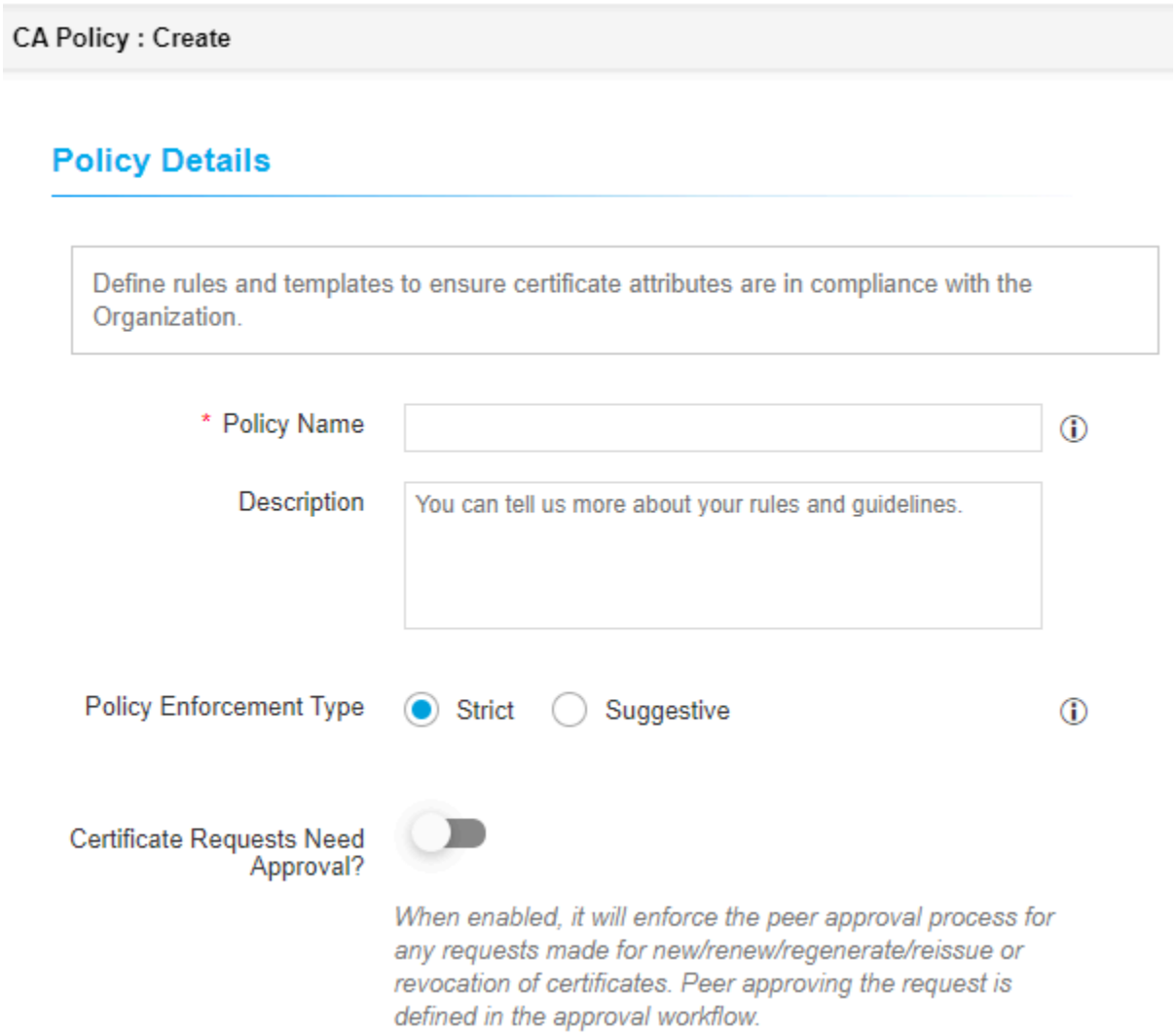
   The **Create** policy page appears.



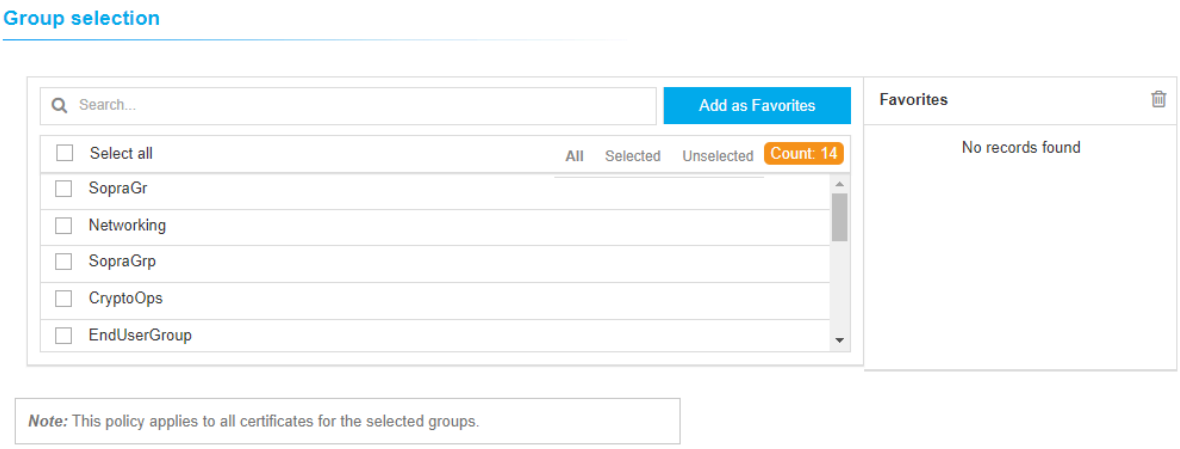
The following table provides the field description in the **Policy Details** section:

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.



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



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

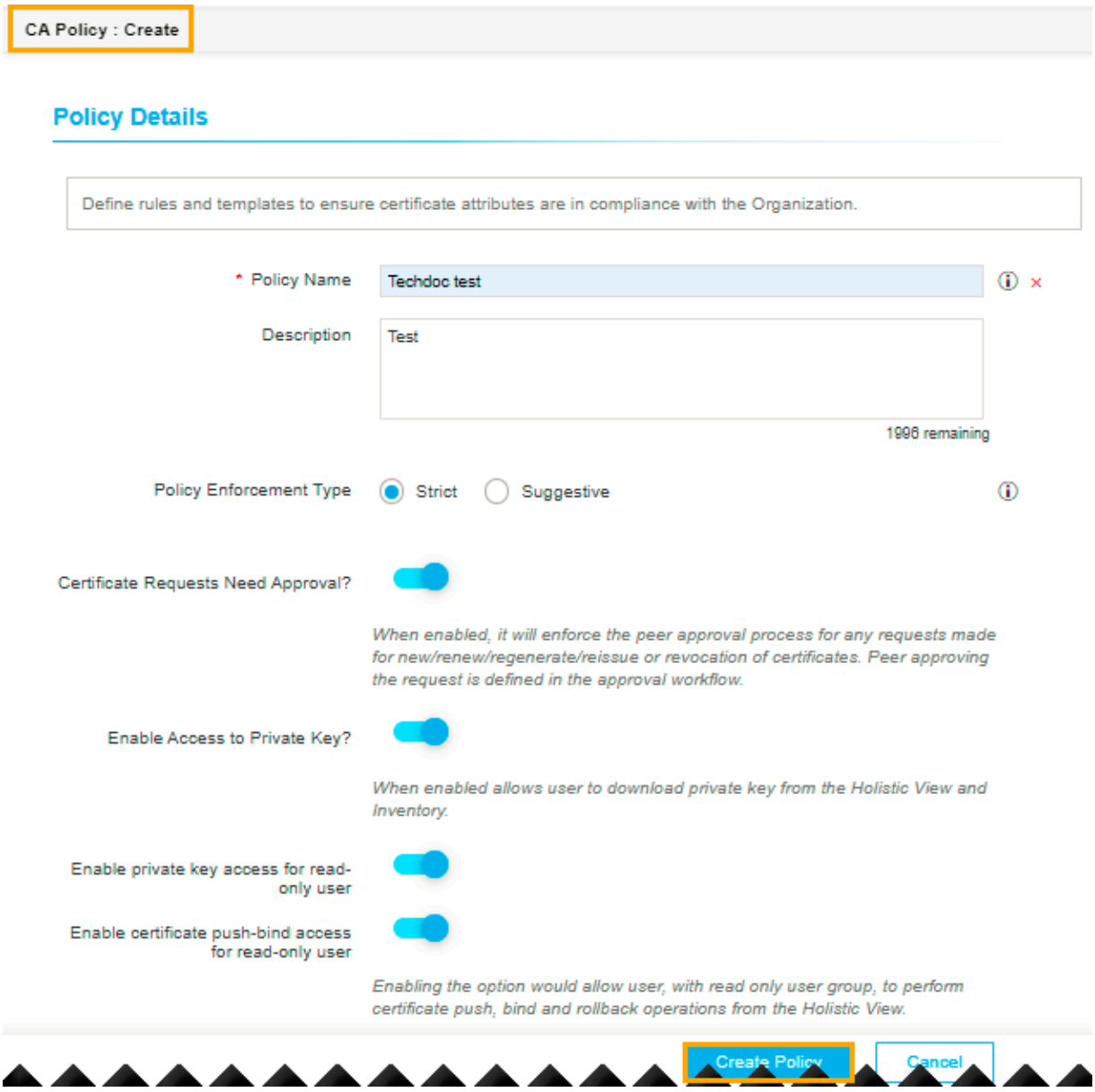
> **Note:** Scheduled Compliance check will run periodically based on the Job scheduler settings.

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.
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** 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:

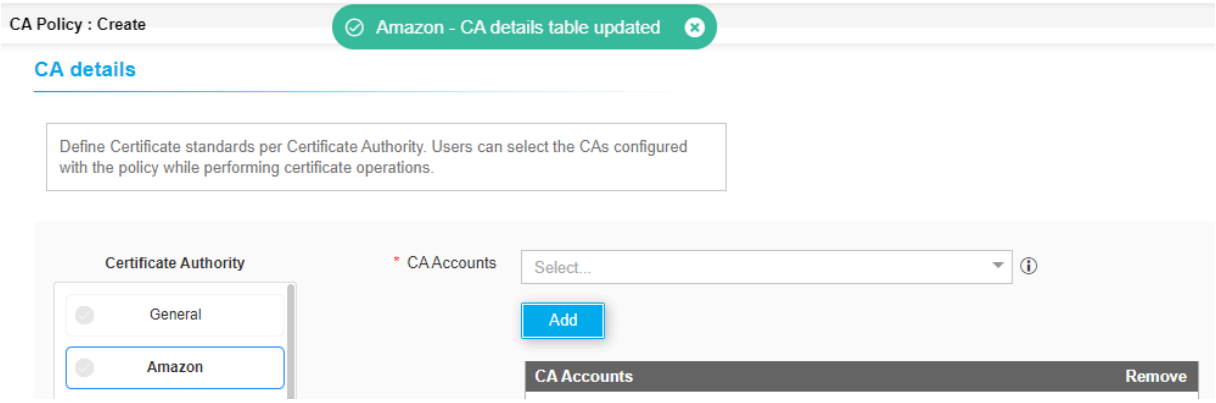
Name	Description
***CA Accounts**	The Amazon CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.

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

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

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 the **Bit Length -Key Type(s), ECDSA curve(s), and Hash Function(s).**

    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.

Name	Description
	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. **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.	

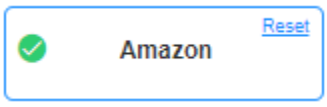
13. You can fill the **Certificate parameters** section based on your organization's policies and standards.

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

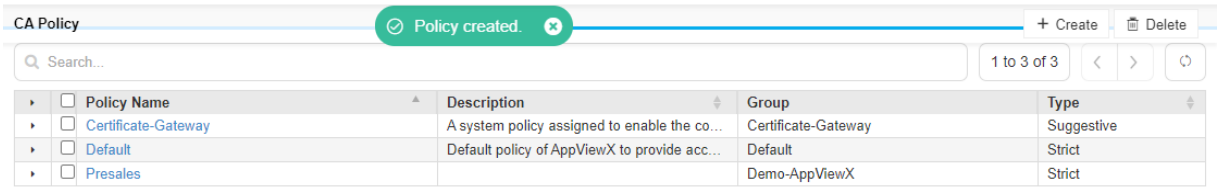
Name	Description
Common Name	You can provide the common name**.** For example, *.domain.com

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, 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 (.)
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 **Amazon** option to indicate the details are successfully stored.



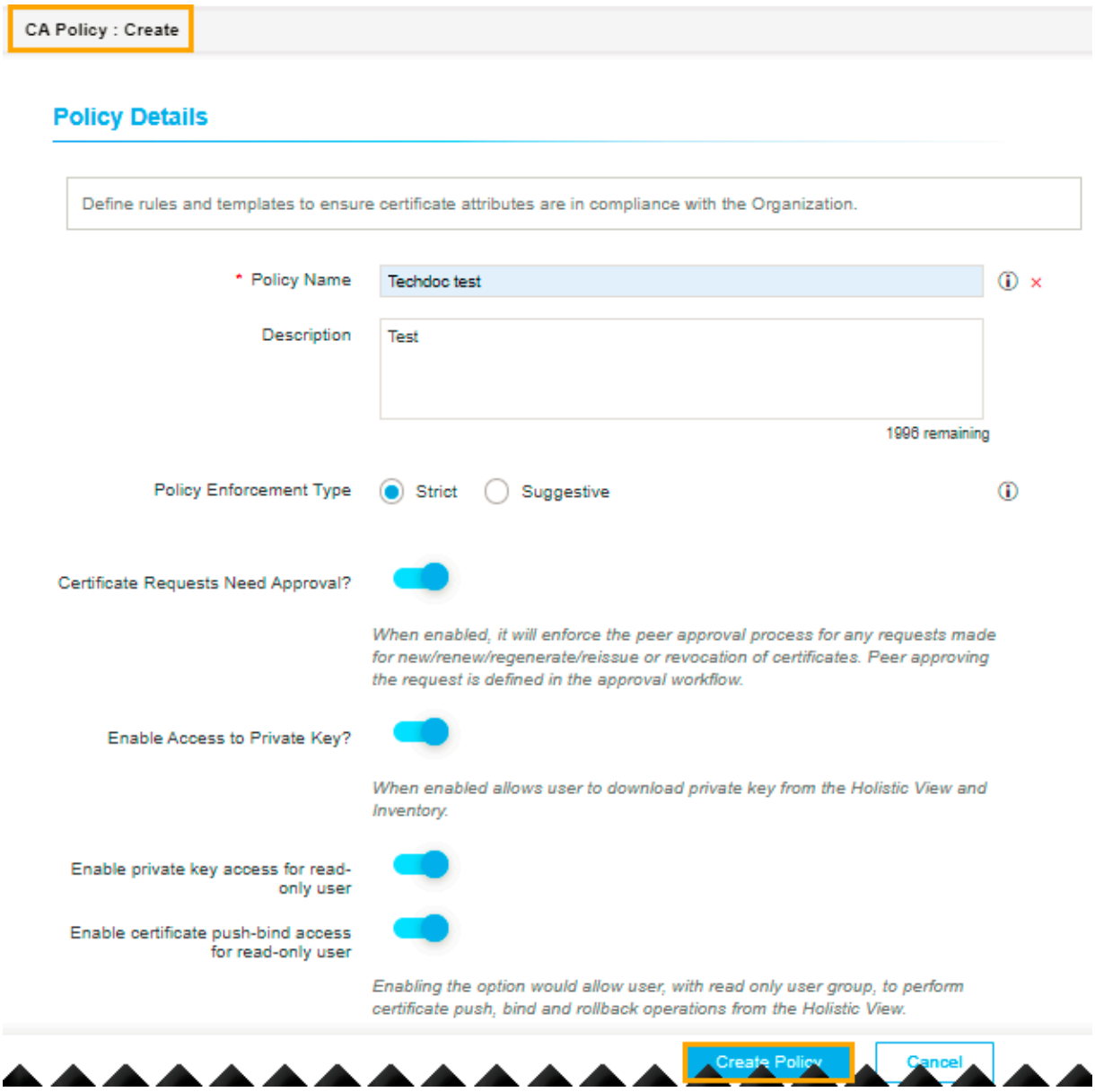
15. Click the **Create Policy** button to create a new policy.
16. The policy is created and a confirmation message displays.



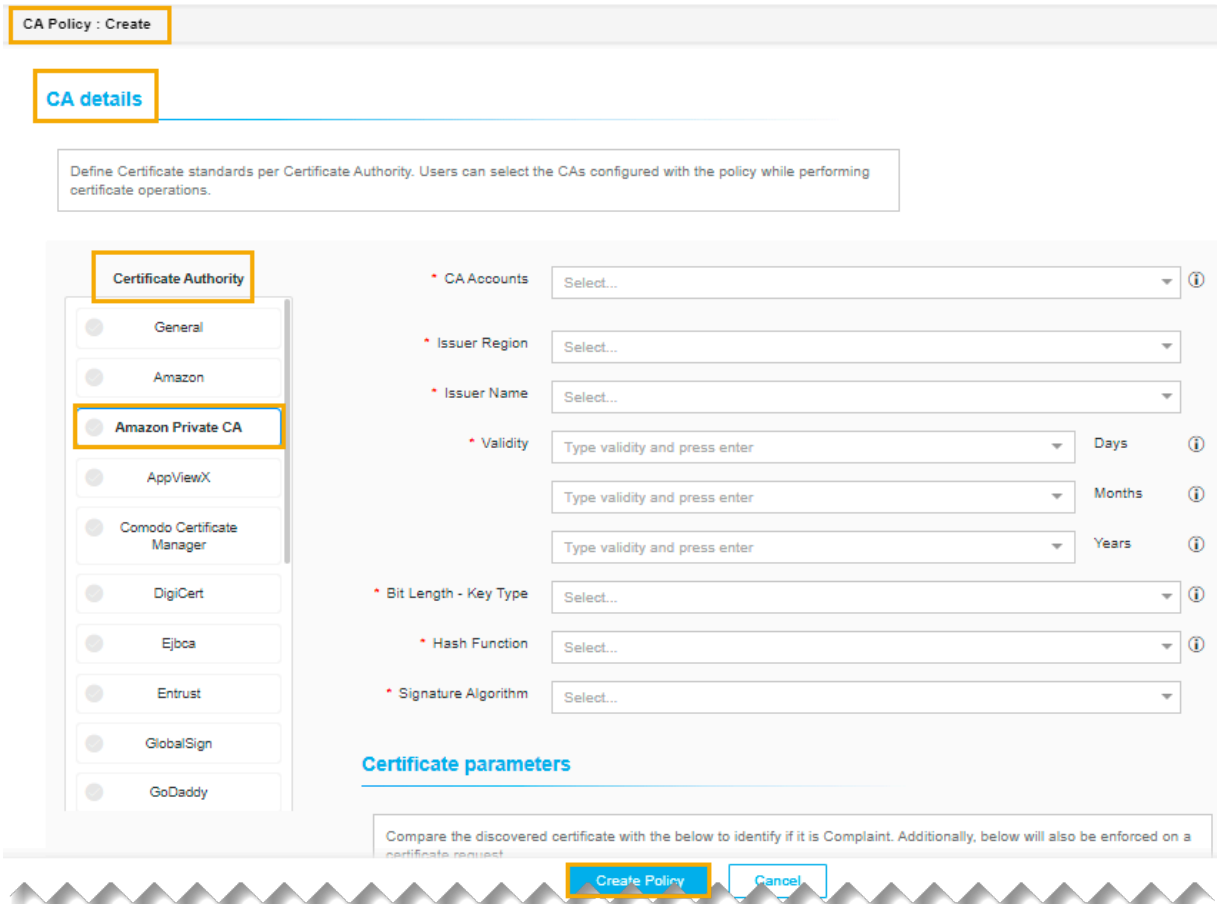
Configuring Policy for Amazon Private CA

- 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.**
   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 Amazon Private CA details, click **Amazon Private CA** 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 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.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Bit Length - Key Type</td><td>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>RSA</td><td>2048
4096</td></tr>
<tr><td>EC</td><td>prime256v1 sec384r1</td></tr>
</table>
</td></tr>
<tr><td>*Hash Function</td><td>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.</td></tr>
<tr><td>*Signature Algorithm</td><td>Select the SignAlgothirm from the dropdown list. The available options are:

• SHA256WITHECDSA
• SHA384WITHECDSA
• SHA512WITHECDSA
• SHA256WITHRSA
• SHA384WITHRSA
• SHA512WITHRSA.</td></tr>
</table>

Field	Description
	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.

   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.

Field	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, 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 (@)

10. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against **the Amazon** option to indicate the details are successfully stored.
11. Click the **Create Policy** button to create a new policy.

    The policy is created and a confirmation message displays.

Configuring Policy for Digicert CA

To configure a Digicert CA policy,

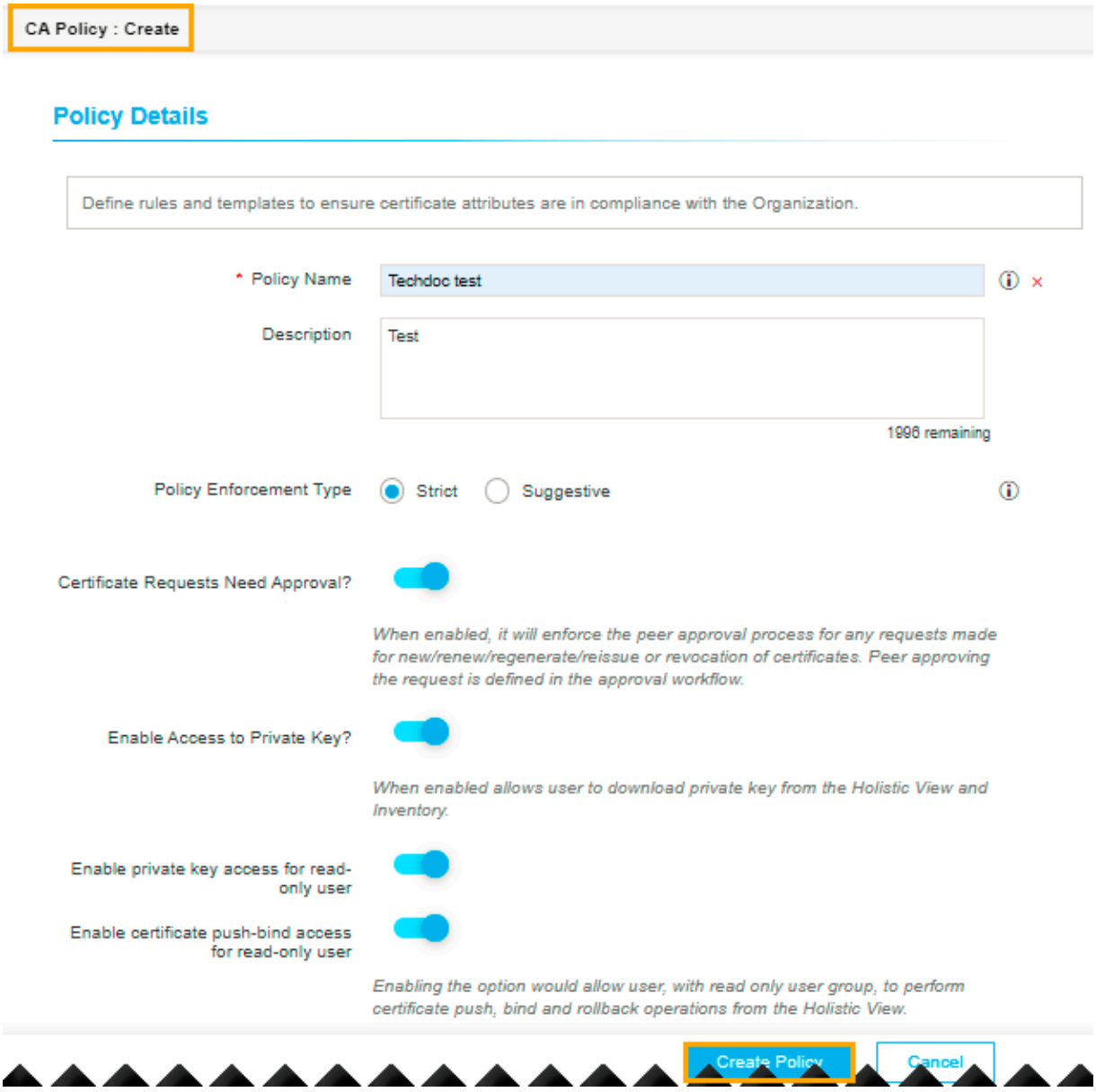
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.

3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**

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

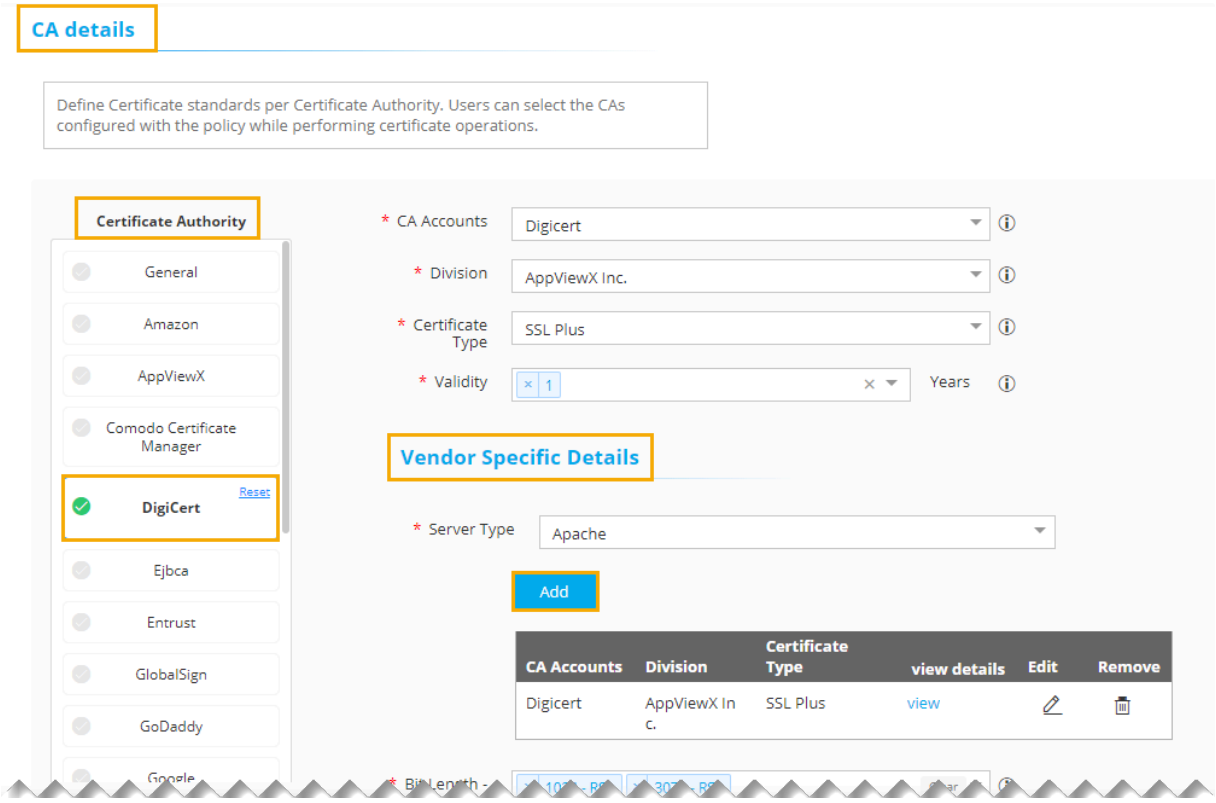
   The **Create** policy page appears.



7. Refer Configuring Policy Details section in admin guide to configure,

- **Policy Details**
- **Group Selection**
- **Compliance Check**

8. To configure a policy with Digicert details, click Digicert 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 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:

Field	Description
	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

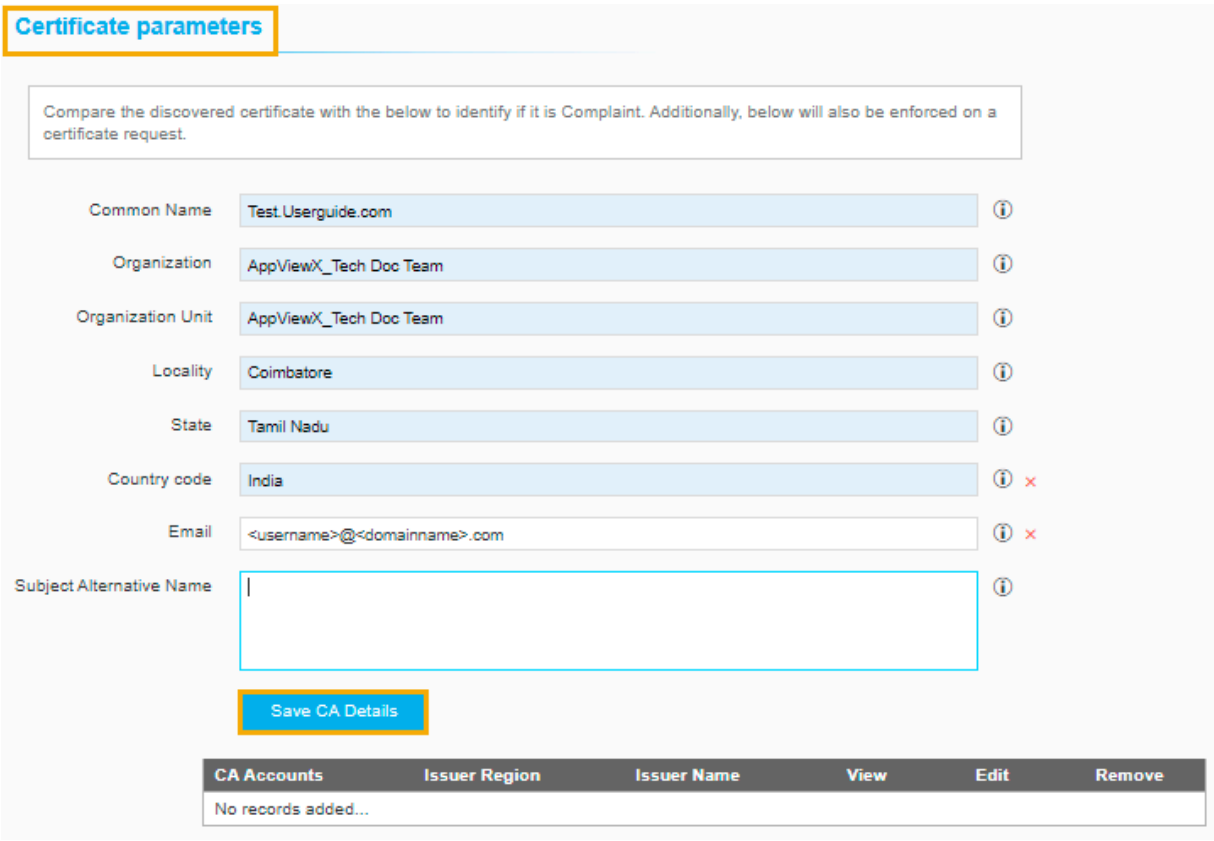
Field	Description
***Server Type**	Select the server type from the dropdown list.
Note: The asterisk (*) symbol indicates a mandatory field.	

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.**

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, 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 **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.

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 **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.

Configuring Policy for EJBCA CA

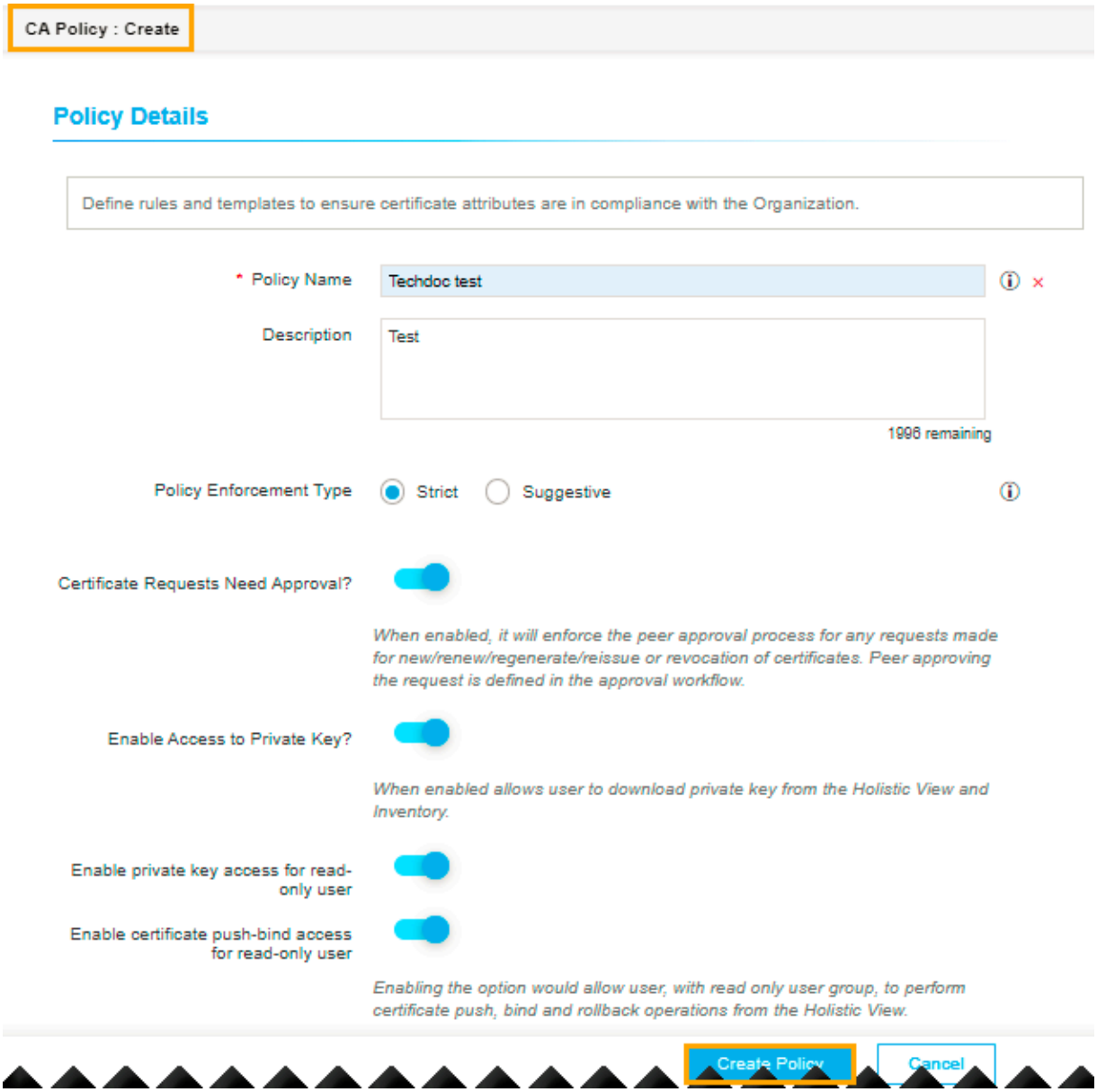
To configure an EJBCA CA policy,

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.

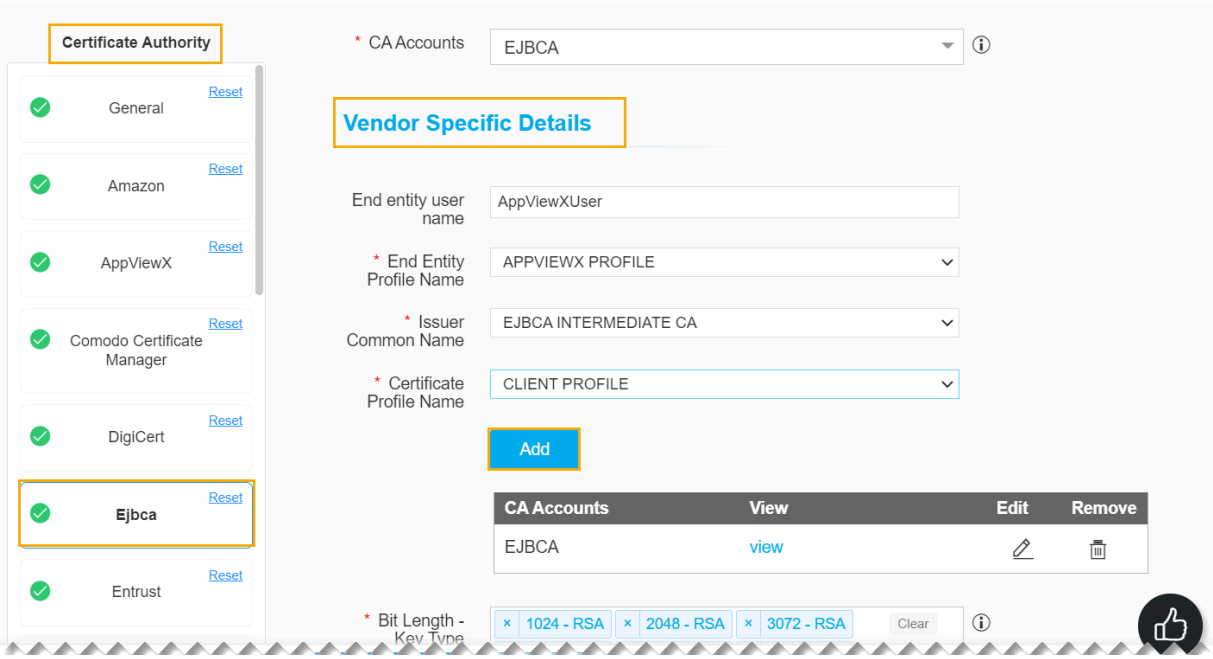
6. Click **+ Create** on the top-right of the page.

   The **Create** policy page appears.



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 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.

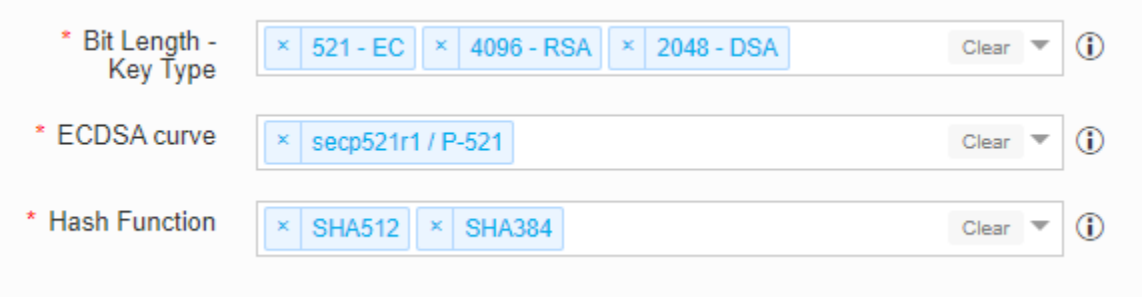
9. In the **Vendor Specific Details section**, select/enter the details as listed in the table.

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.

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.**

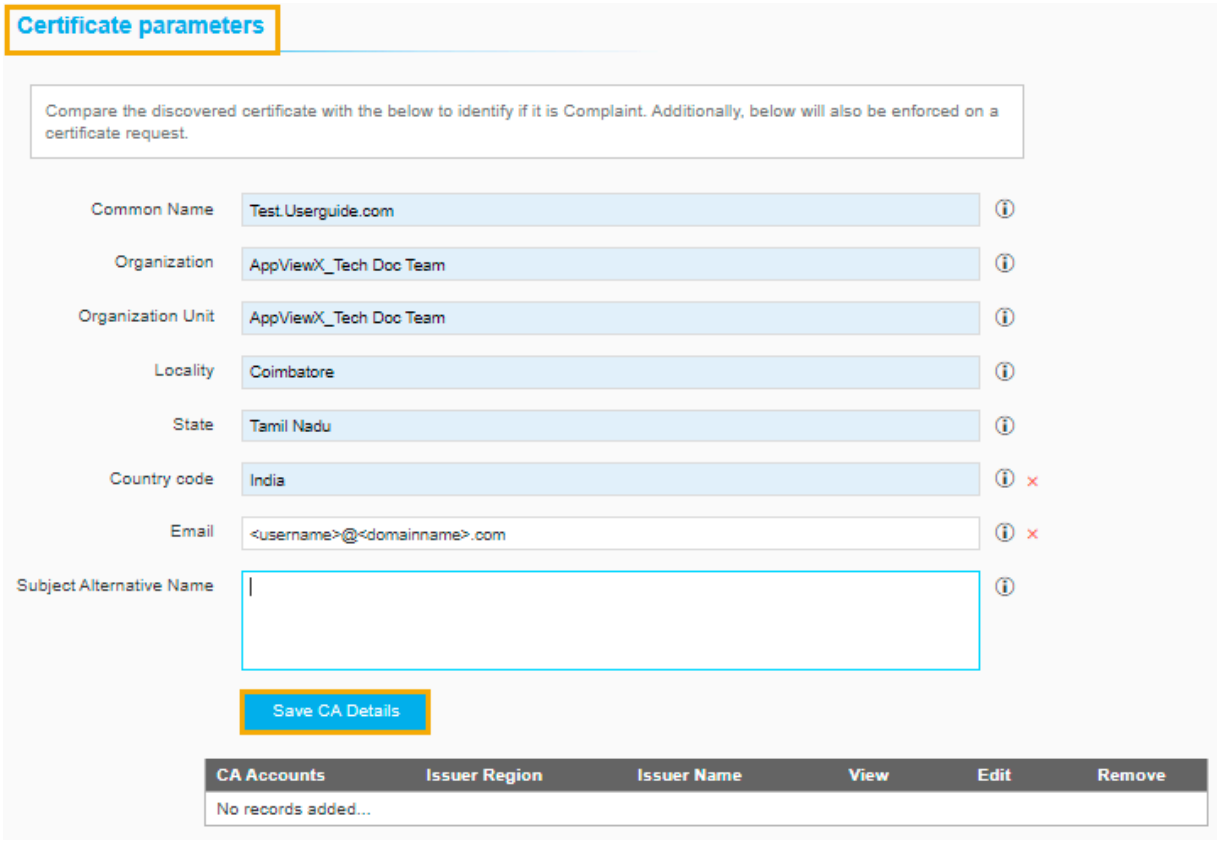


The following table provides the description of other fields in the **CA Details** section:

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.

Name	Description	Purpose
***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 the **Certificate parameters** section based on your organization's policies and standards.



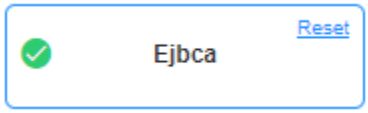
The following table provides the field description under the **Certificate parameters** section:

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, 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**

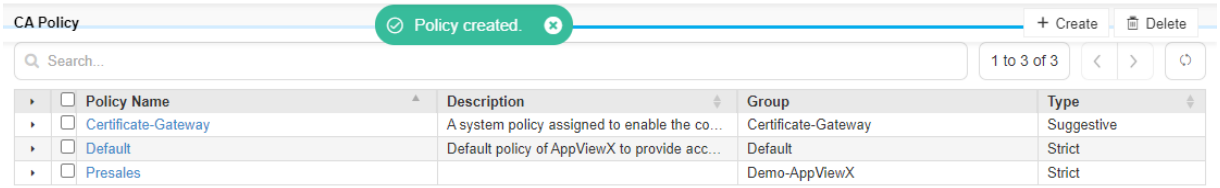
Name	Description
	organization is enforced while performing any certificate request operations such as New, Renew, and Regenerate.
Organization Unit	You can provide an organization unit. The discovered certificate's **Subject Organization Unit** will be compared against the organization unit provided 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 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.

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 (@)

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.

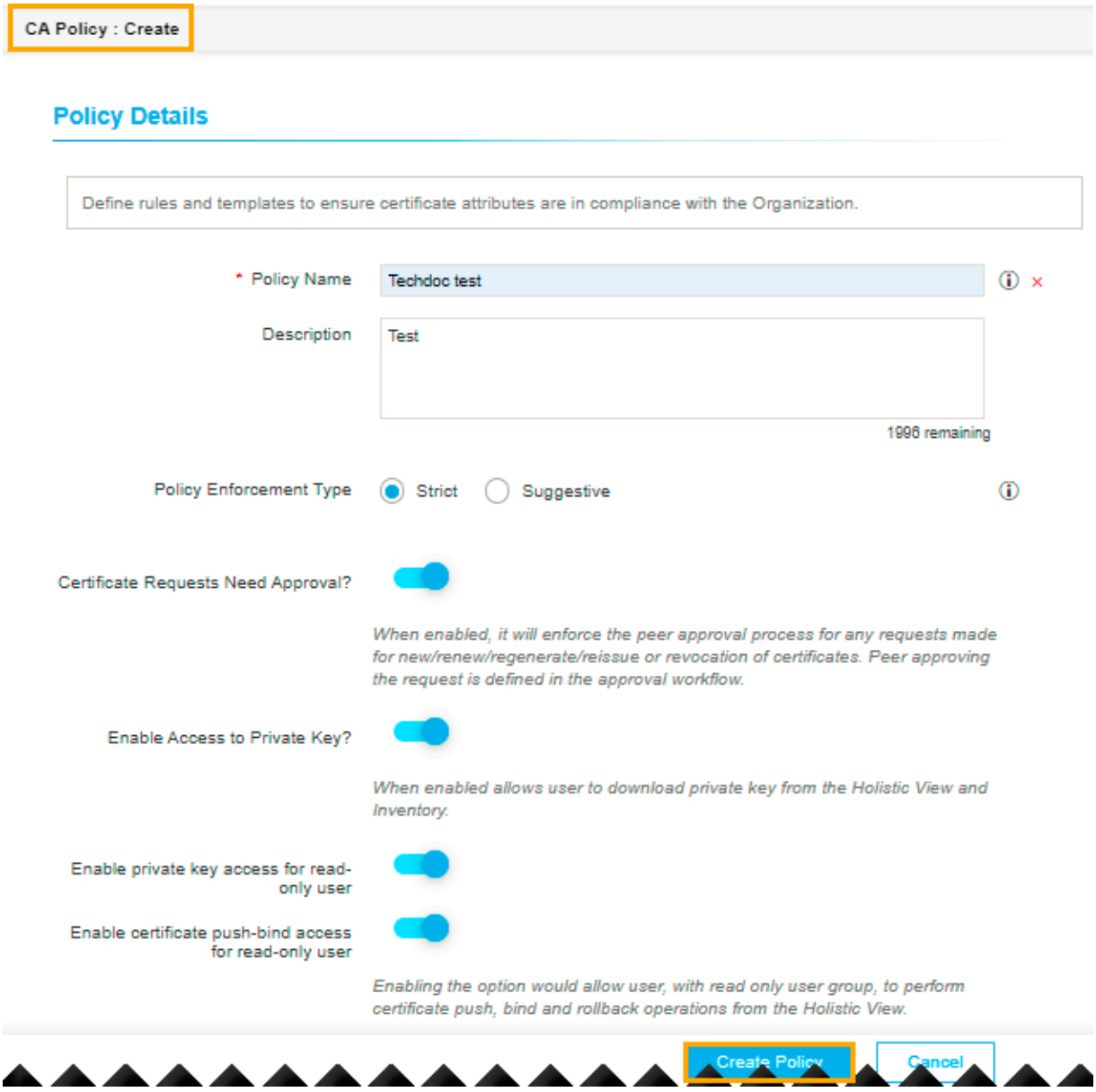


Configuring Policy for Entrust CA

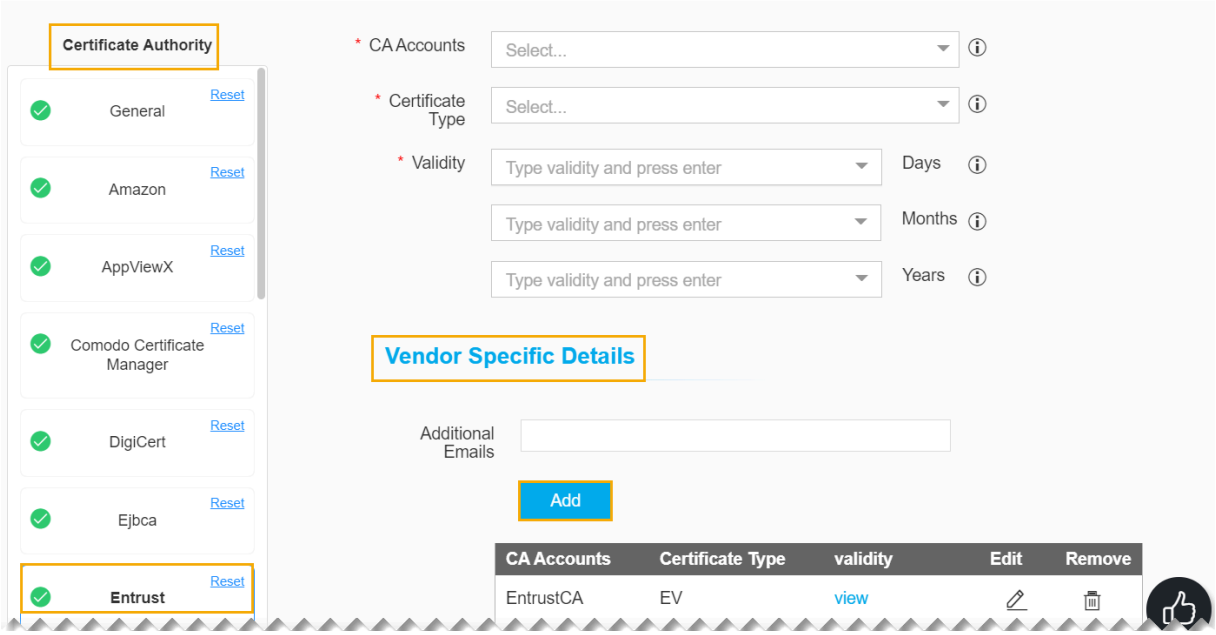
To configure an Entrust CA policy,

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.**
   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 Entrust details, click Entrust 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 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.

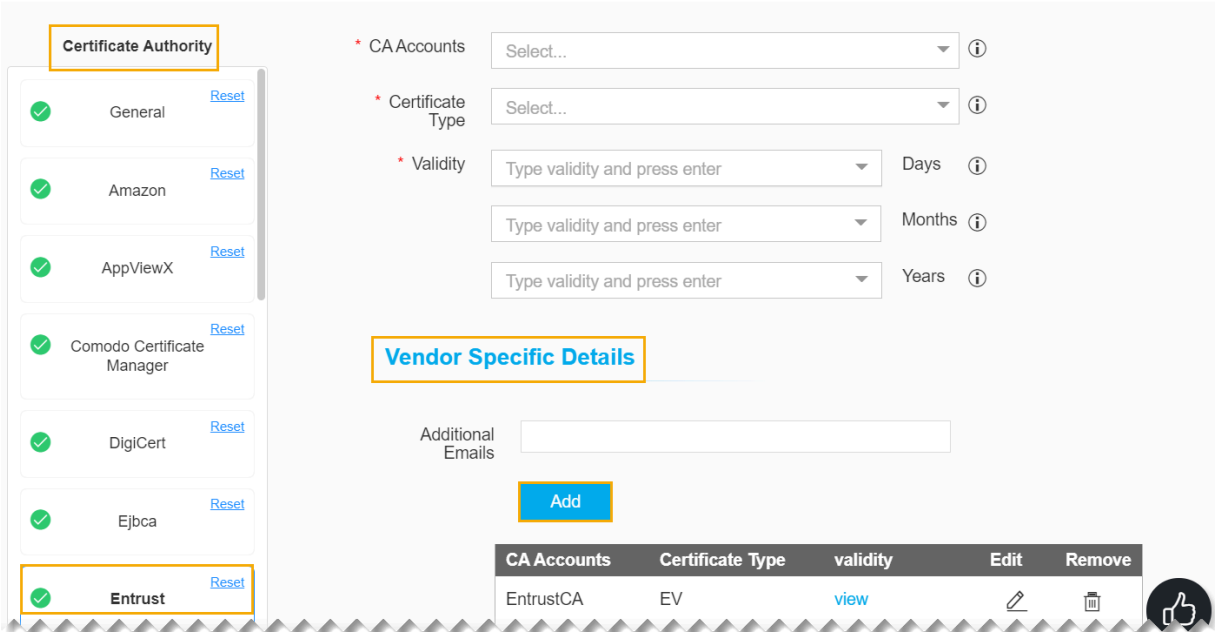
9. In the **Vendor Specific Details section**, select/enter the details as listed in the table:

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

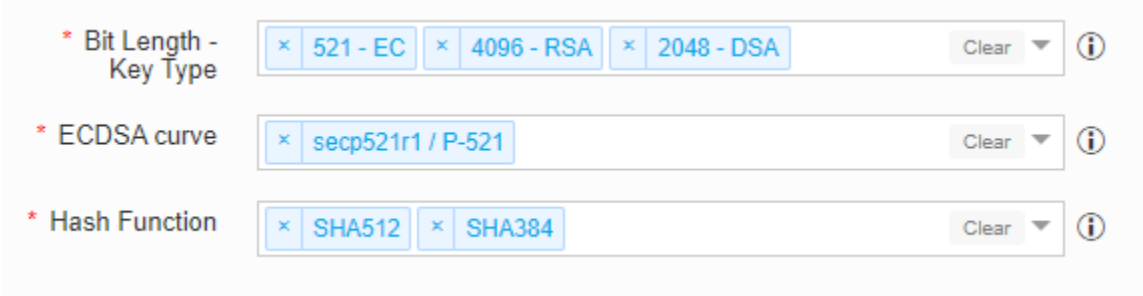
10. Click the **Add** button.

    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.



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

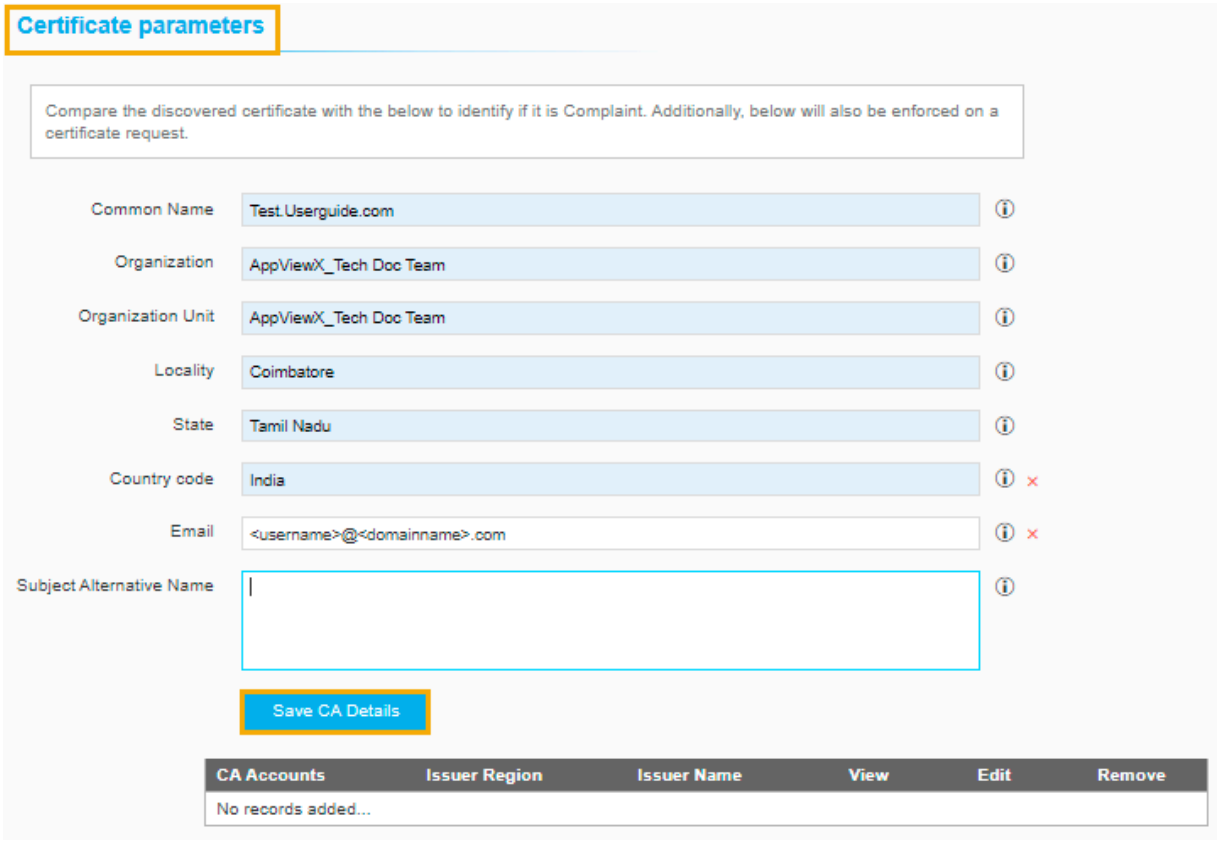


The following table provides the field description in the **CA Details** section:

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	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

Name	Description	Purpose
	Bit Length - Key Type(s) from the drop-down.	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** 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.



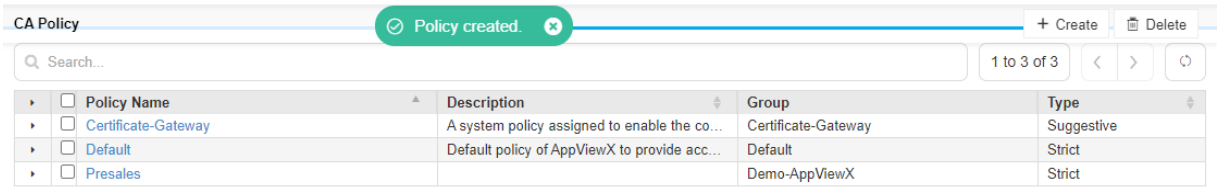
The following table provides the field description under **the Certificate parameters** section:

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, 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**

Name	Description
	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 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 (@)

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.



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

9. 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, and Regenerate. **Note:**

Name	Description
	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 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.	

10. 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.

Configuring Policy for GlobalSign CA

To configure a GlobalSign CA policy,

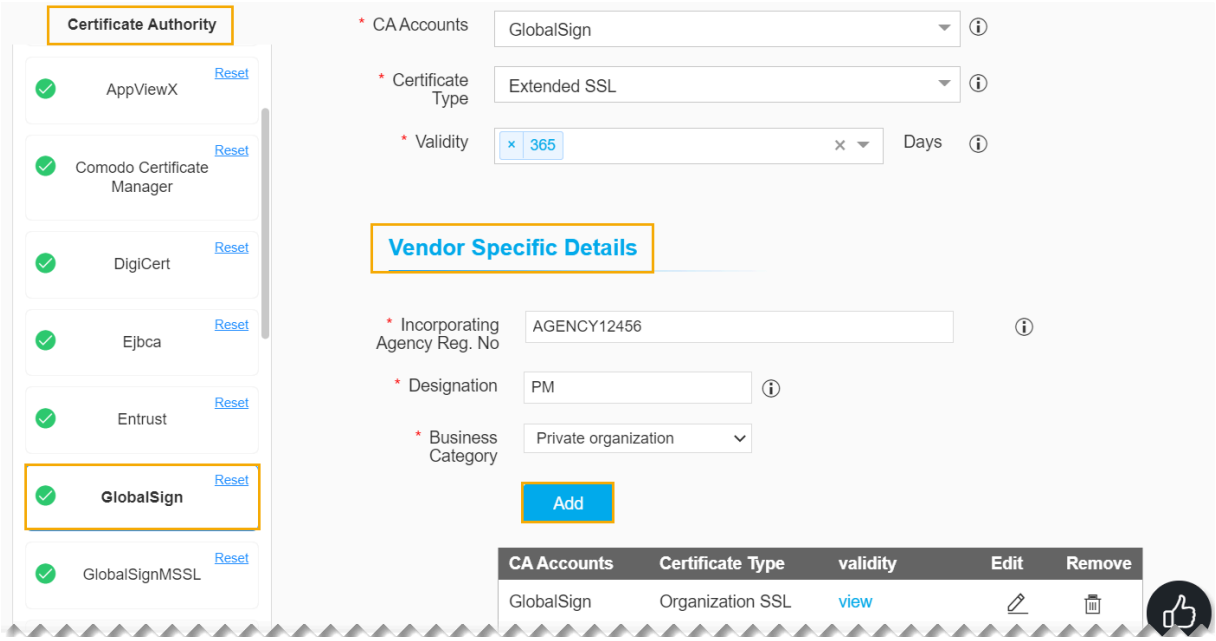
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.

3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**

   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 GlobalSign details, click **GlobalSign** in the **Certificate Authority** pane on the left side of the page.



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

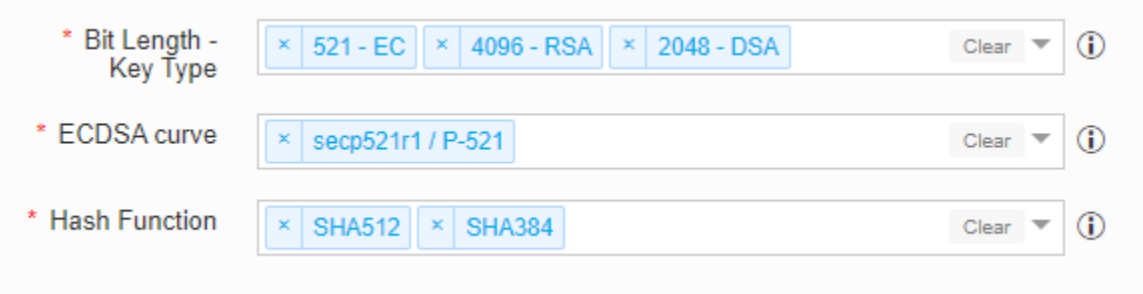
Field	Description
*Incorporating Agency Reg. No	Enter the agency registration number.
*Designation	Enter the designation.

Field	Description
*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.**

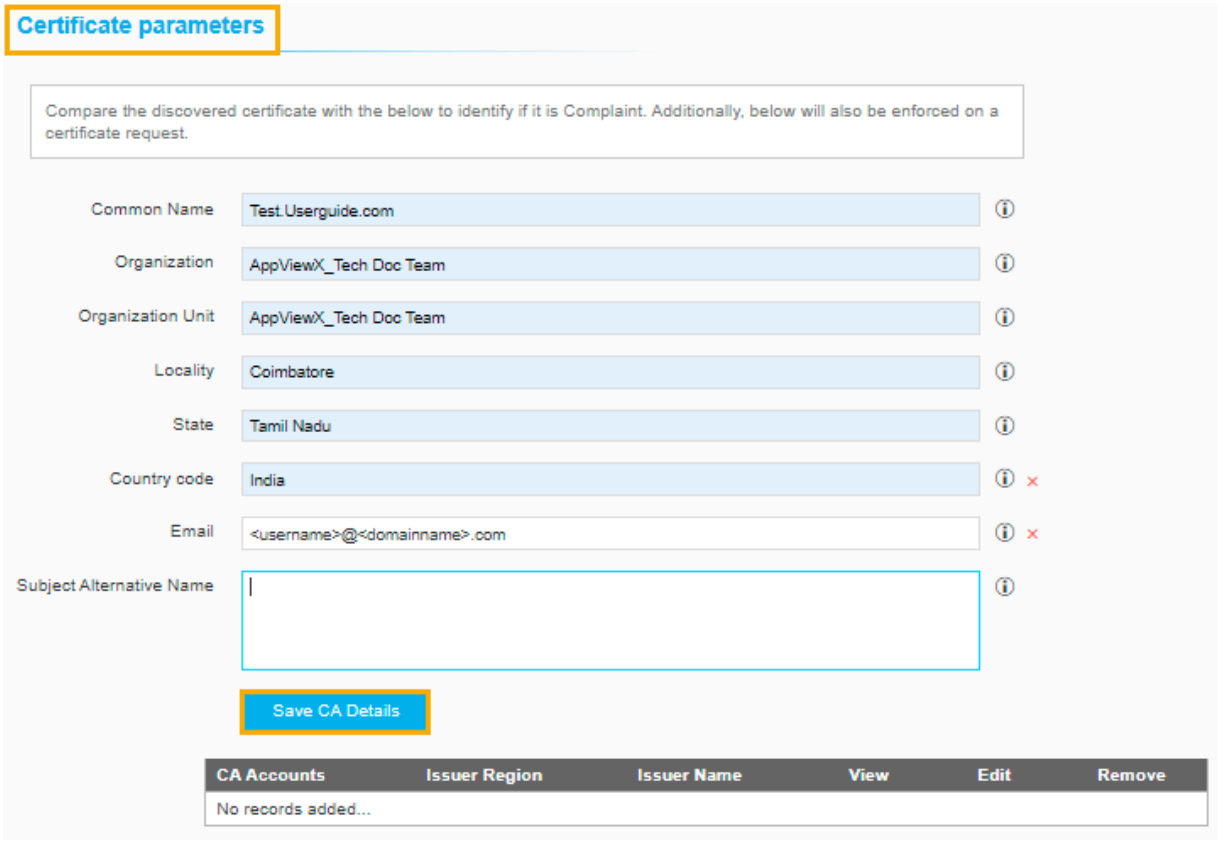


The following table provides the field description in the **CA Details** section:

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**	The discovered certificate's Key elliptic curves will be compared against the selected **ECDSA curve(s)** to identify if they are

Name	Description	Purpose
	curve from the drop-down. for a certificate.	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 the **Certificate parameters** section based on your organization's policies and standards.



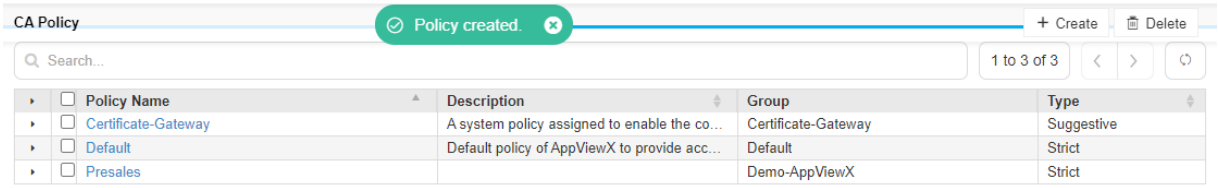
The following table provides the field description **in the Certificate parameters** section:

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

Name	Description
	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. 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

Name	Description
	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.



Configuring Policy for GoDaddy CA

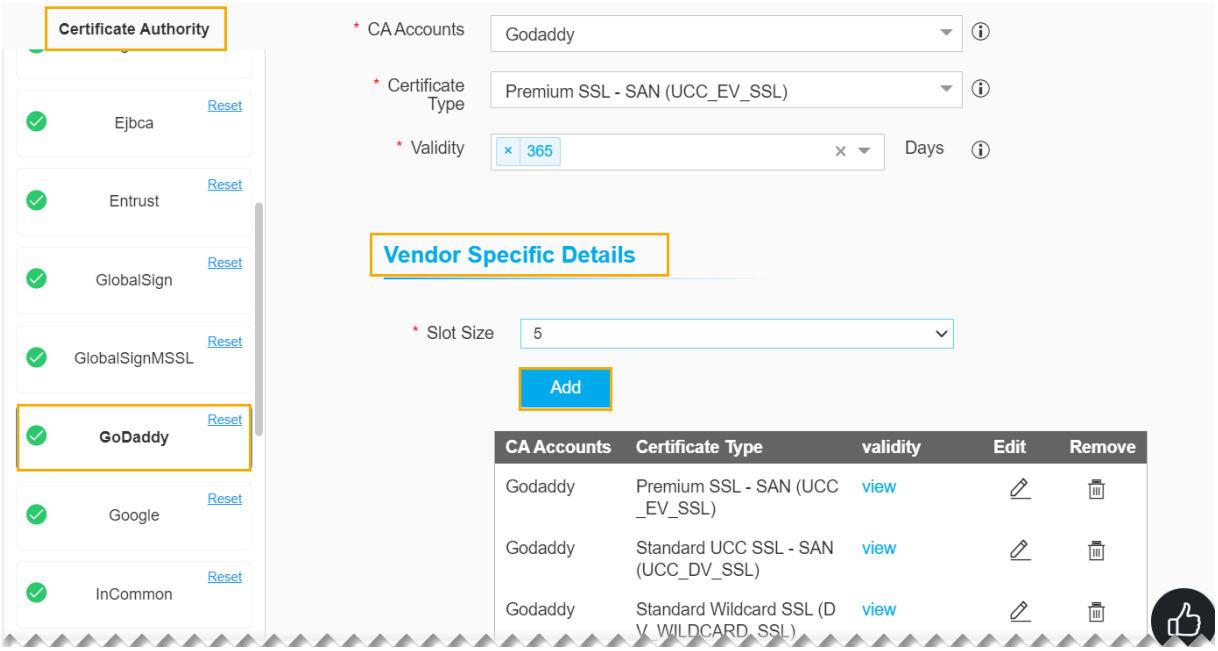
To configure a GoDaddy CA policy,

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.



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.

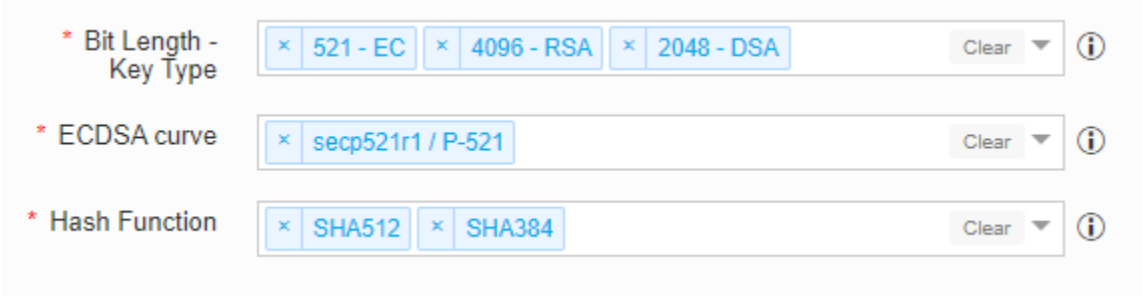
Field	Description
	Month - You can enter more than one validity period in Months, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment.
Note: The asterisk (*) symbol indicates a mandatory field.	

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.

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

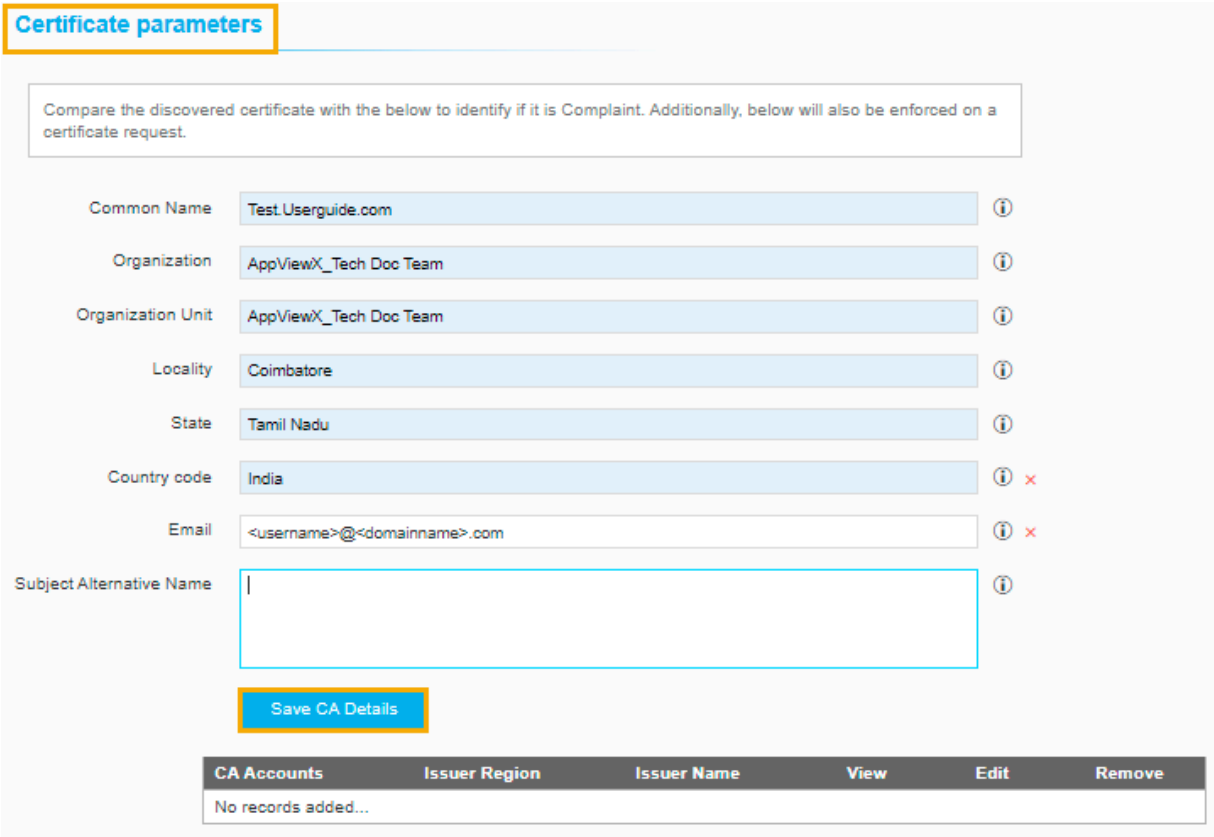


The following table provides the description of other fields under the **CA Details** section:

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 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.



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

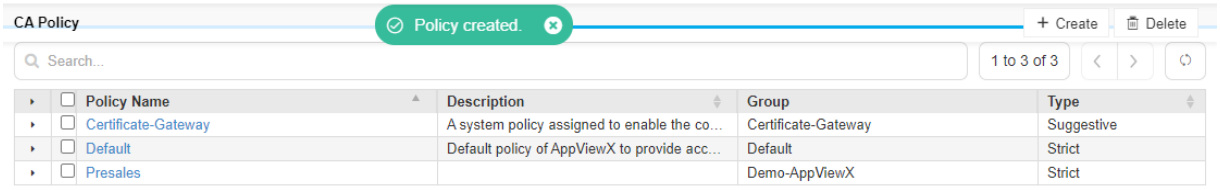
Name	Description
Common Name	You can provide the common name**.** For example, *.domain.com It helps enforce domains for which a certificate can be requested. **Common Name** is enforced while performing any certificate request operations such as New, Renew, and Regenerate. **Note:** Use Asterisk (*)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

Name	Description
	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.



Configuring Policy for Google CA

To configure a Google CA policy,

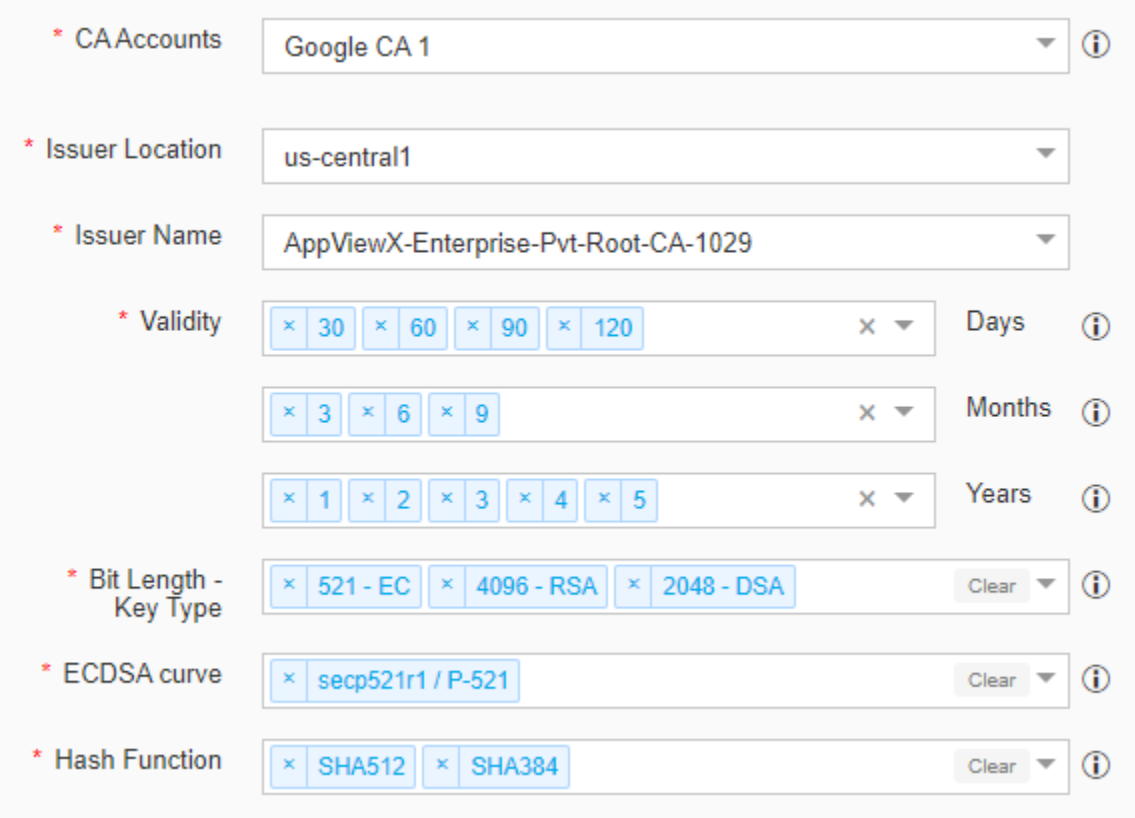
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**

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 Google details, click Google in the **Certificate Authority** pane on the left side of the page.

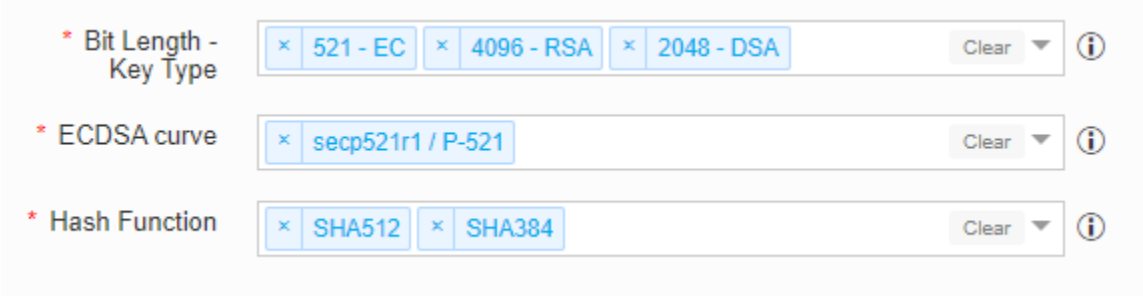


The following table provides the field description **in the CA Details** section:

Field	Description
***CA Accounts**	The Google CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.

Field	Description
***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).**

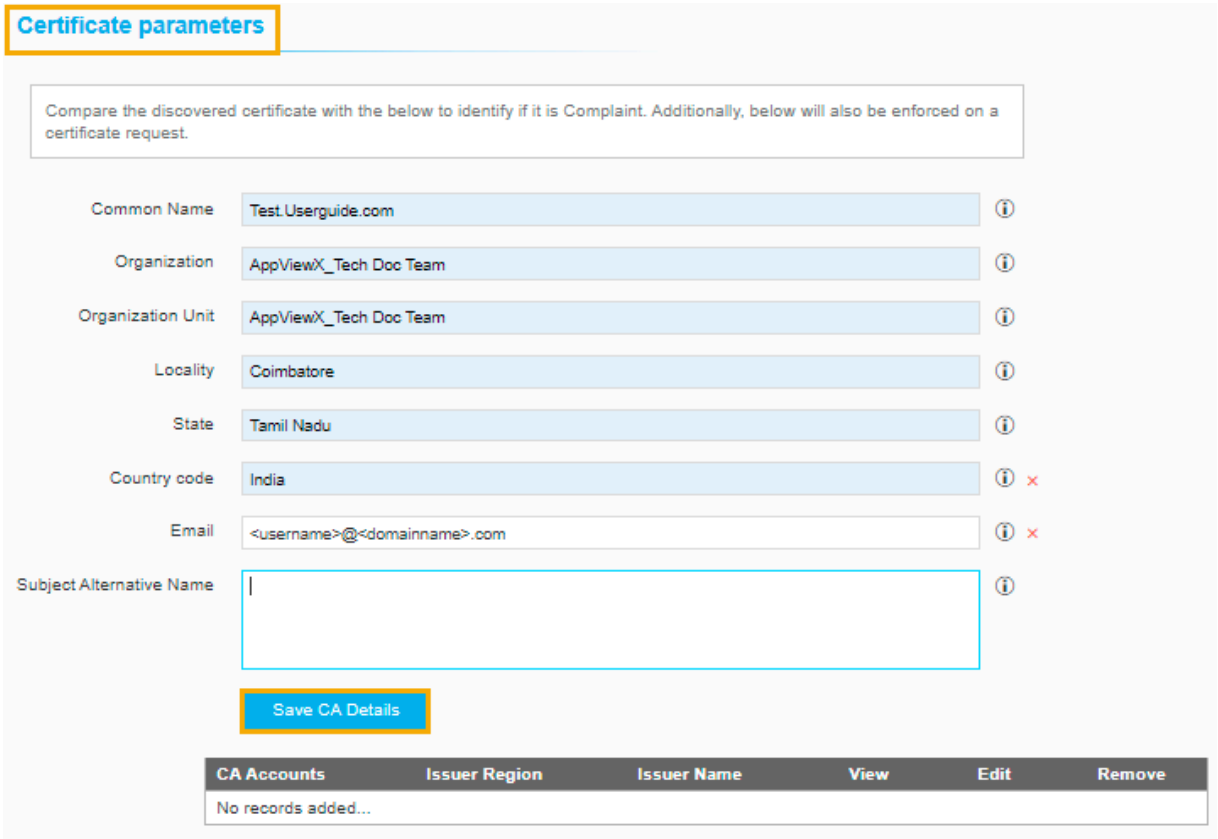


The following table provides the field description in the **CA Details** section:

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 if they are complaint with the

Name	Description	Purpose
	can select one (or) more than one **ECDSA curve** from the drop-down. for a certificate.	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.

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

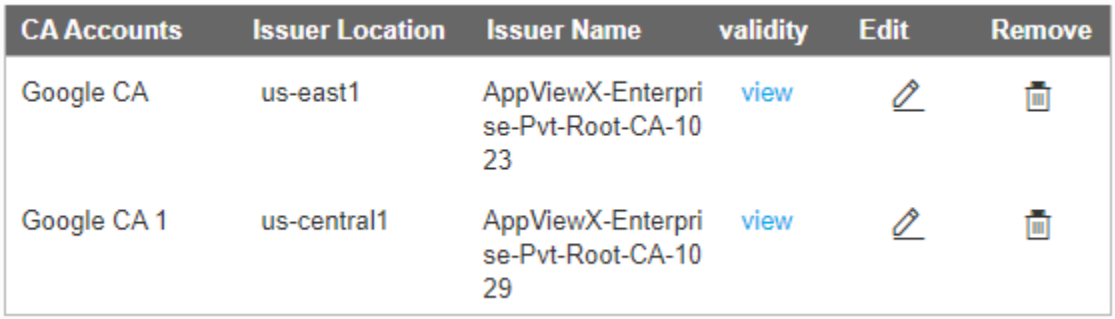


The following table provides the field description in the **Certificate parameters** section:

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, 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. 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.

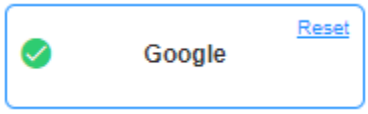
Name	Description
	The discovered certificate's **Country code** will be compared against the country code provided in the policy to identify if they are complaints. **Country code** is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Email	You can provide an 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 (@)

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

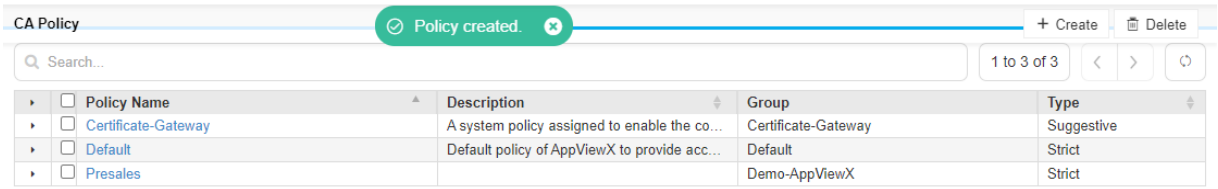


CA Accounts	Issuer Location	Issuer Name	validity	Edit	Remove
Google CA	us-east1	AppViewX-Enterprise-Pvt-Root-CA-1023	view		
Google CA 1	us-central1	AppViewX-Enterprise-Pvt-Root-CA-1029	view		

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



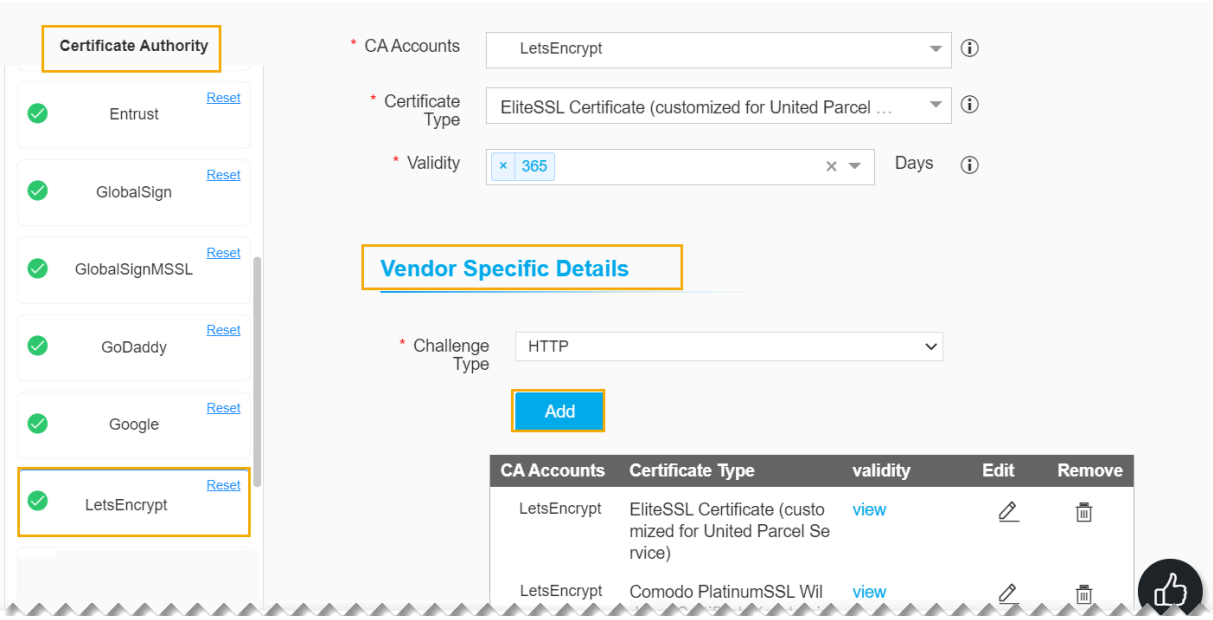
13. Click the **Create Policy** button to create a new policy.
14. The policy is created and a confirmation message displays.



Configuring Policy for Let's Encrypt CA

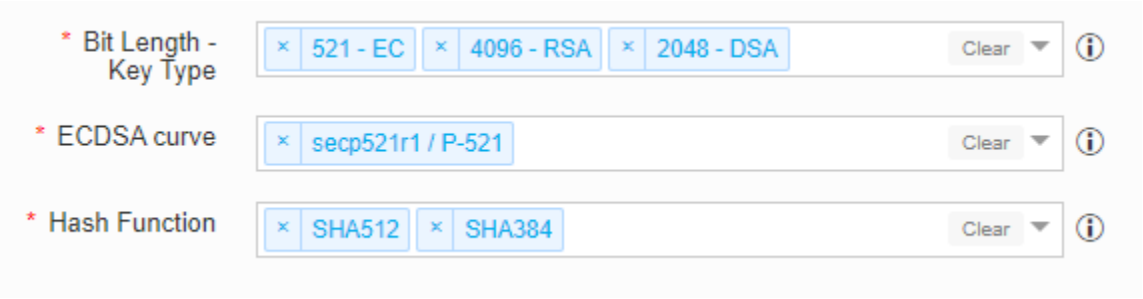
To configure the Let's Encrypt CA policy,

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.
   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.



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.

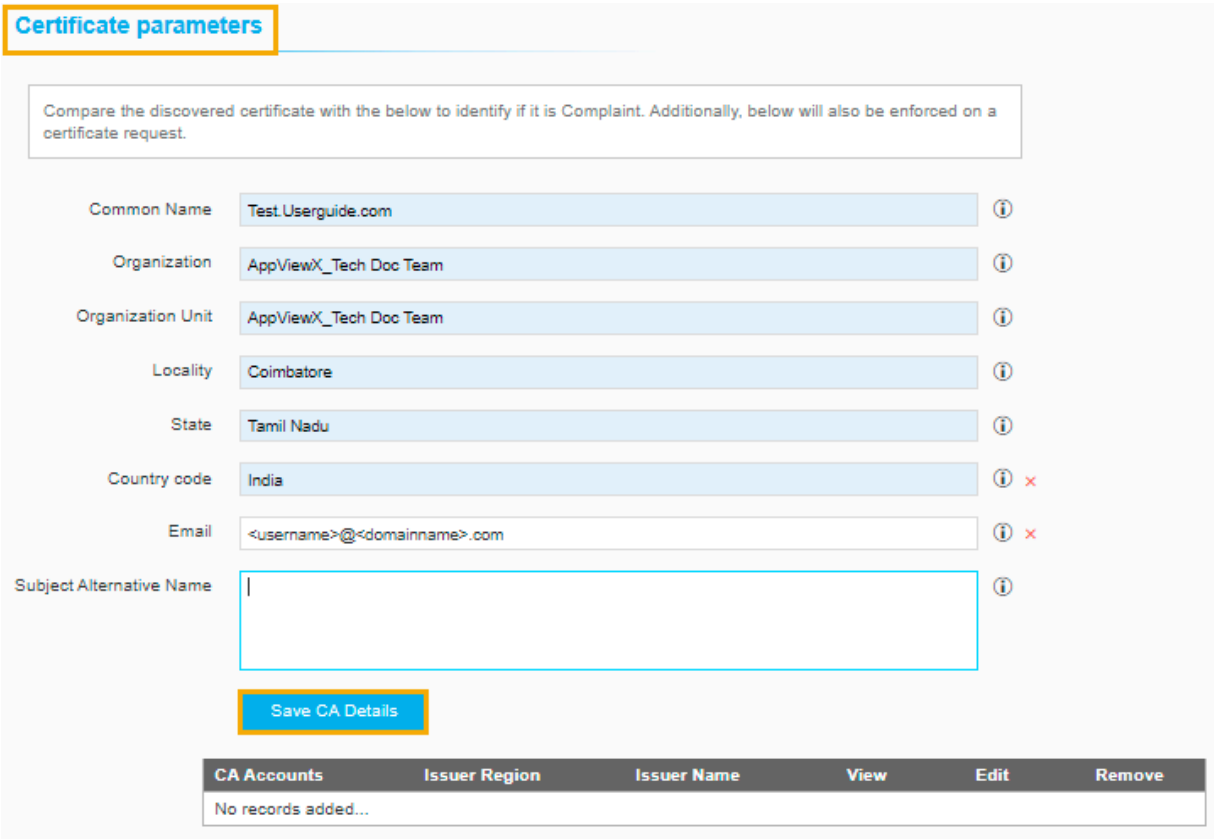


The following table provides the field description in the **CA Details** section:

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	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**

Name	Description	Purpose
	Bit Length - Key Type(s) from the drop-down.	**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.
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:

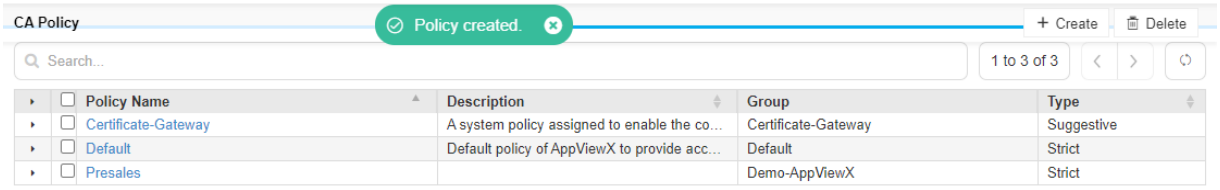
Name	Description
Common Name	You can provide the common name. For example, *.domain.com It helps enforce domains for which a certificate can be requested. **Common Name** is enforced while performing any certificate request operations such as New, Renew, and Regenerate. **Note:** Use Asterisk (*) for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

Name	Description
	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. 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

Name	Description
	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 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.



Configuring Policy for Microsoft Enterprise CA

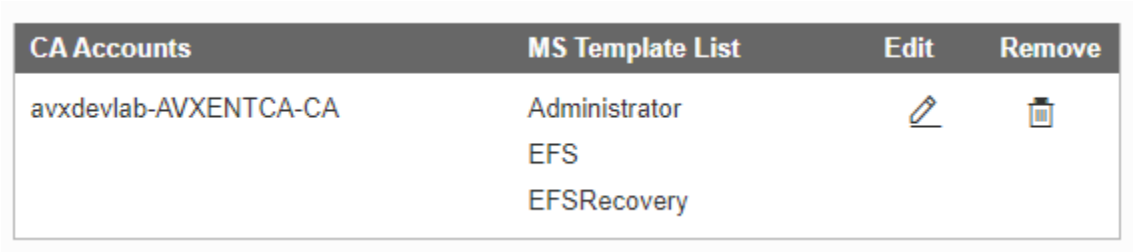
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**
   The CA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



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

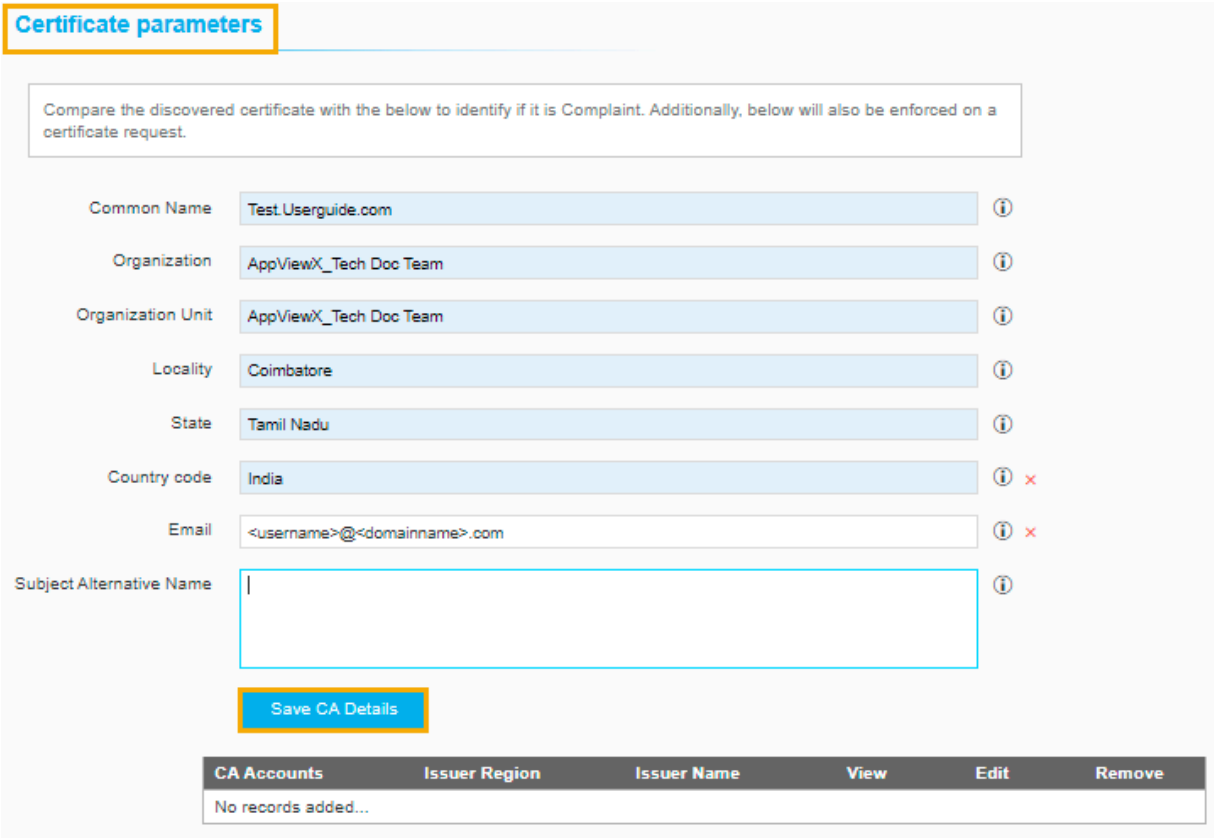
The following table provides the field description in the **CA Details** section:

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 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

Name	Description	Purpose
		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.



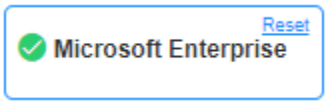
The following table provides the field description **in the Certificate parameters** section:

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

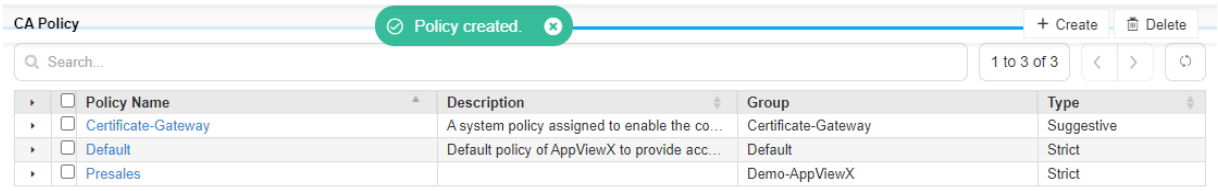
Name	Description
	It helps enforce domains for which a certificate can be requested. **Common Name** is enforced while performing any certificate request operations such as New, Renew, and Regenerate. **Note:** Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com 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, 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.

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 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 (@)

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 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.



Configuring Policy for Microsoft Standalone CA

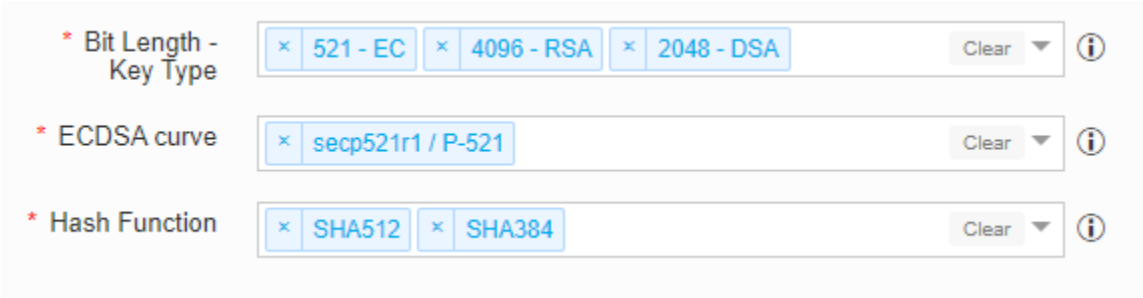
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **GROUPS & POLICIES**.
5. Click **CA Policy.**
   The CA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

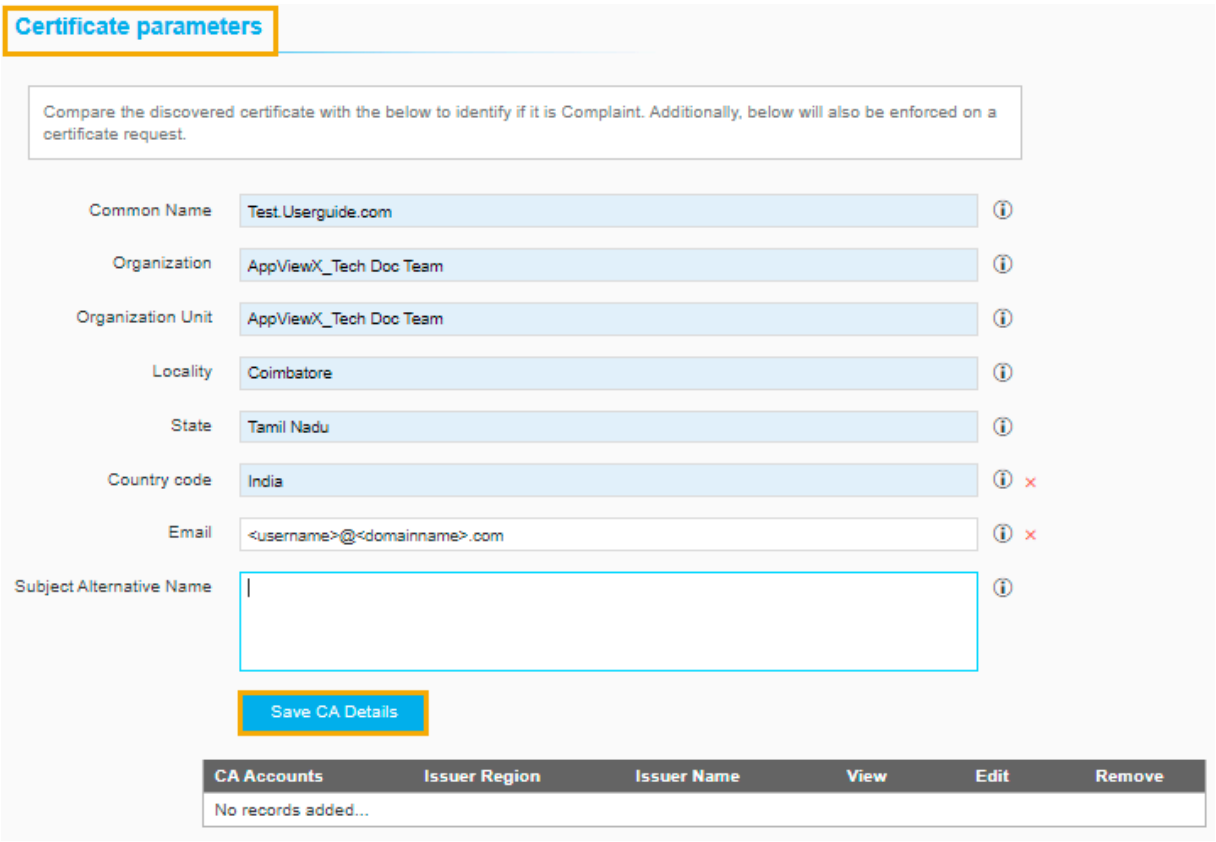


The following table provides the description of other fields in the **CA Details** section:

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 while performing any certificate request operations such as New, Renew, Regenerate.

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

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



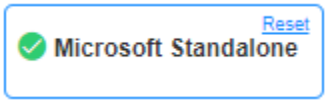
14. The following table provides the field description under **Certificate parameters** section:

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

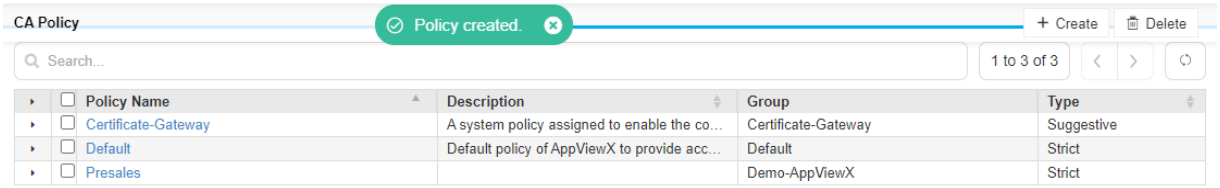
Name	Description
	to request certificates with domain.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Organization	You can provide the organization's name. The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify 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. **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.

Name	Description
	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 (@)

15. 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.



16. Click the **+ Create Policy** button to create a new policy.
17. 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.

   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 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.
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.**
    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 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.

    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. **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.

Name	Description
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. **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 (@)

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.

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.**
   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 Sectigo details, click **Comodo Certificate Manager** 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 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.

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

Name	Description	Purpose
		request operations such as New, Renew, Regenerate.

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 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.

Name	Description
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. **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 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.

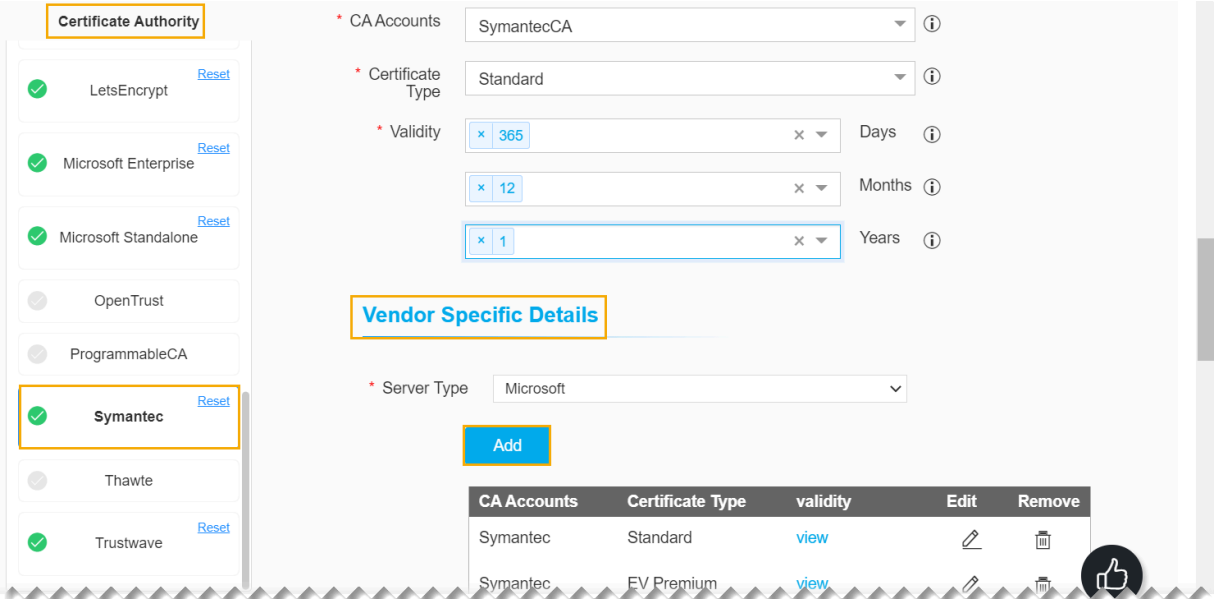
Configuring Policy for Symantec CA

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

   The **Create** policy page appears.

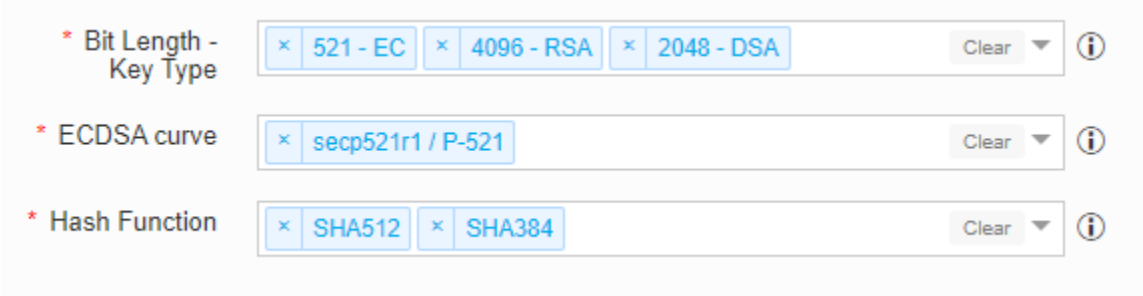
7. Refer Configuring Policy Details section in admin guide to configure,
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
8. To configure a policy with Symantec details, click **Symantec** in the **Certificate Authority** pane on the left side of the page.



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

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

9. In the **Vendor Specific Details section**, select the server 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. In the **CA details** section, select **Bit Length -Key Type, ECDSA curve,** and **Hash Function.**

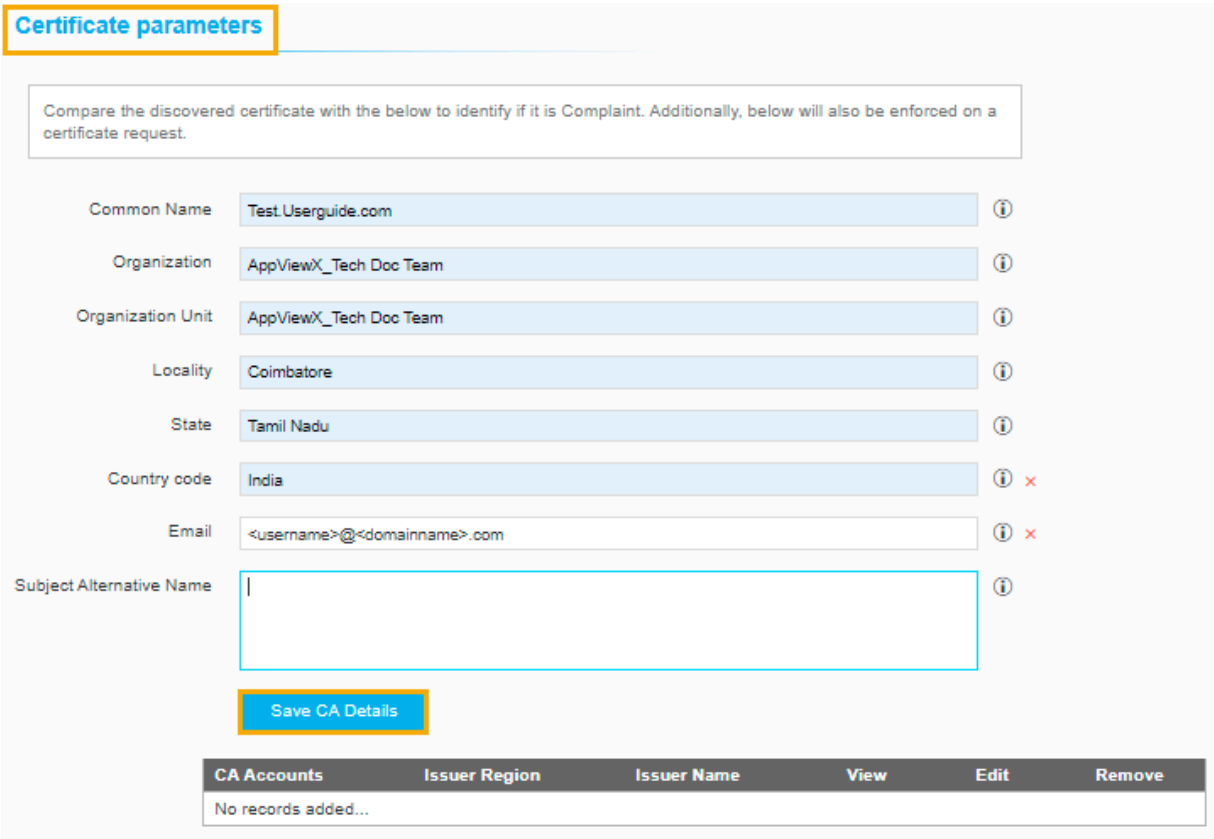


The following table provides the field description in the **CA Details** section:

Name	Description	Purpose
***Bit Length - Key Type**	All the **Key Types** are listed with corresponding **Bit Length.** You	The discovered certificate's Key Type and Bit length will be compared

Name	Description	Purpose
	can select one (or) more than one **Bit Length - Key Type(s)** from the drop-down.	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 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.



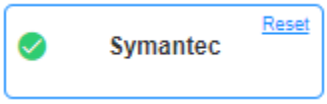
The following table provides the field description in the **Certificate parameters** section:

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.

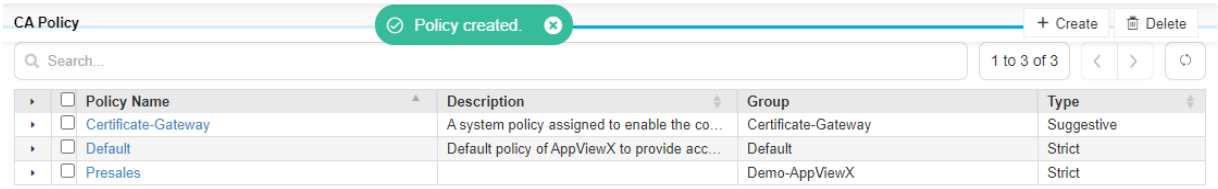
Name	Description
	The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify if they are complaints. **The organization** is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Organization 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, 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, 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 (@)

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 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.

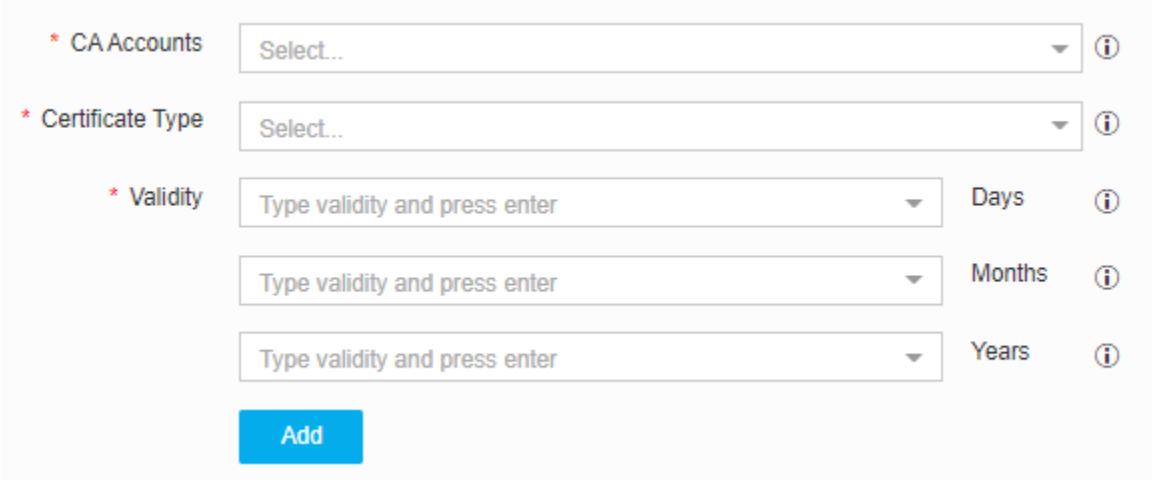


Configuring Policy for Trustwave CA

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.

   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.

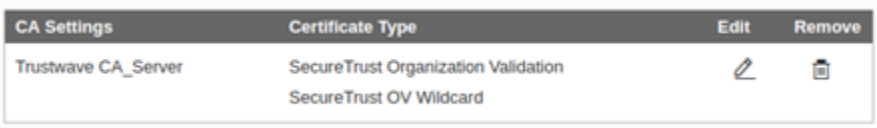


The following table provides the field description under **CA Details** section:

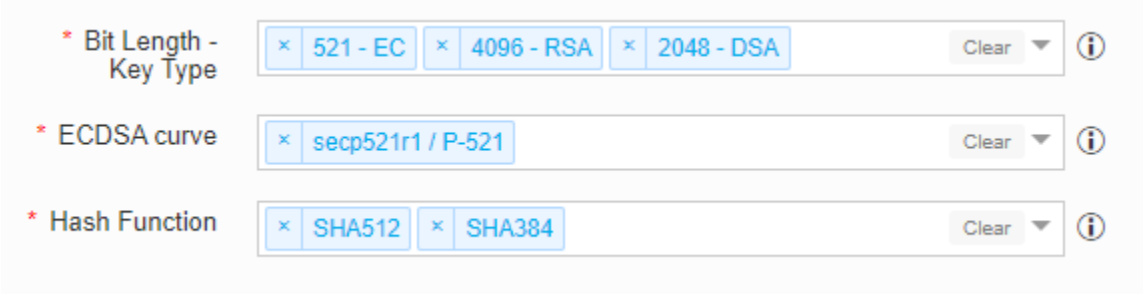
Name	Description
***CA Accounts**	The Trustwave CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The **Certificate Types** corresponding to the selected CA account are listed. Select one (or) more **Certificate 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.

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.**



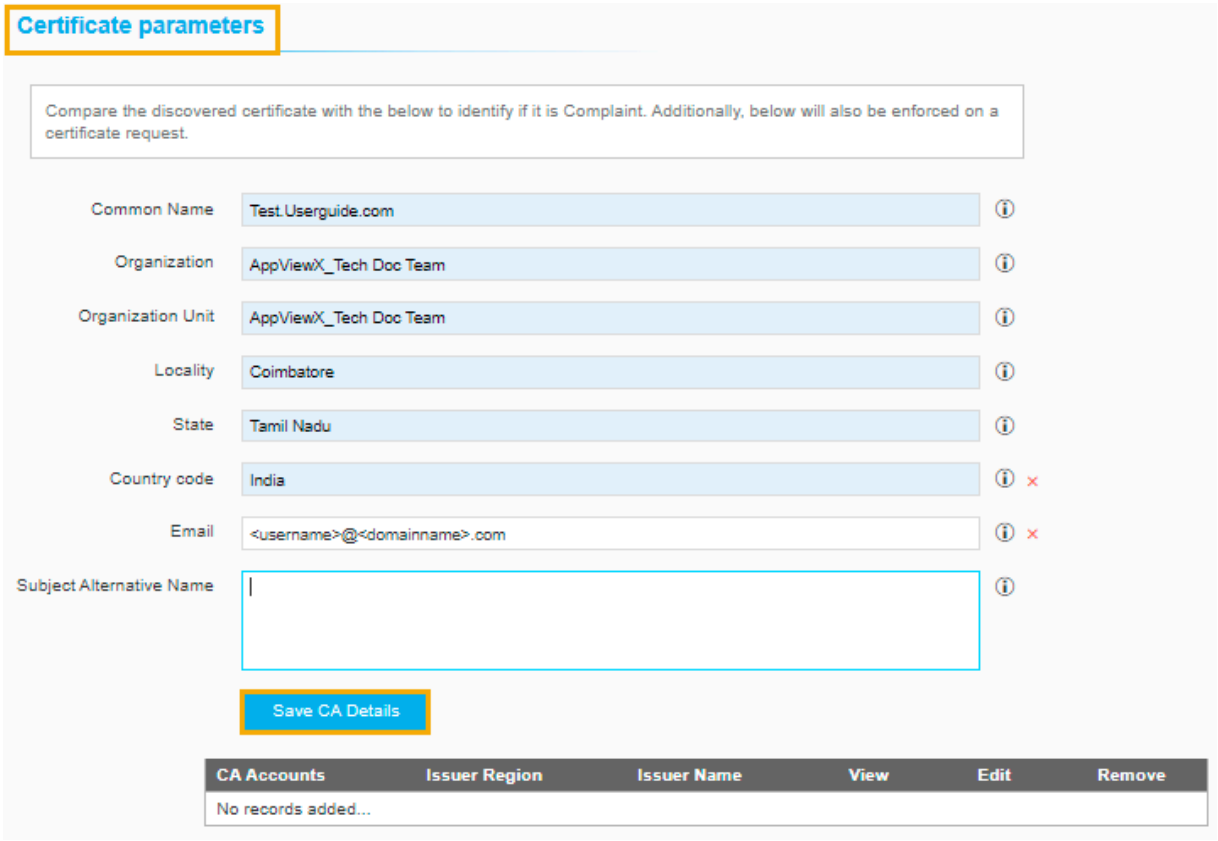
The following table provides the field description under **CA Details** section:

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**	The discovered certificate's Key Type and Bit length will be compared against the selected **Bit**

Name	Description	Purpose
	Length - Key Type(s) from the drop-down.	**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 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.



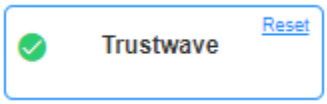
The following table provides the field description in the **Certificate parameters** section:

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.

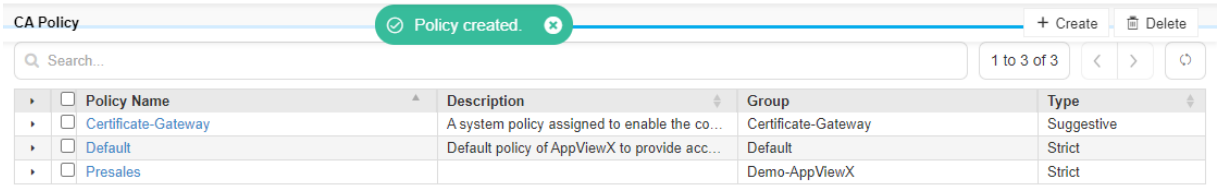
Name	Description
	The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify if they are complaints. **The organization** is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Organization 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. 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)

Name	Description
	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 **Trustwave** 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.



Configuring Policy for GlobalSign CA

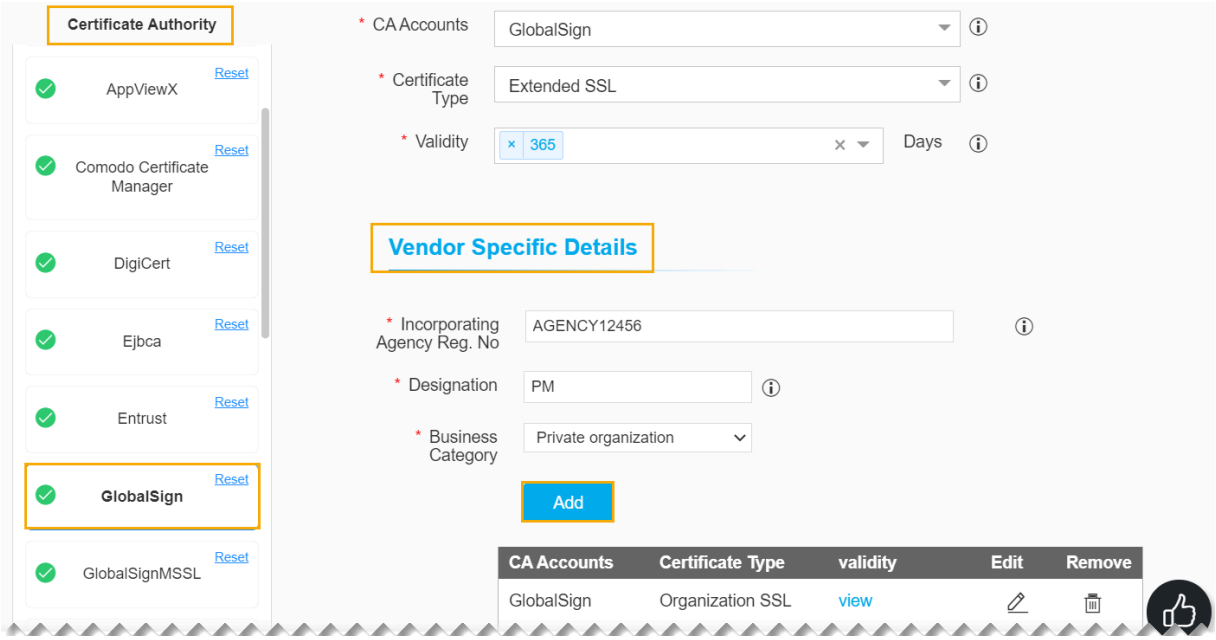
To configure a GlobalSign CA policy,

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.**

   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 GlobalSign details, click **GlobalSign** in the **Certificate Authority** pane on the left side of the page.



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

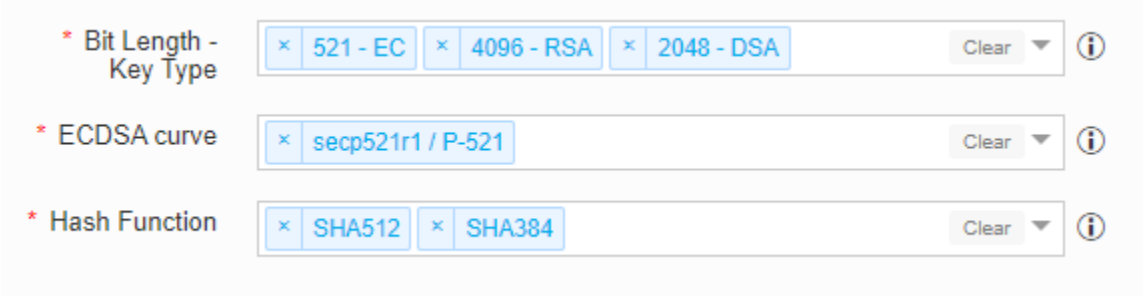
Field	Description
*Incorporating Agency Reg. No	Enter the agency registration number.
*Designation	Enter the designation.
*Business Category	Select the business category from the dropdown list.

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 **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.**

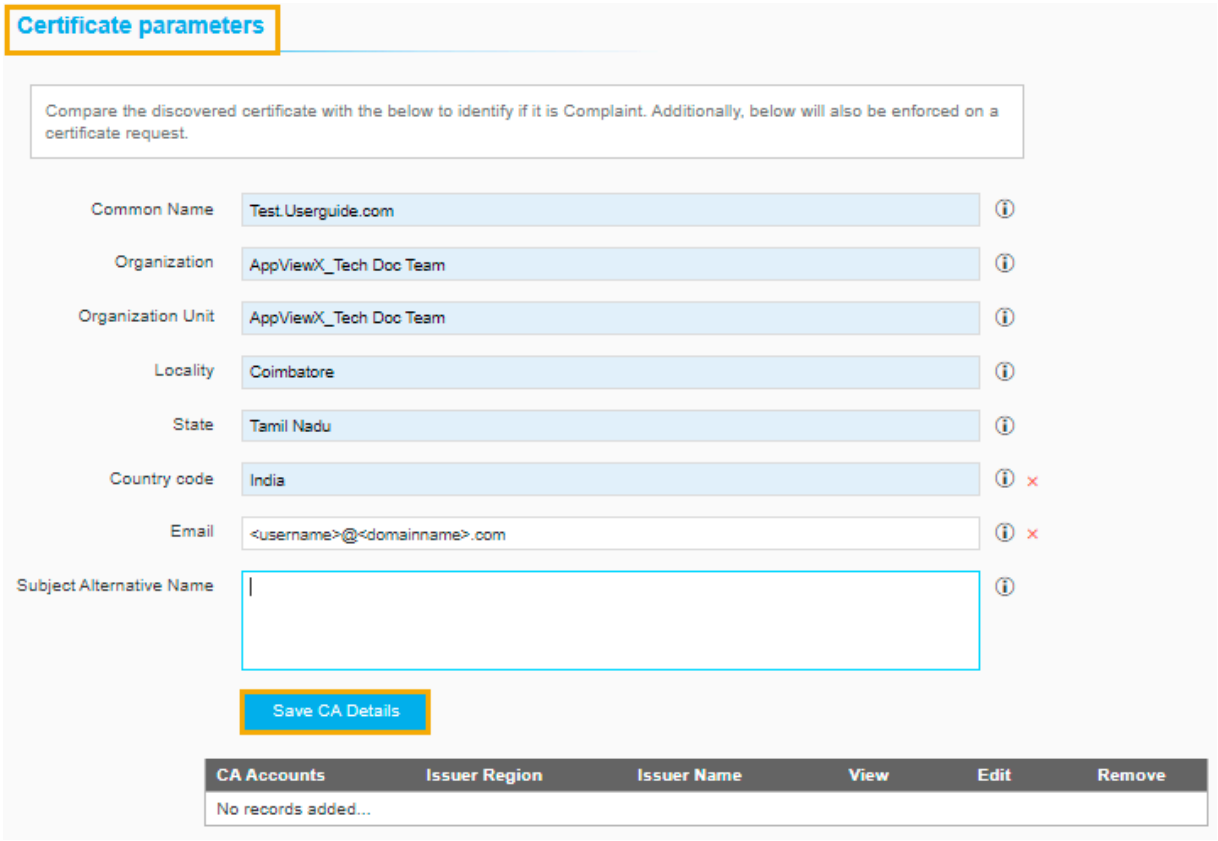


The following table provides the field description in the **CA Details** section:

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

Name	Description	Purpose
		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 the **Certificate parameters** section based on your organization's policies and standards.



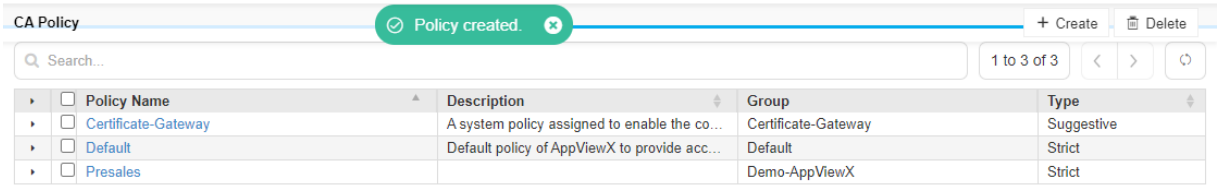
The following table provides the field description **in the Certificate parameters** section:

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

Name	Description
	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. 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

Name	Description
	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.

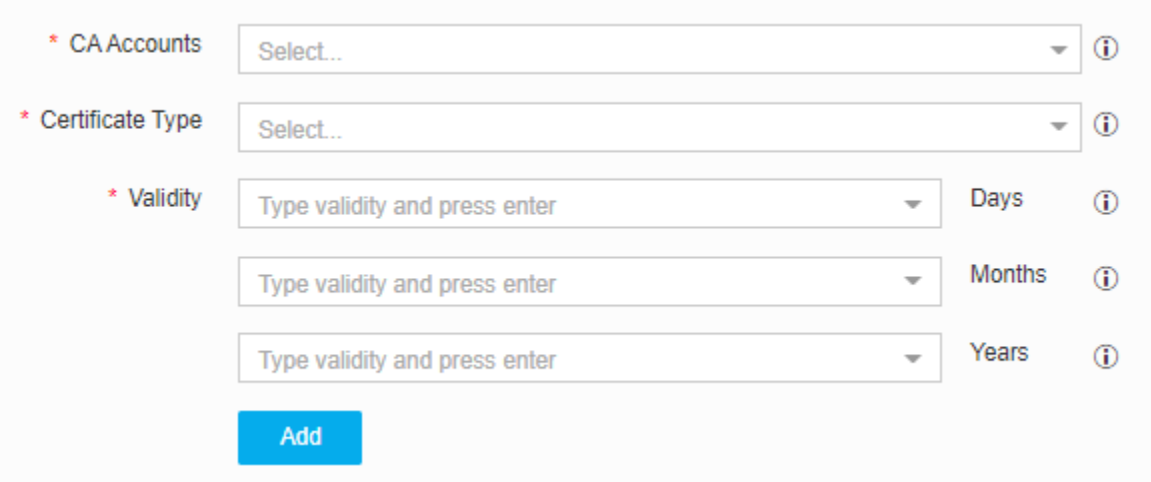


Configuring Policy for Nexus CA

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.**
   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 Nexus details, click **Nexus** 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.



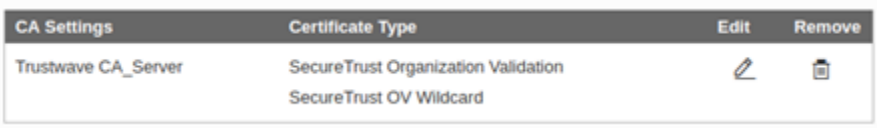
The following table provides the field description under **CA Details** section:

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.

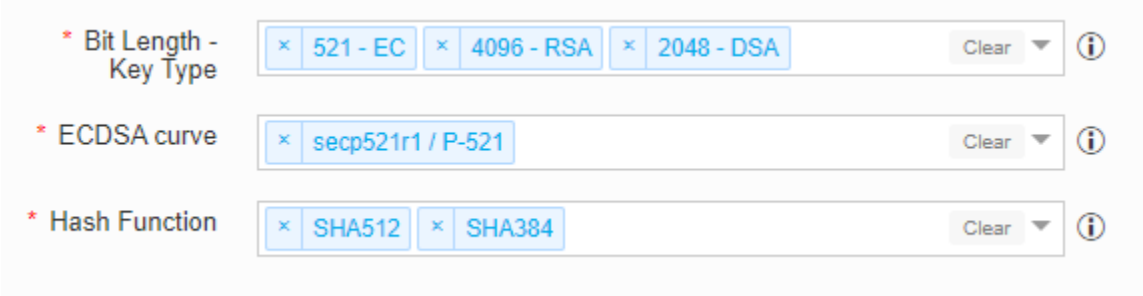
Note: The asterisk (*) symbol indicates a mandatory field.

10. 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.**

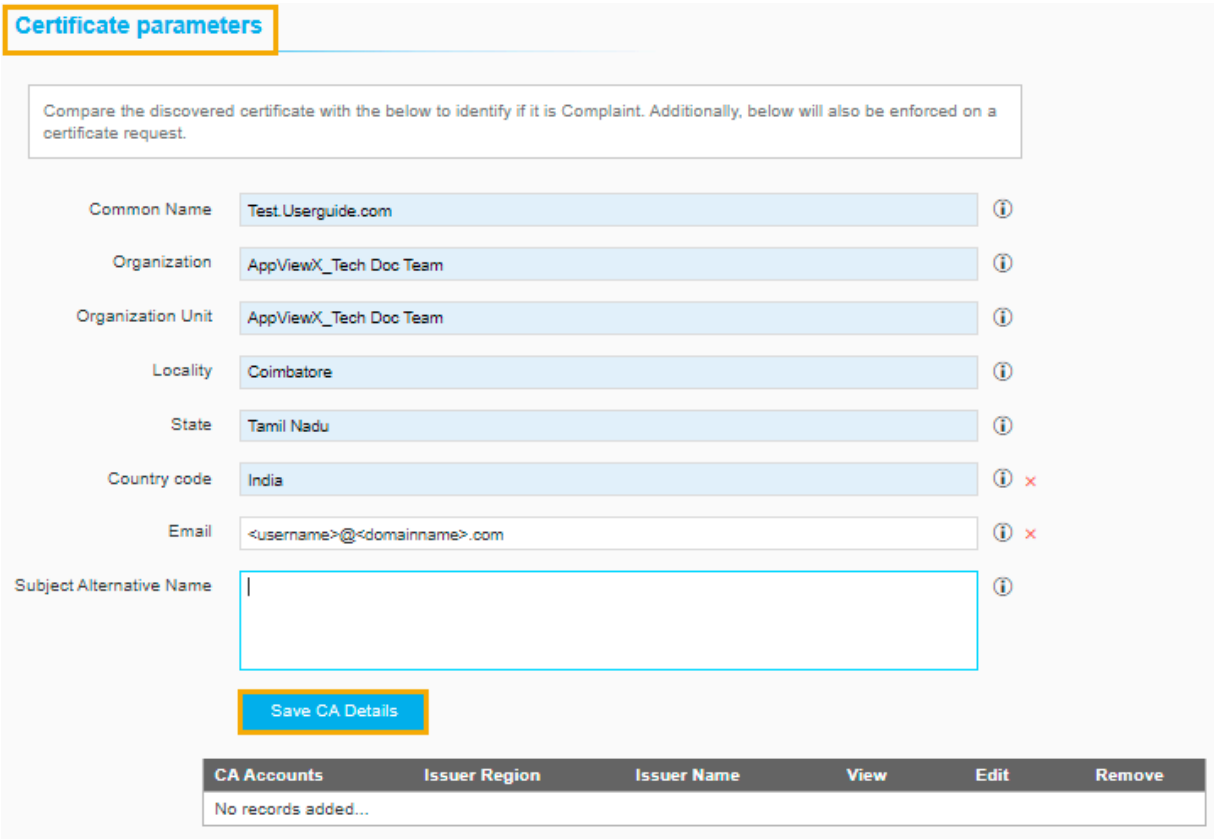


The following table provides the field description under **CA Details** section:

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,

Name	Description	Purpose
		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.



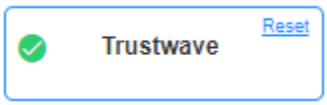
The following table provides the field description in the **Certificate parameters** section:

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.

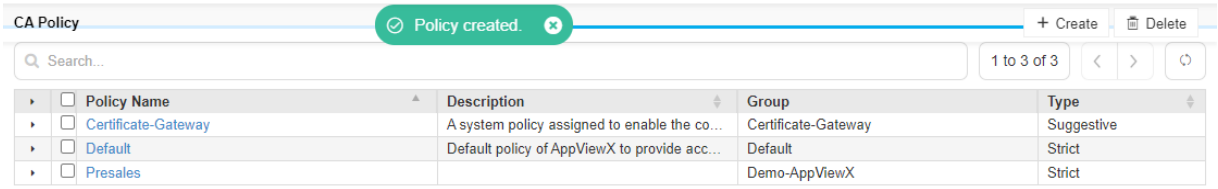
Name	Description
	The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify if they are complaints. **The organization** is enforced while performing any certificate request operations such as New, Renew, Regenerate.
Organization 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. 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)

Name	Description
	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 **Trustwave** 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.



Certificate Group

- Overview
- Assign Certificate to a Group
- Create a Group

Overview

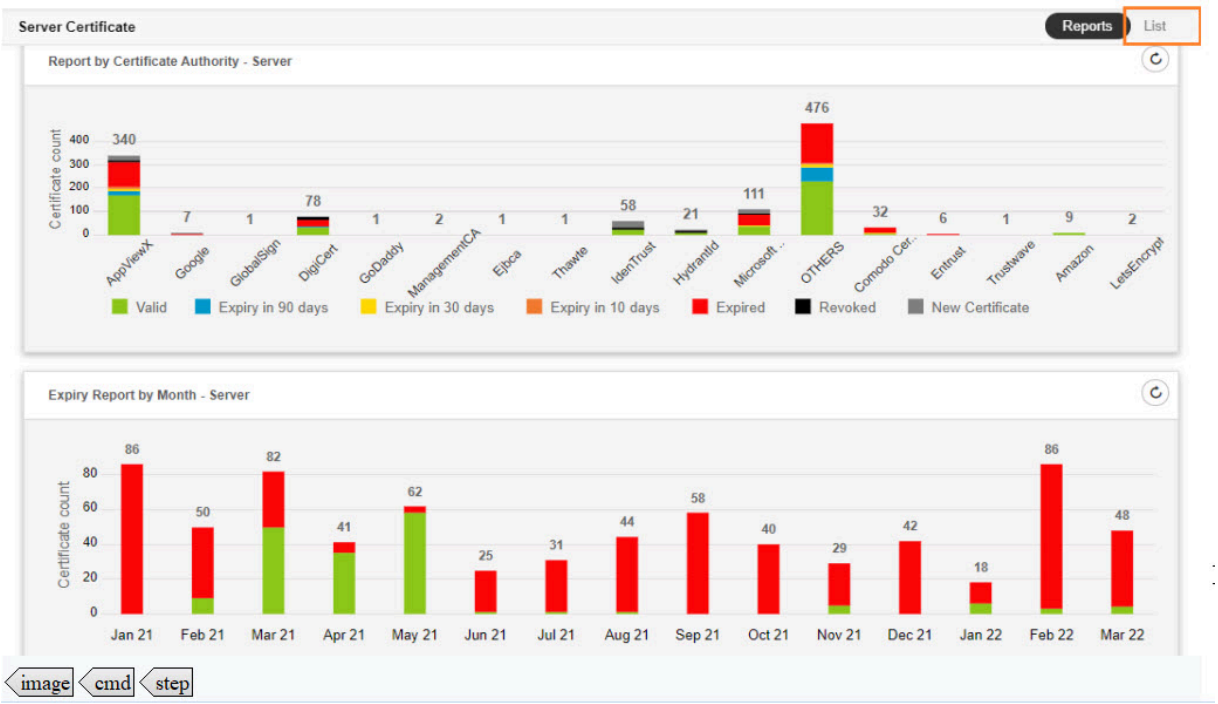
Before you Begin

Following are the points needed to be known before starting **Certificate Groups** configuration:

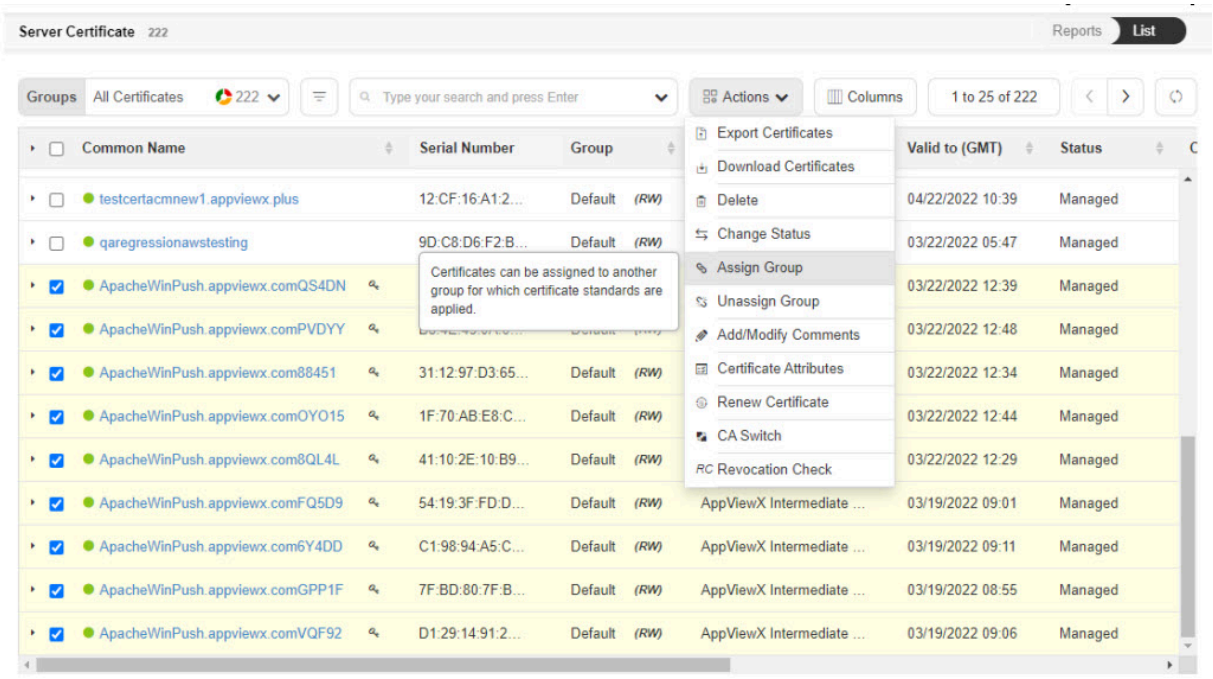
- **Certificate Groups** are used to categorize the certificates according to various **business units.**
- In some organizations, **Certificate Groups** are also used to assign access permissions. Only privileged users (inherits from Resource > User Group) can view the respective **Certificate Groups**.
- 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.

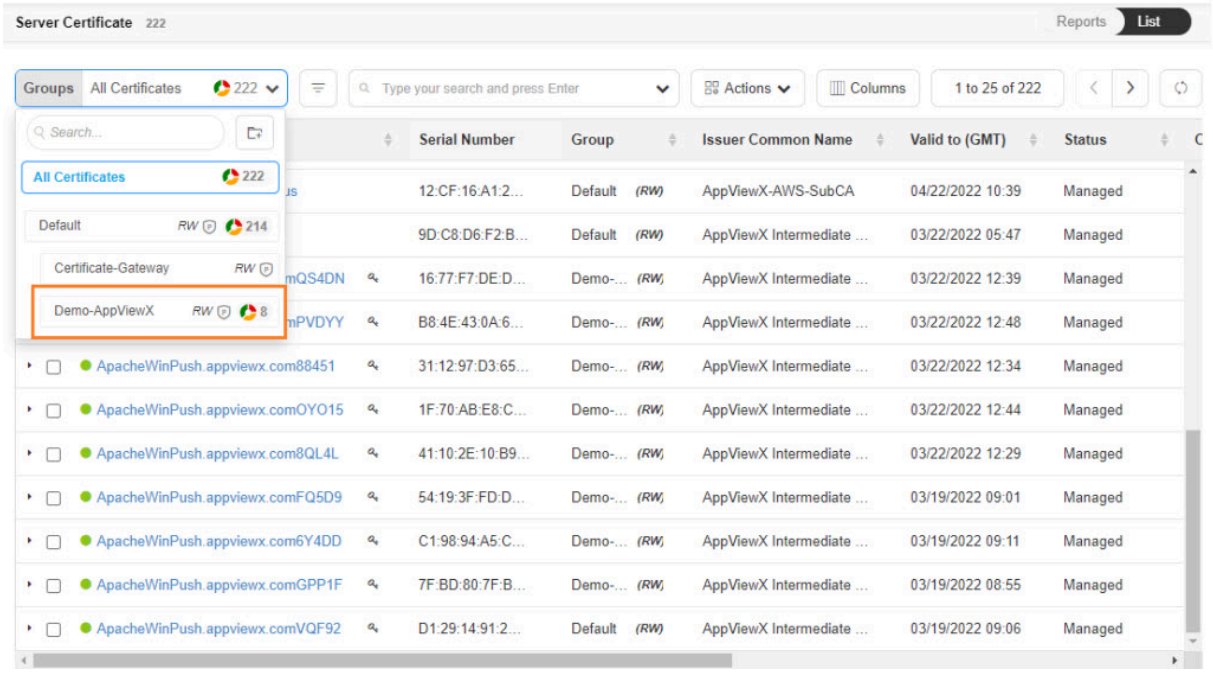


5. Select the check box against the certificate(s) you want to assign to a group.
6. Click the **Actions** drop-down and select the **Assign Group** option from the drop-down.

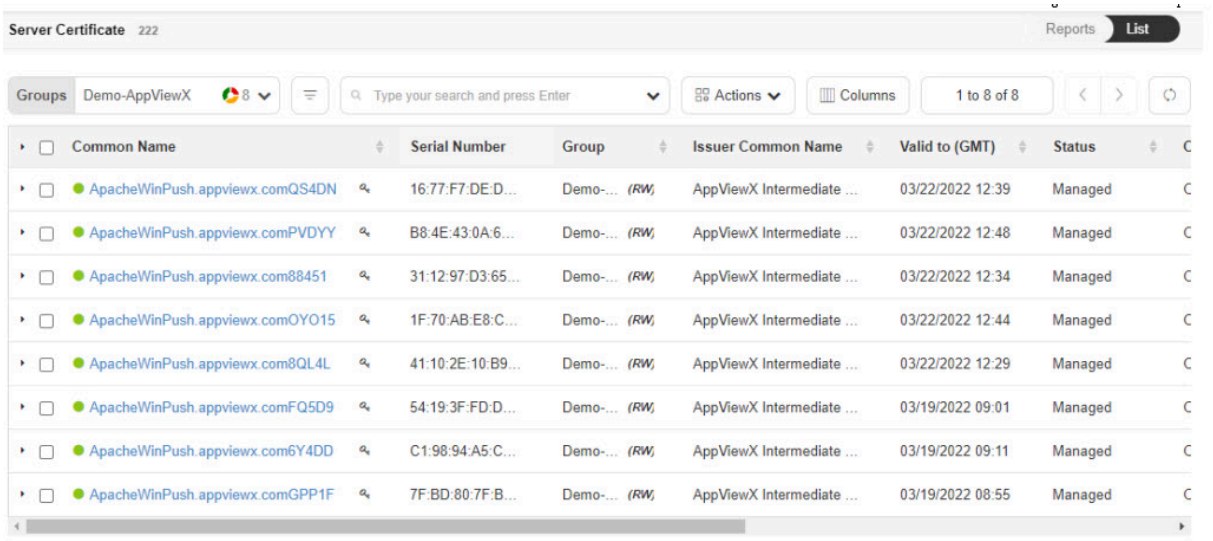


7. The **Assign to Group** pop-up appears. Select the **Group** from the list.
8. Click the **Assign** button to move the certificate(s) to the selected **Group.**

9. Click the **Groups** drop-down and select your **Group** from the drop-down.



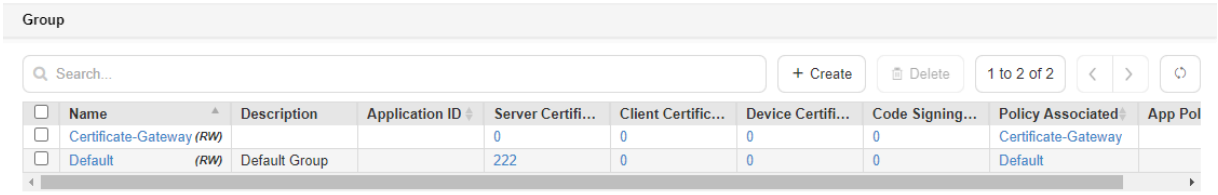
10. You can view the certificate(s) assigned to the **Group**. The table provides certificate(s) details.



Create a Group

Assign the user to a user group that (inherits from resource and role) have access to certificate group

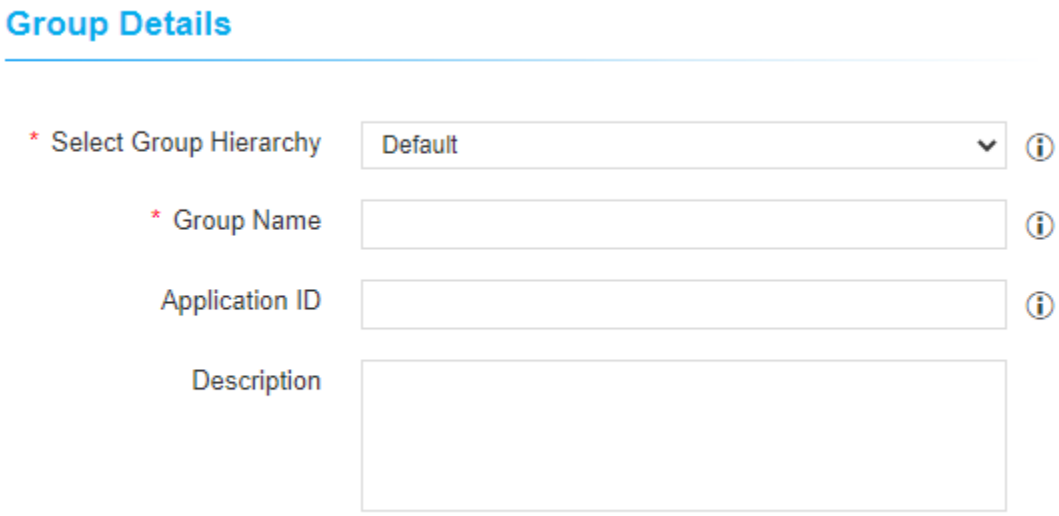
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Click **Groups** under **Groups & Policies.**
   The Group inventory 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.



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

7. Group Name is mandatory in the **Group Details** section. Provide the **Group Name** to create a new group.

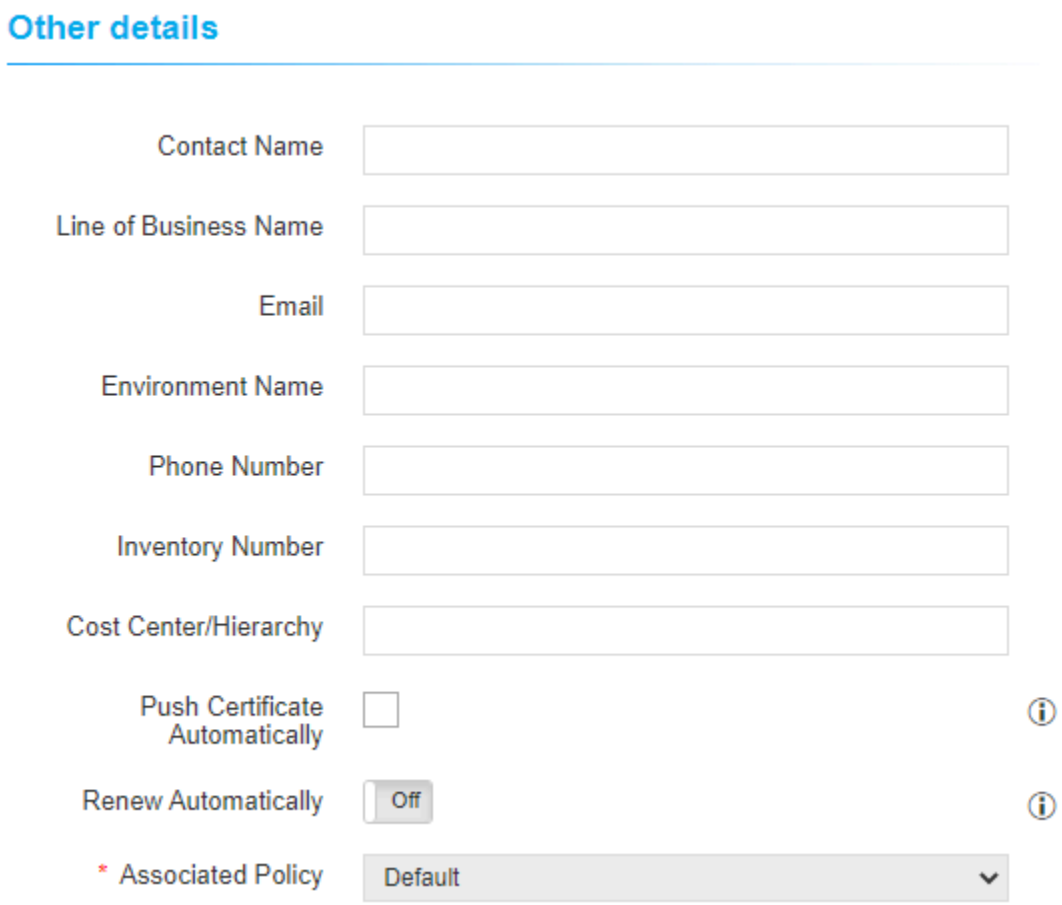


The following table provides the field description under the **Other Details** section:

Name	Type	Mandatory	Description	Validation
Contact Name	Text	No	Provide contact person to whom changes should be intimated	NA
Line of Business Name	Text	No	Provide the name of the business unit	NA
Email	Text	No	Provide contact mail address	NA
Environment Name	Text	No	Provide environment name	NA
Phone Number	Text	No	Provide a phone number for contact	NA
Inventory Number	Text	No	Provide inventory number	NA
Cost Center/ Hierarchy	Text	No	Provide Cost Center code/ label	NA

Name	Type	Mandatory	Description	Validation
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

8. The fields in the **Other Details** section are used based on the organization's needs.

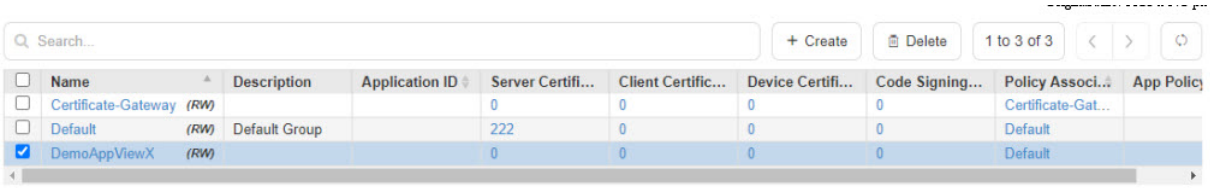


9. Click **Create** button to create the group.

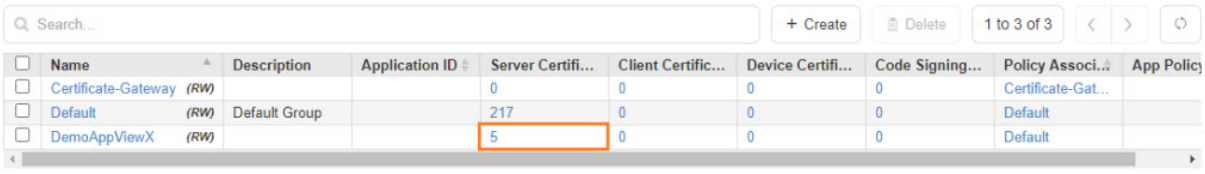
   Users can view the group only if it is associated with the **Resource** of their **User Group**. To associate the **Group** to a **Resource** click the **Update Group and Configure the Resources for User Access**

button instead of **Create** button. This will create the group and navigates to **Resource.** Refer **Create a Resource** 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.

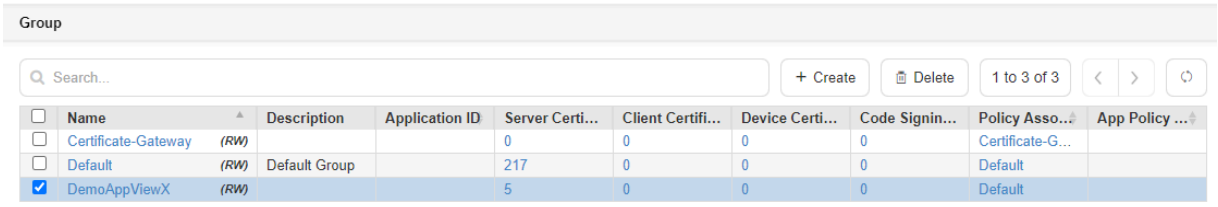


11. Post certificate discovery, you can view the count of certificates (Server, Client, Device, and Code Signing) associated with this group.
12. Click the count to view the certificates.

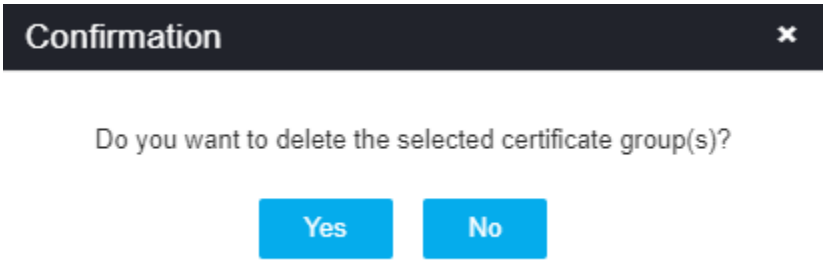


Delete a Group

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.



7. A confirmation pop-up appears. Click the **Yes** button to proceed.

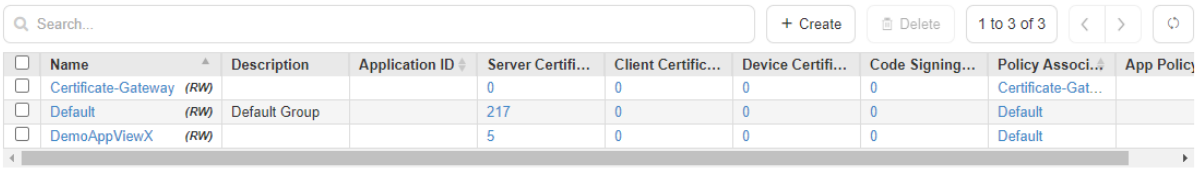


The group is deleted and a confirmation message displays.

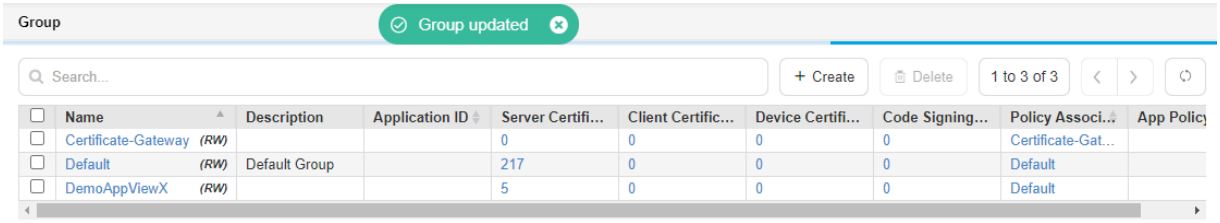
Modify a Group

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.



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.

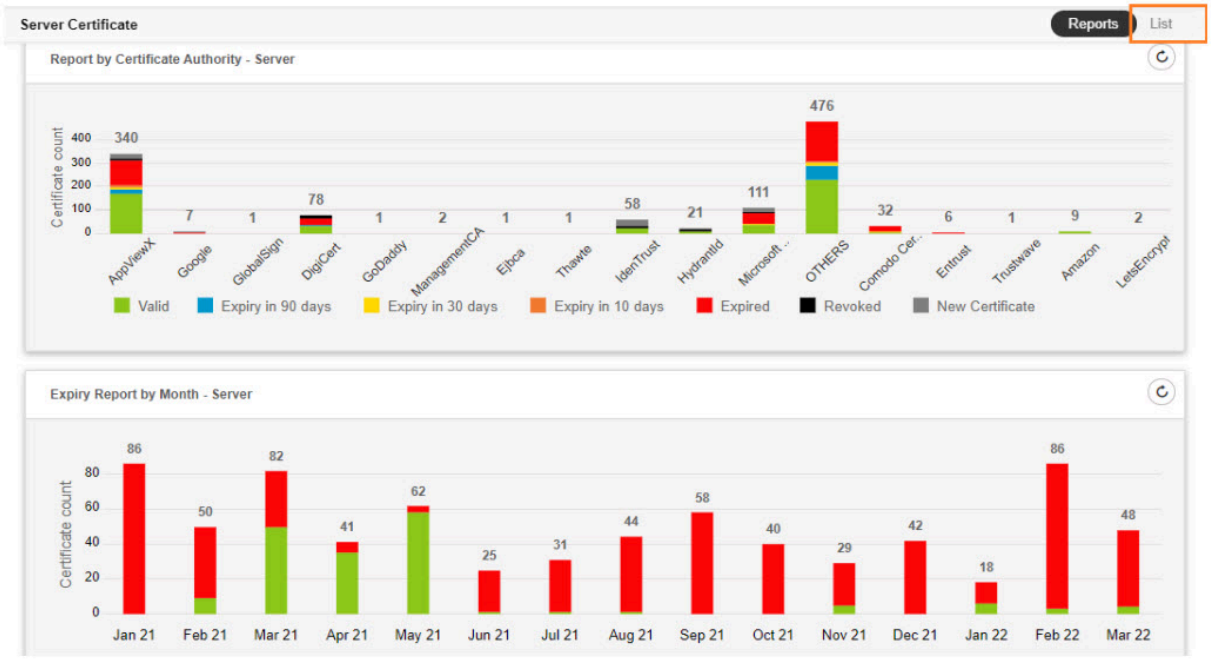


Unassign Certificate from a Group

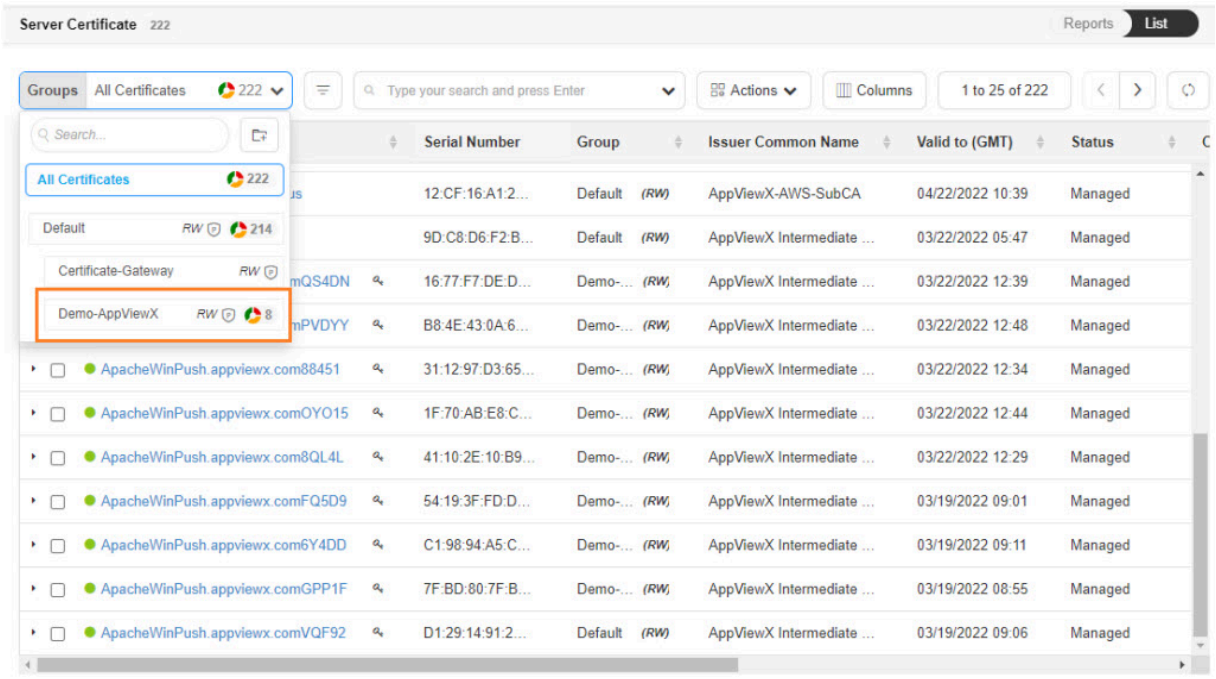
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.
3. Click **CERT+** on the left navigation pane.

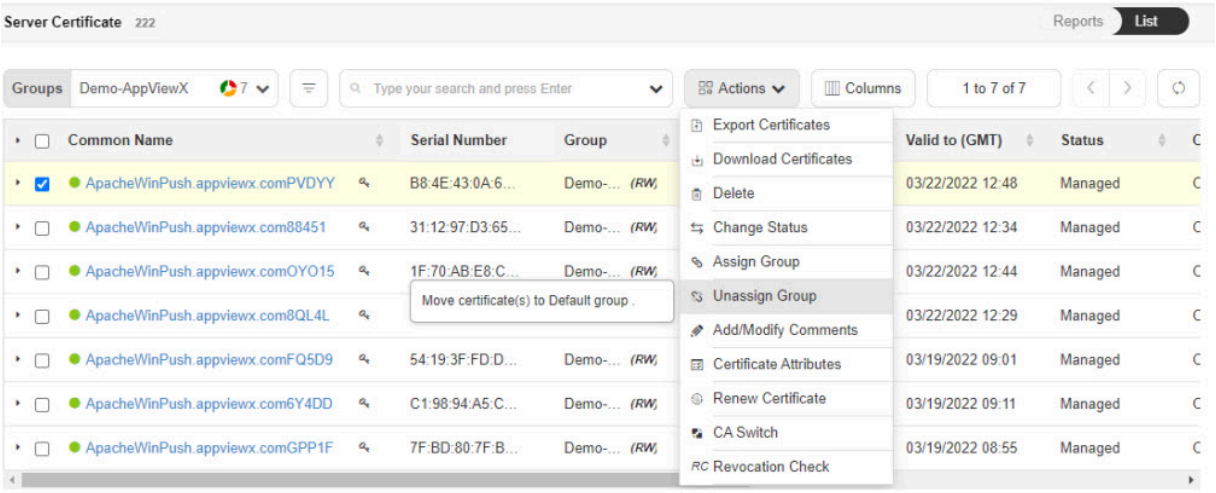
   The **Server Certificate** Inventory appears.
4. Click the **List** button on the upper right of the server certificate inventory screen.



5. Click the **Groups** drop-down and select a **Group** from the drop-down.



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 Password Vault

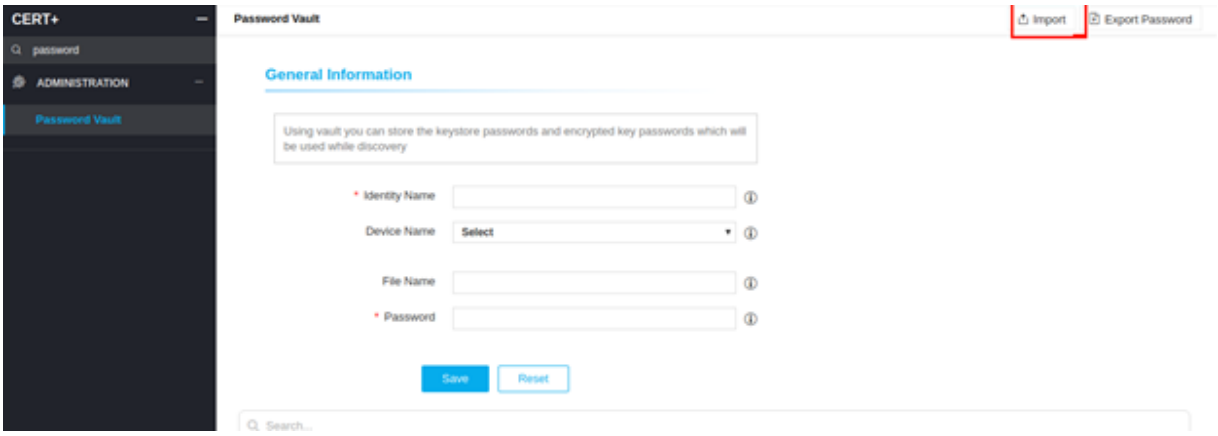
The password vault option is used to store all certificate passwords of the selected ADC devices. All the password-protected certificates that are discovered, will be decrypted and pushed to the discovery grid in the AppViewX Inventory. This happens only if passwords are matched with passwords that are stored in the vault.

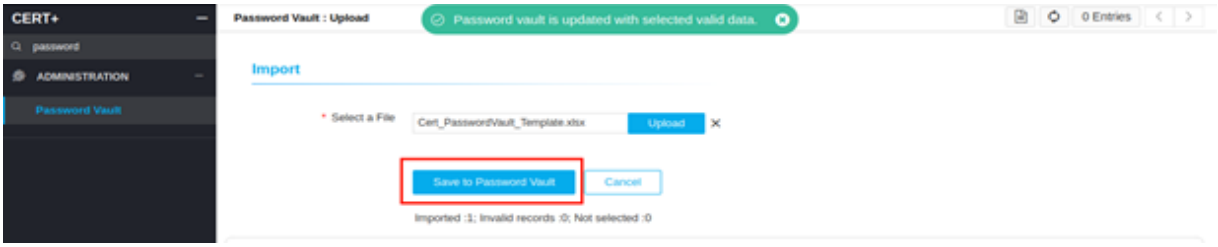
Before you Begin

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.





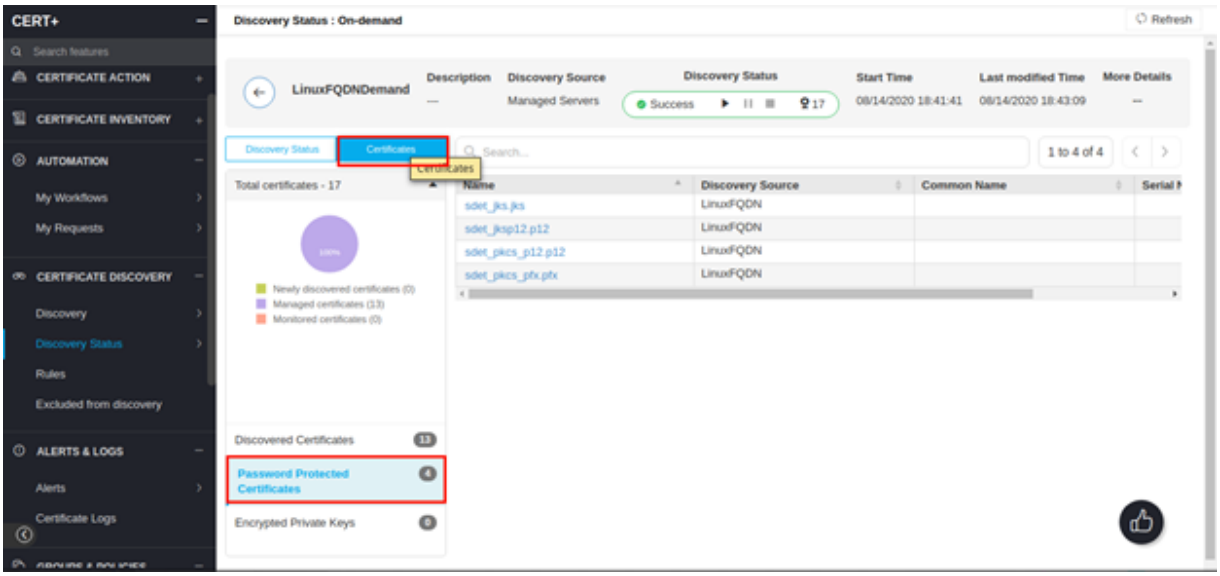
11. Click **Export Password** on the top-right to export all stored certificate passwords from the vault as a zip file to your computer.
12. To modify the existing details, Click **Edit.**
13. To update the password, click **Update.**
14. To delete the password details, click **Delete.**

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 Certificate Attributes

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+**.

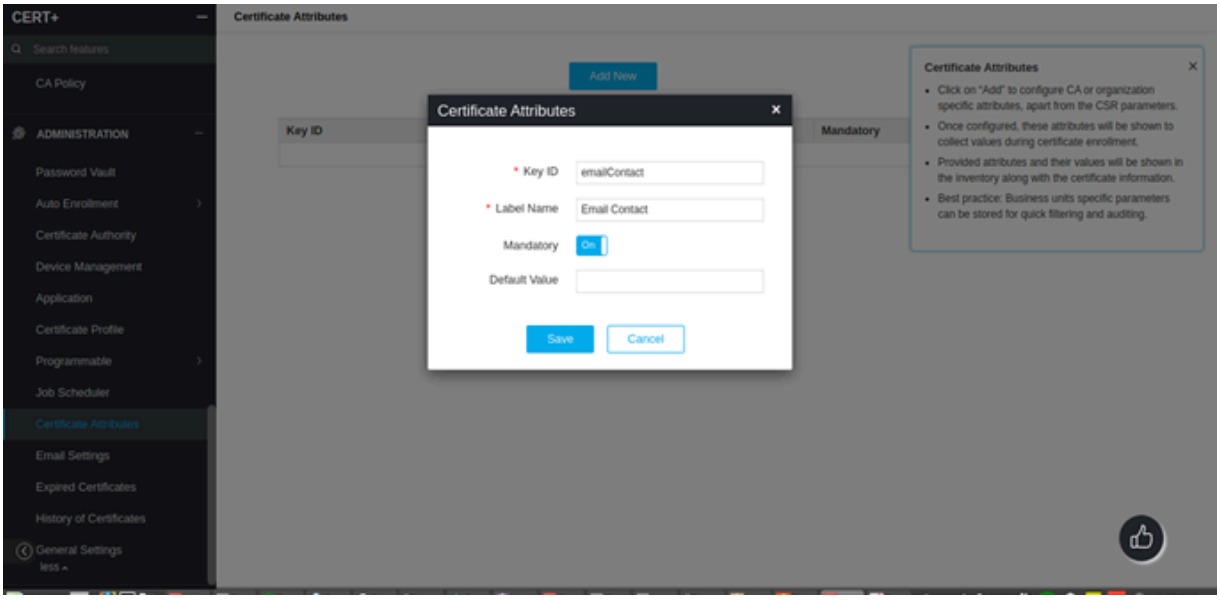
The **CERT+** left navigation pane appears.

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.
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
- Delete Certificate Attribute

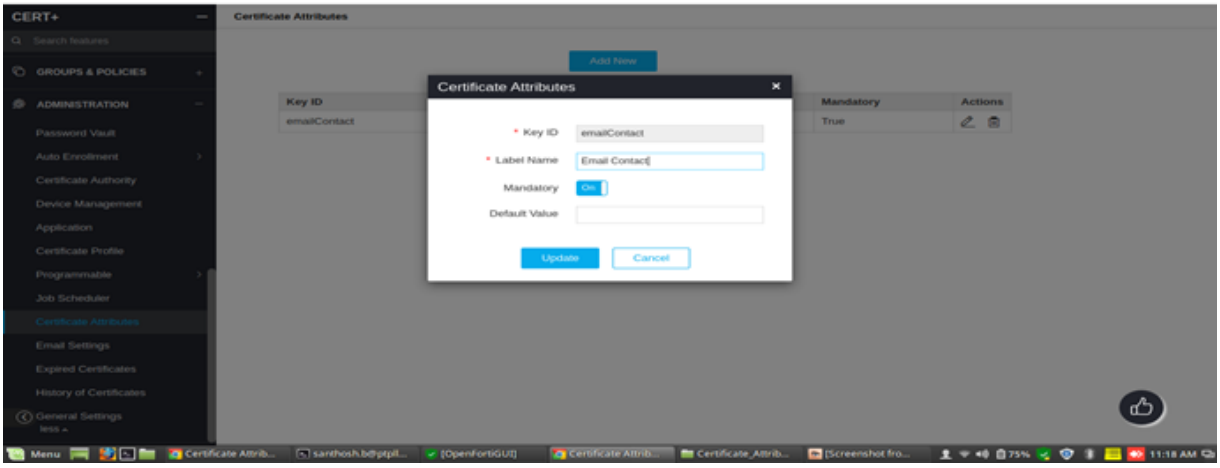
- Certificate Attributes in Certificate Enrollment
- Certificate Attributes in certificate inventory

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+**.

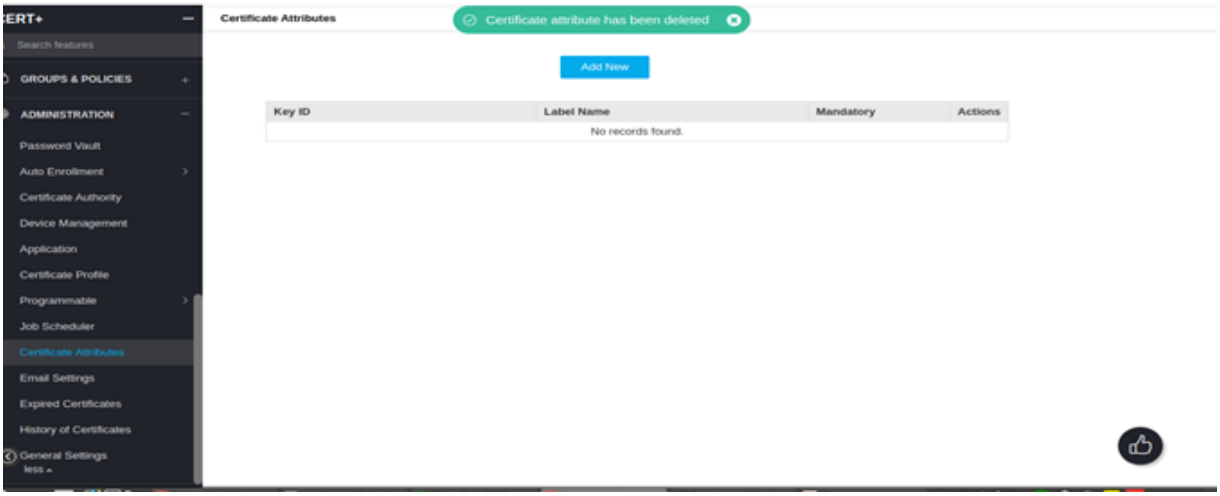
   The **CERT+** left navigation pane appears.
4. **Expand ADMINISTRATION**, and then select **Certificate Attributes**.
5. Under **Actions**, click **Delete**.

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

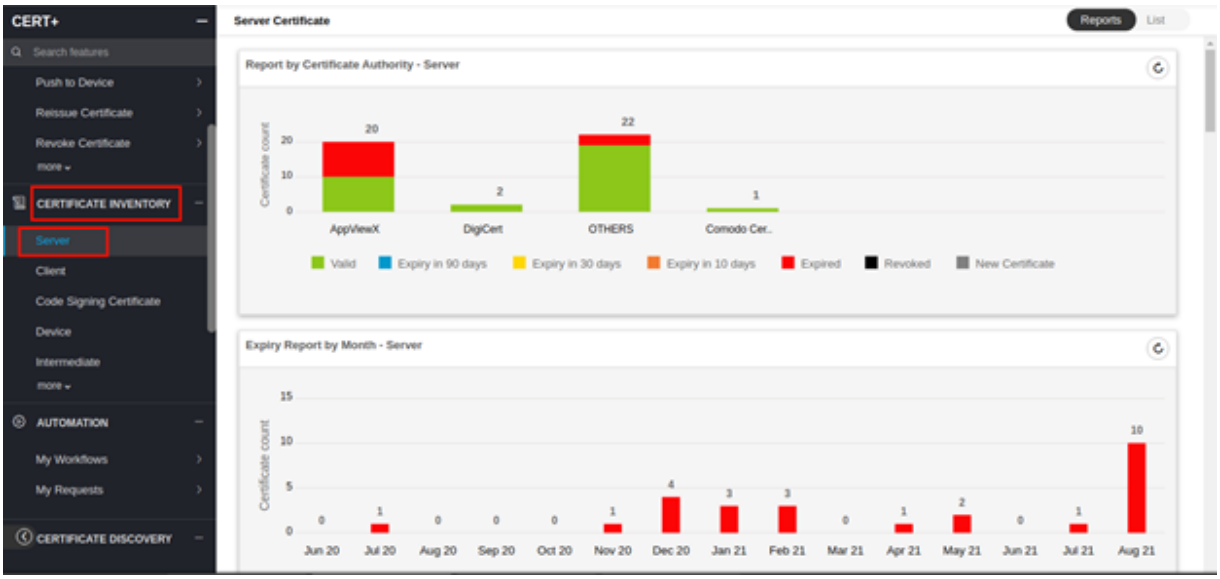
Following are the points needed to be known before starting the configuration for expired certificates:

- 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.

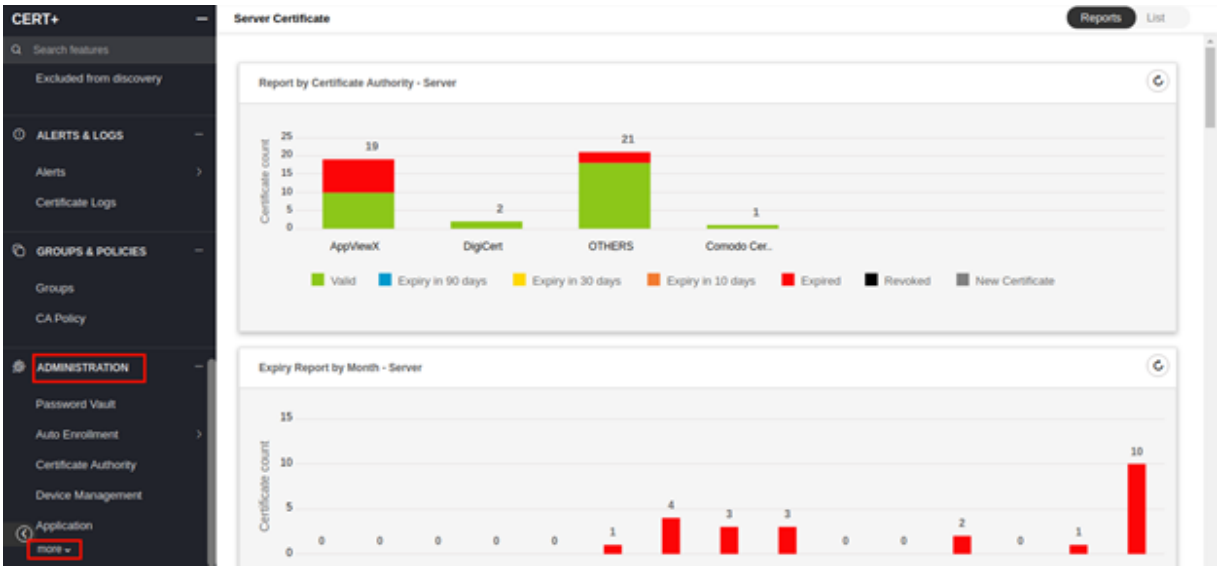


Configuring Expired Certificates

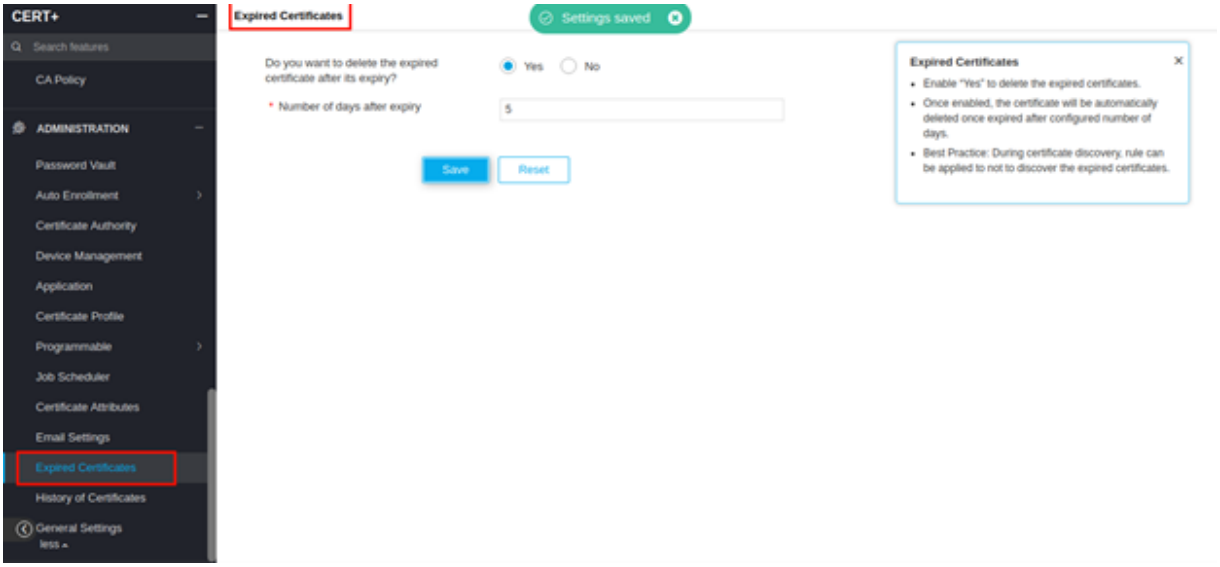
1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button.

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

   The **CERT+** left navigation pane appears.
4. Expand **ADMINISTRATION.**



5. Under **Administration**, click **Expired Certificates.**



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

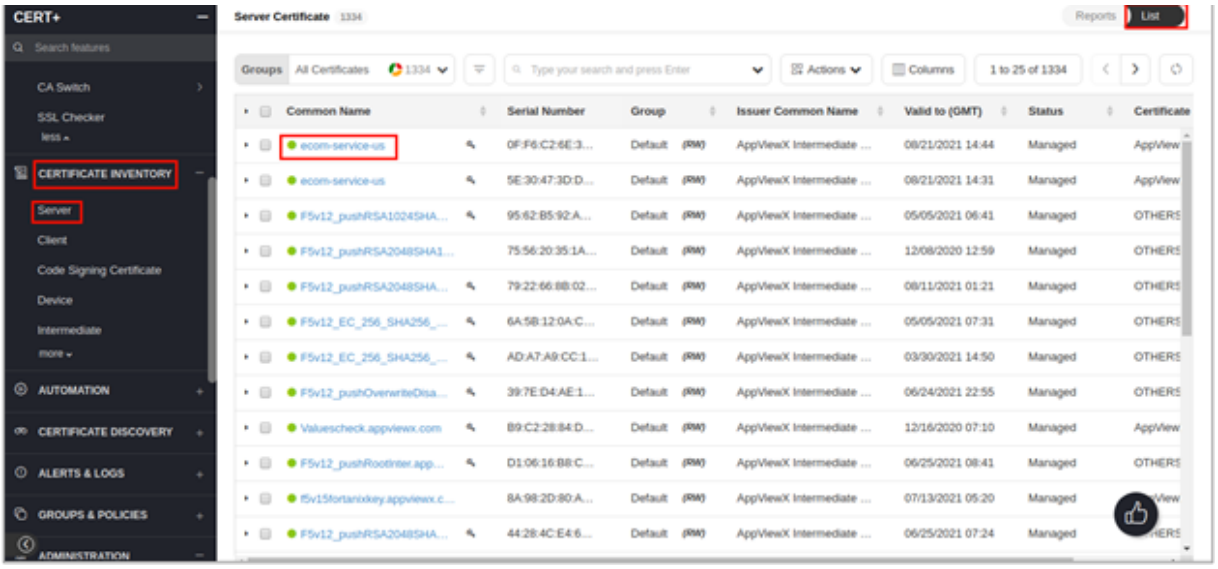
Following are the points needed to be known before starting the configuration for the history of certificates:

- 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

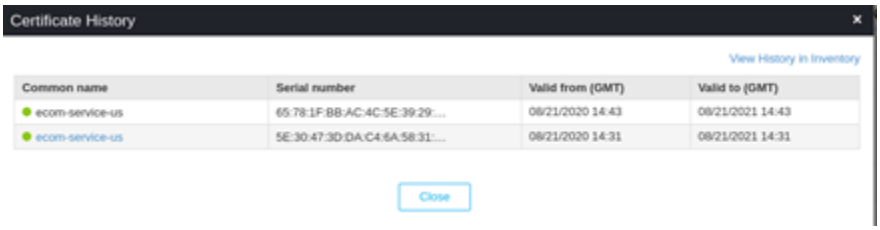
History of certificates, if enabled, can be checked on the Certificate Topology page by following these steps:

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.

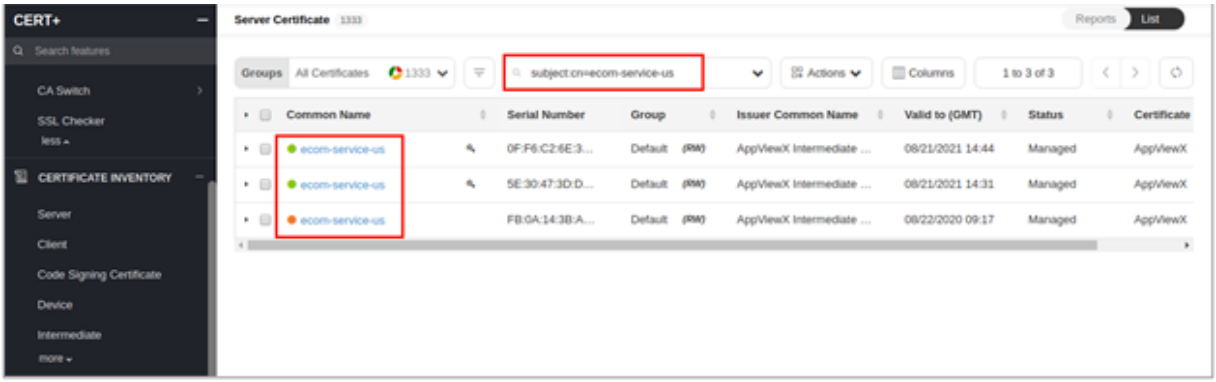


8. Click on the (History) icon on the certificate topology page to check the History of certificate. If the certificate renewal/regeneration was successful, the History icon will be present.

9. Click on the History to view the history of the certificate in the pop-up window.



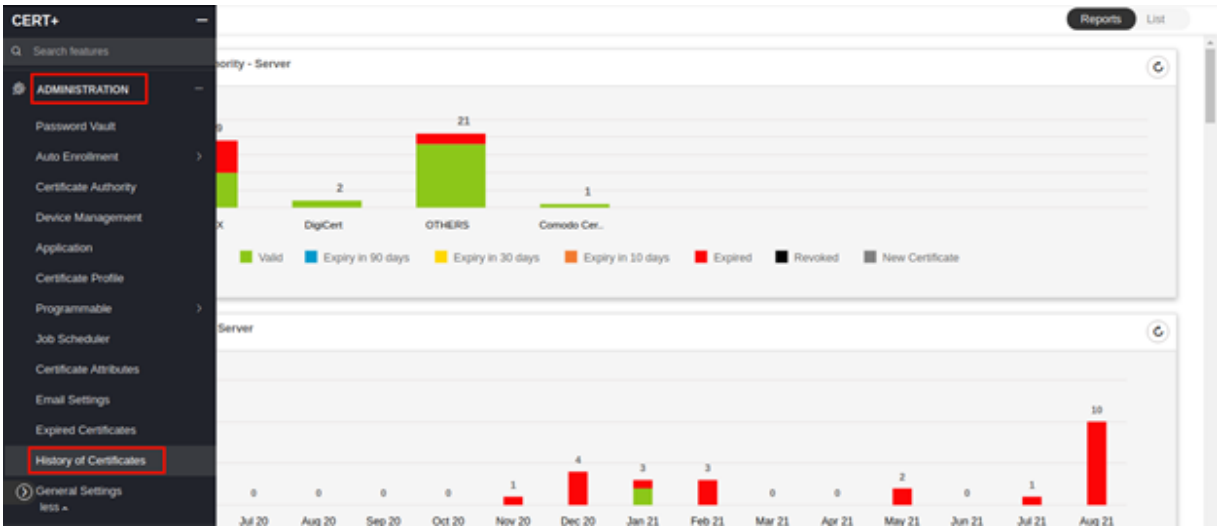
10. The respective query for this will be automatically framed and search results will be shown.



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

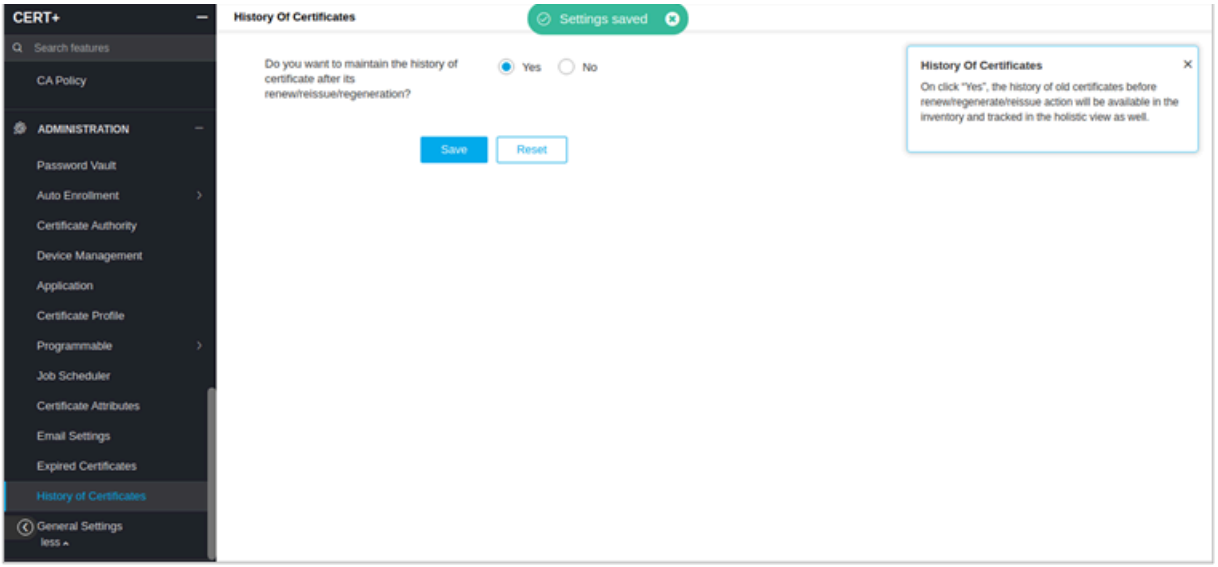
1. Log in to the **AppViewX** application with valid credentials.
2. Click the menu button.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. **Expand ADMINISTRATION.**
5. Under **Administration**, click **History of Certificates**.



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.



Configuring Certificate Profiles

Overview

AppViewX Cert+ offers administrators capability to define the type or purpose of a certificate through Certificate Profiles. An administrator can configure multiple Profiles definining 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

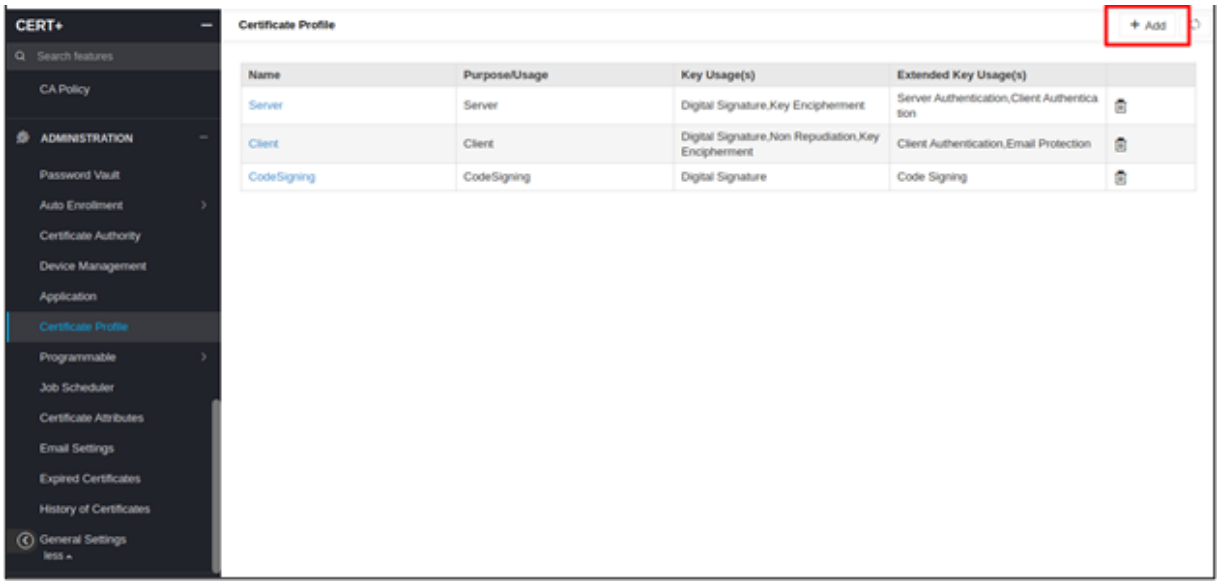
Following are the points needed to be known before starting to configure Certificate profile -

- 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:

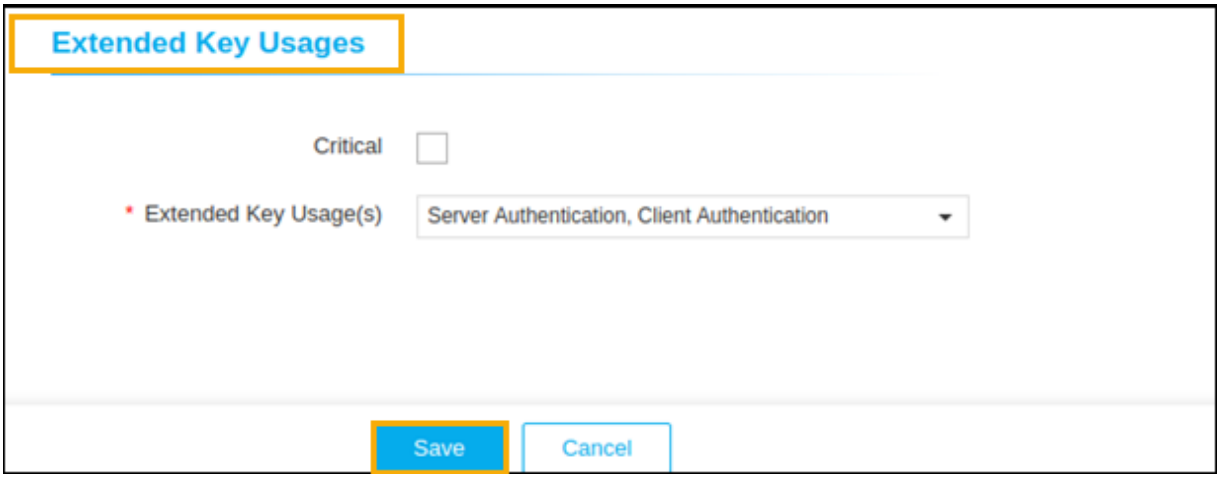
Name	Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the profile.	Profile name should not start with special characters. Can contain only alphanumeric characters, no special characters except -, _, . are allowed.
Purpose/Usage	Multi - Select	Yes	Certificate Type to which the Key	NA

Name	Type	Mandatory	Description	Validation
			Usage extensions are signed with. For example: Server or Client.	

7. Configure the **Key Usages** .

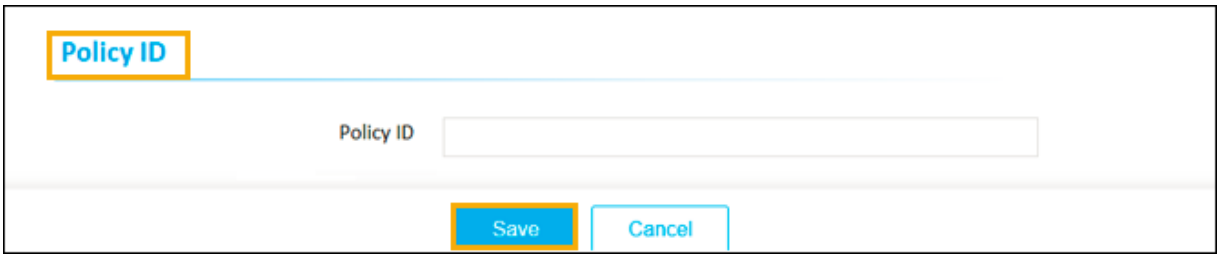
Name	Type	Mandatory	Description	Validation
Critical	Checkbox	No	Enable this field to sign the Key Usage extensions as **critical**.	NA
Key Usage(s)	Multi - Select	Yes	Key Usage extensions along with which the CSR is signed.	NA

8. Configure the **Extended Key Usages** as given below.



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 pollicy id in the field as given below.

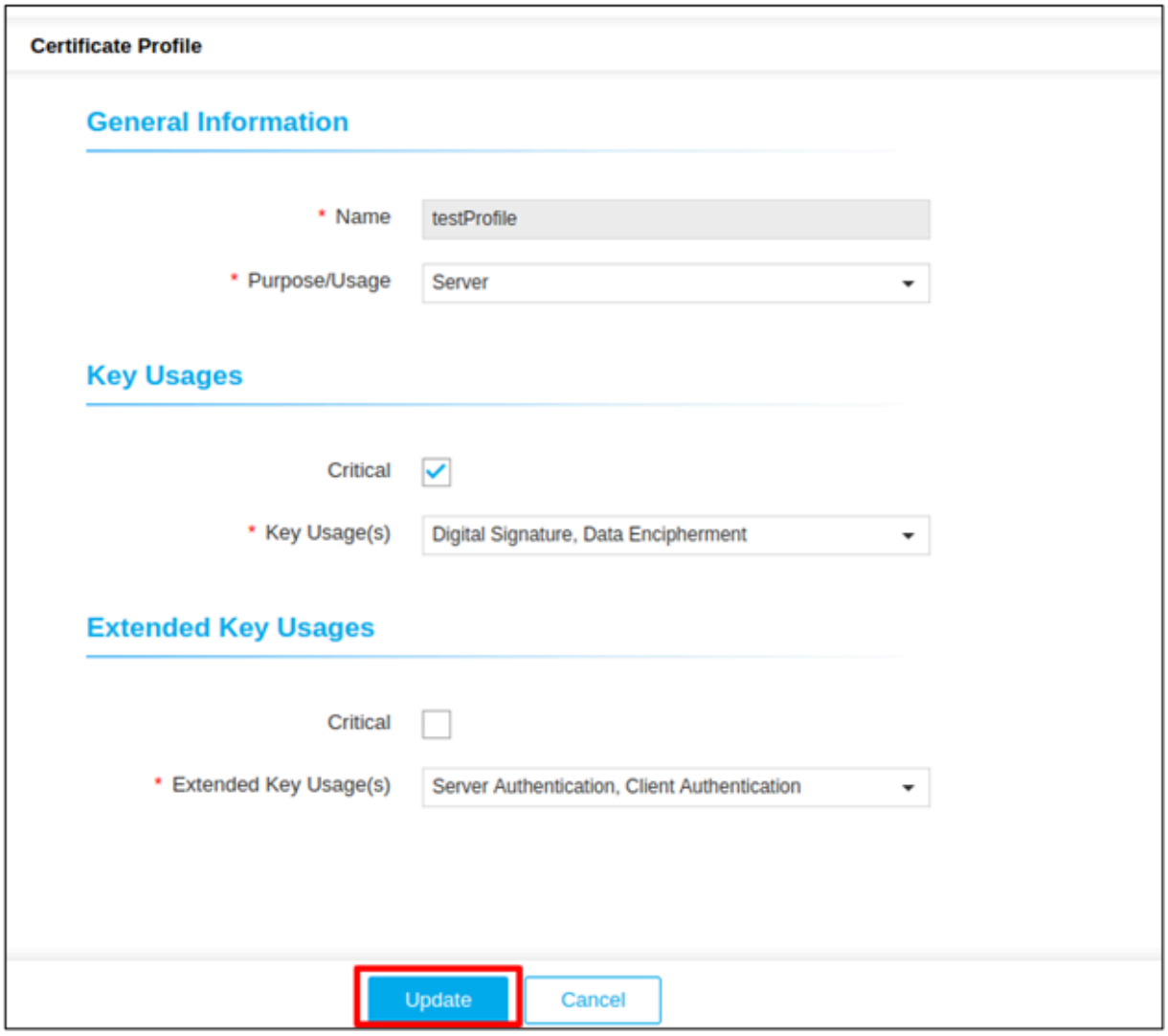


10. Click **Save**.

Update Certificate Profile

To update certificate profile settings:

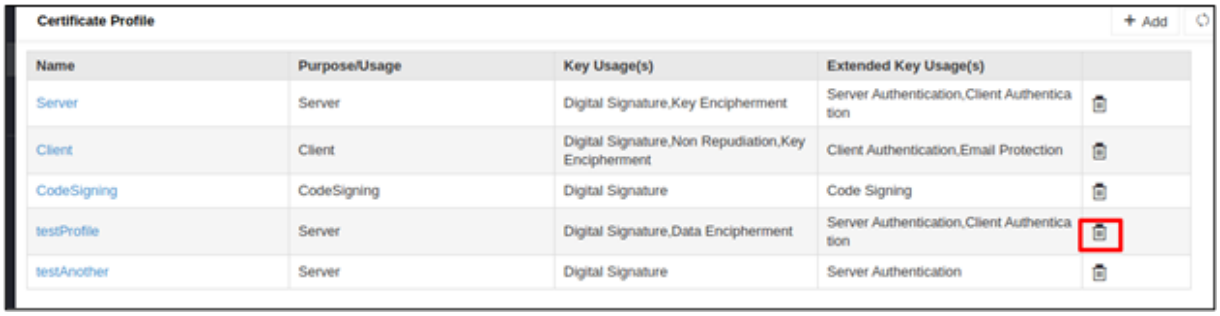
1. Click **Menu** > **CERT+** > **ADMINISTRATION**.
2. Under Administration, select **Certificate Profile**.
3. Click on the Profile that needs to be edited.
4. Edit existing values.
5. Click **Update.**



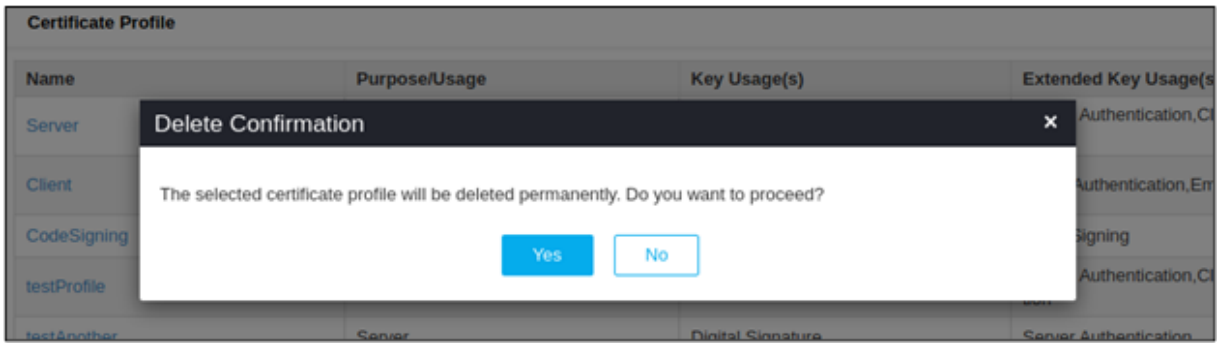
Delete Certificate Profile

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.



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

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.

   The following table describes the options available in the Server details section:

Options	Description
Server Type	Select the required server type. The possible options are: • Apache • Tomcat.
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.

8. In the **Credentials** section, select/enter the details as follows.

   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.
Username	Enter the desired username.
Password	Enter the secured password.

9. In the **Windows gateway details** section, select/enter the details as follows.

   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.

10. In the **Certificate details** section, enter the server path.

    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

11. Click the **Add** button**.**
12. Once the server is added successfully, the server path will be listed in the **Server path** section.
13. Click the Delete icon, if you want to delete the server path from the list.
14. The status of the server can be viewed in the Status column.
15. You can configure multiple device details 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.

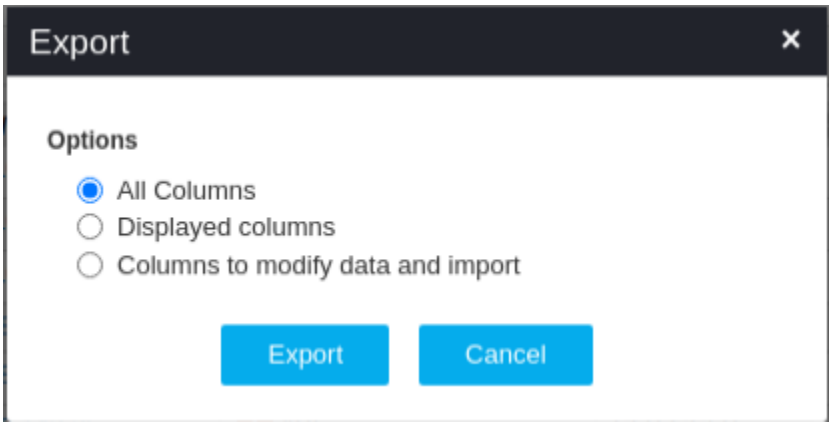
Export Server Details

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.

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.

4. Click the **Server** tab.
5. If the server is not listed on the screen, run a search to locate it.
6. Click the checkbox beside the server name. If you want to fetch configurations for multiple servers of the same type, select their checkboxes, too.
7. Click the **Fetch Config** icon in the command bar.
8. A notification appears at the top of the screen stating, "**Fetch config has been triggered for the server.**
9. The configuration will be fetched from the server.

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

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.

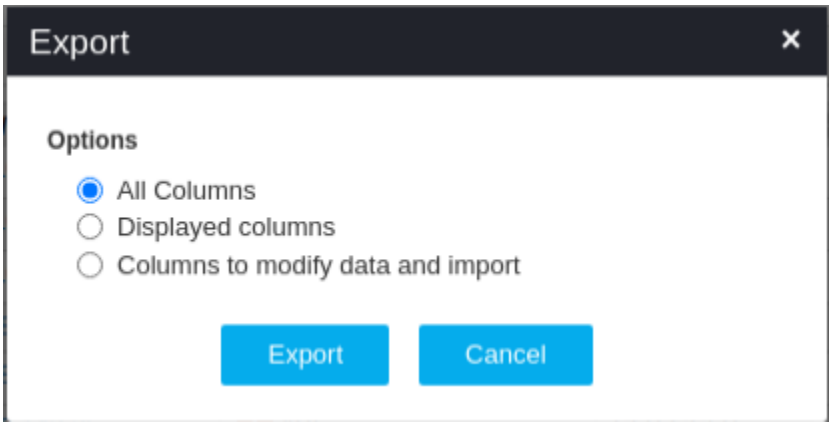
Export Firewall Details

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

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.

Unmanage Cloud

To unmanage the cound 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.

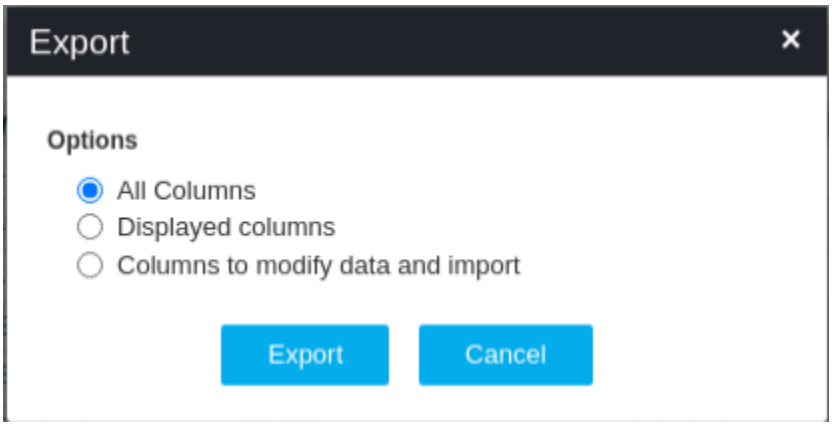
Export Cloud Details

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
- Configuring Report Settings and Schedule
- Job Scheduler
- Device and Certificate Synchronization
- CRL Certificate Revocation Check
- 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

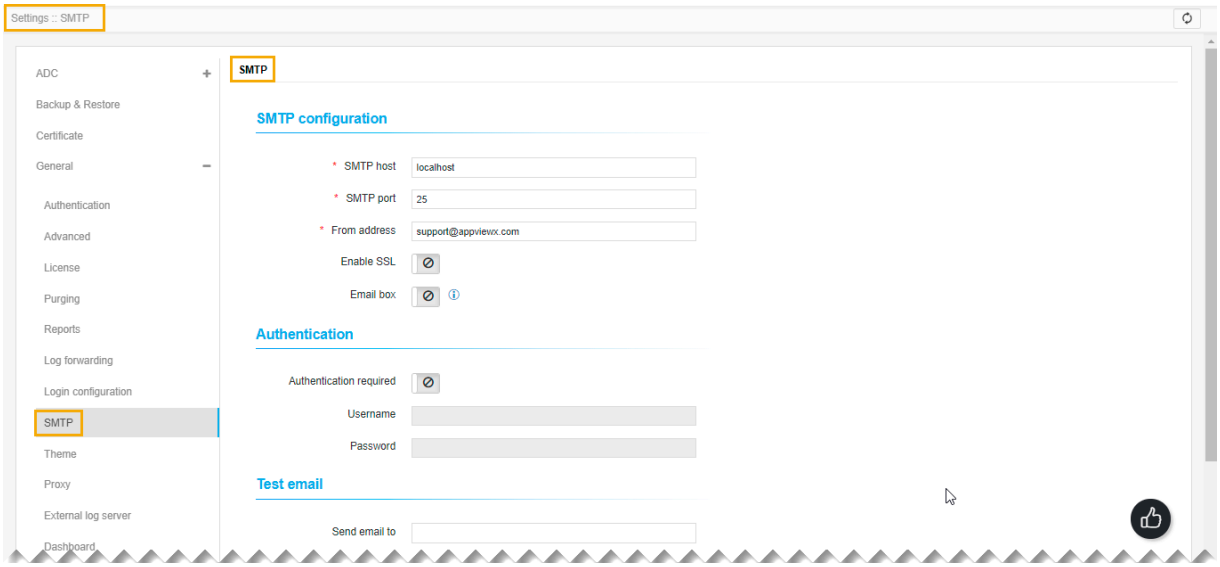
Following are the prerequisites for configuring certificate Reports in AppViewX:

- 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.**



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
* Username	Text	Mandatory if Authentication required is selected as true.	The username if authentication required.	NA

Name	Type	Mandatory	Description	Error Message
* 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

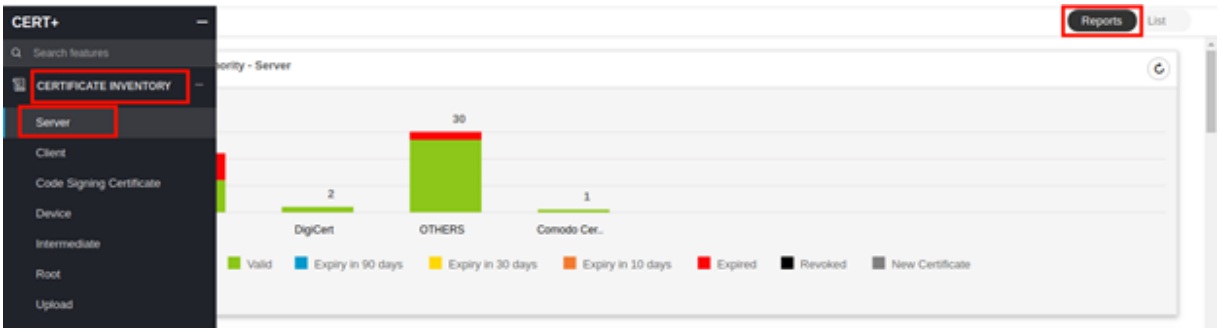
Error Message	Possible Cause	Possible Solution
Please provide a valid value.	Anyone of the mandatory fields is invalid or is missing.	Provide valid values for all mandatory fields.
E-Mail sending was unsuccessful.	• If trying to test, no/valid email is not provided in the ‘send email to’ field. • Credentials 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.



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.

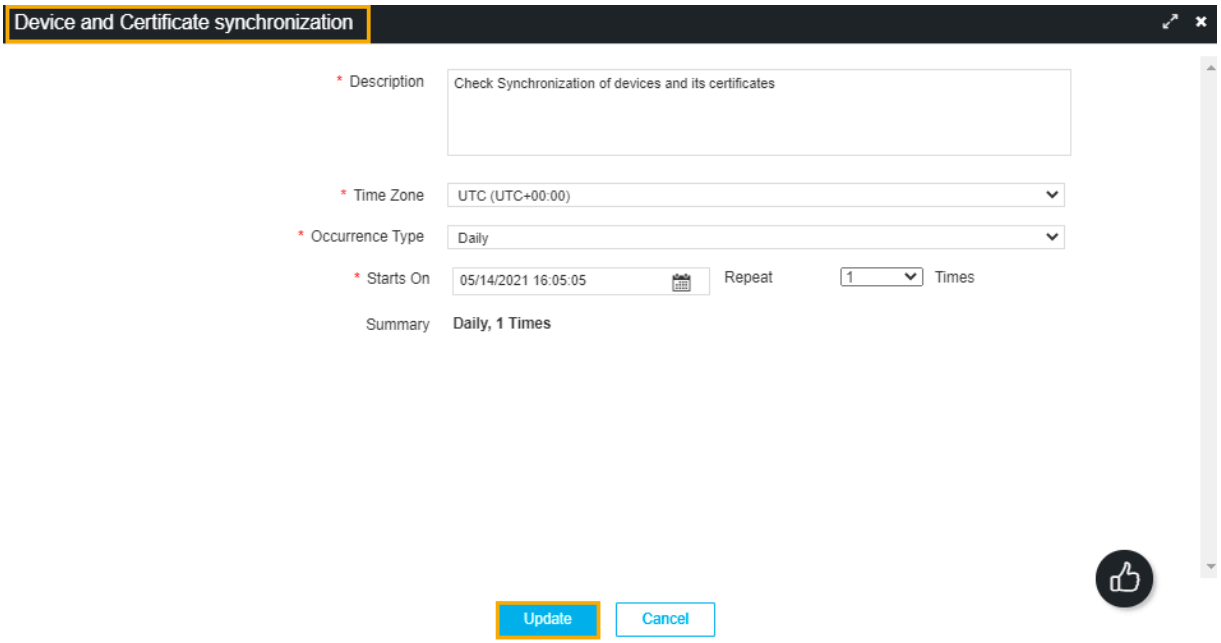
To configure the Job Scheduler,

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
Sear 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.



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 • Monthly • Yearly.
* **Start On**	Set the start date and time.

Options	Description
Repeat	The number of times the job schedulers to be completed. **Note:** You can repeat this activity maximum of Six times.
Summary	Displays the occurrence type and frequency of the job scheduler.

8. After configuring the details, click **Update**.

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

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.

> **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

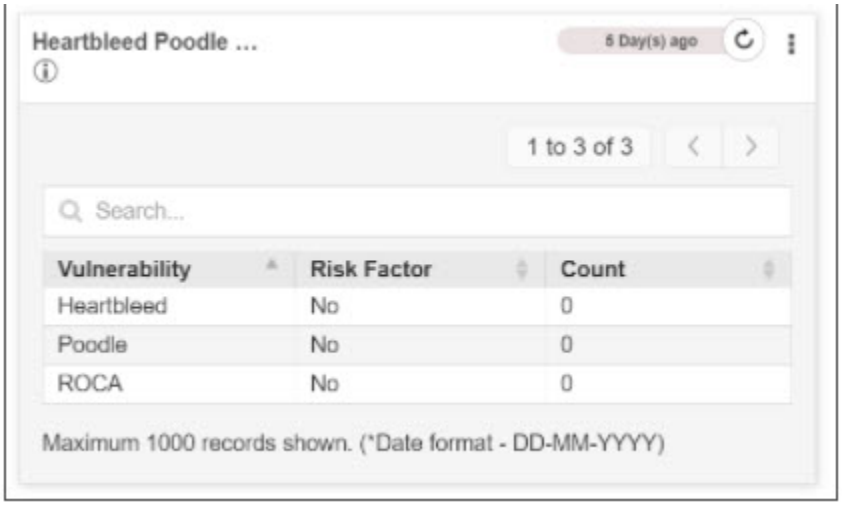
- The cron job is executed to check the certificates and their device association
- There is internal business logic to check the Poodle, Heart bleed, and Roca vulnerabilities for the associated device.
- Once the job is completed the “Vulnerability reports” are updated in “Server_Endpoint_Security”, “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

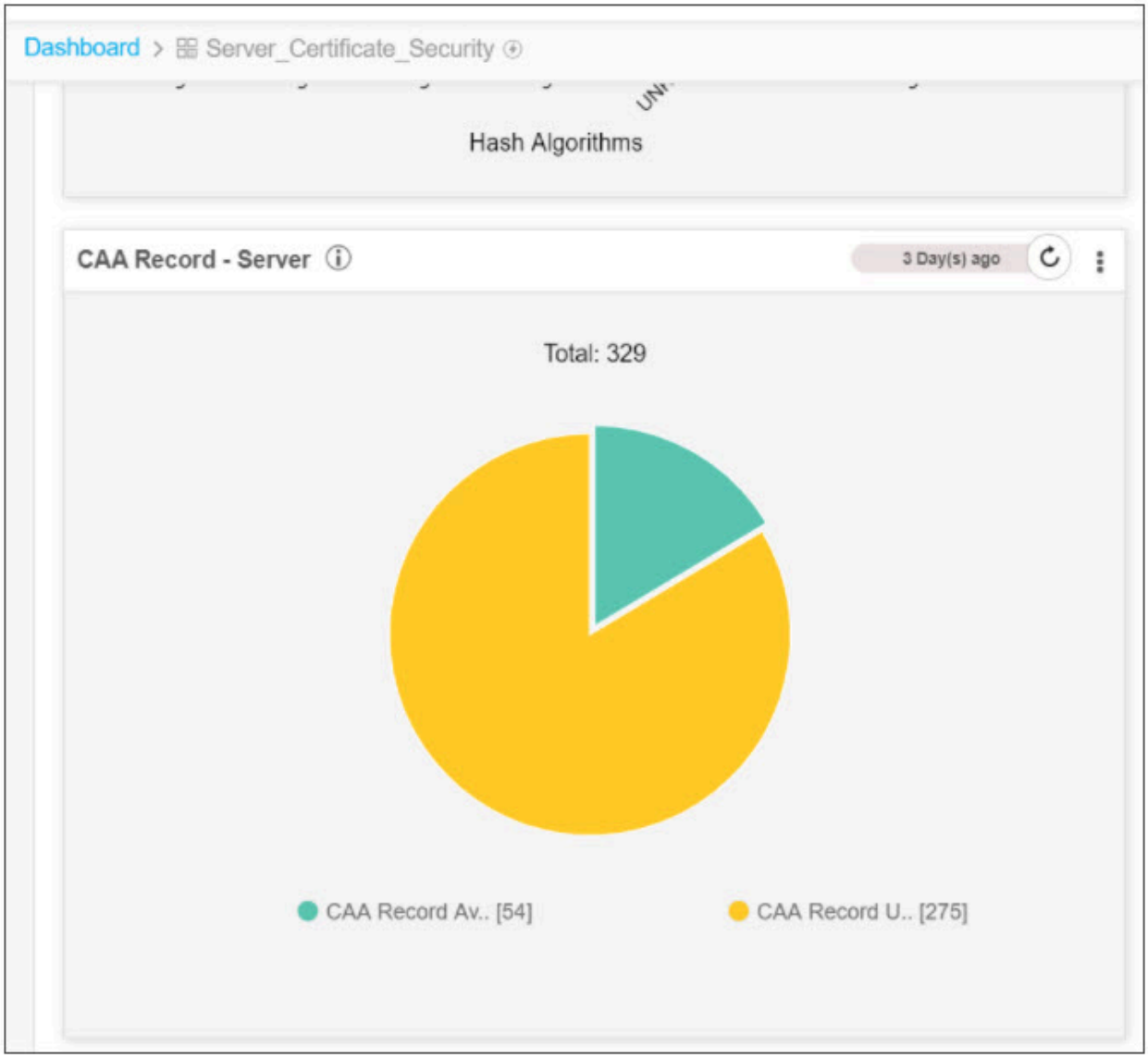
The internal business logic to check the vulnerability of the device. It is captured via audit logs and notification logs in the logging module.



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

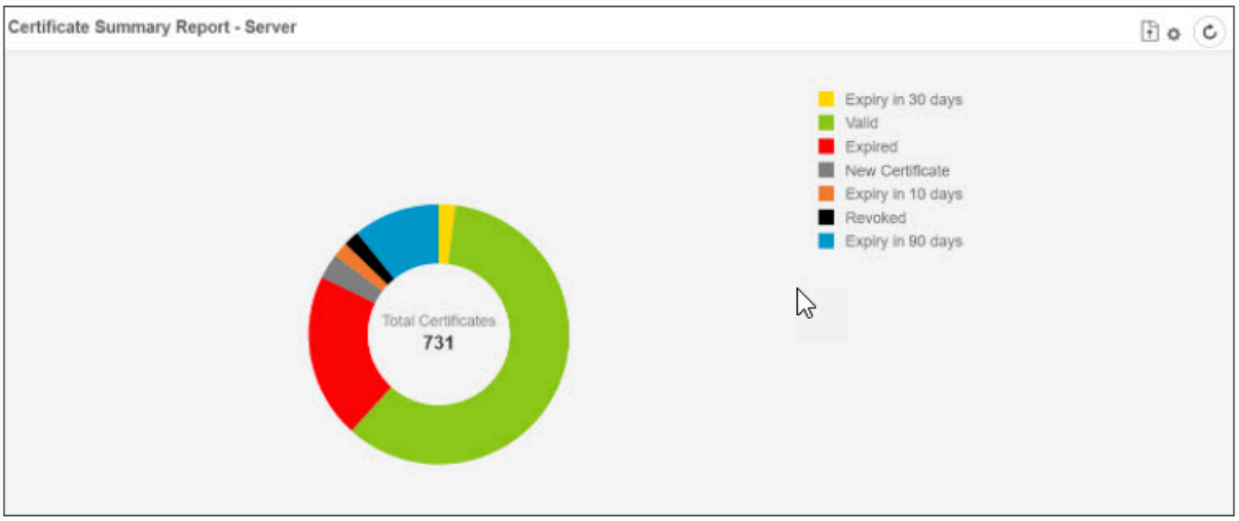
The scheduled job is monitored and triggered by default weekly, on Sunday.

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.

Report Routing

This functionality is applicable only to the following reports:

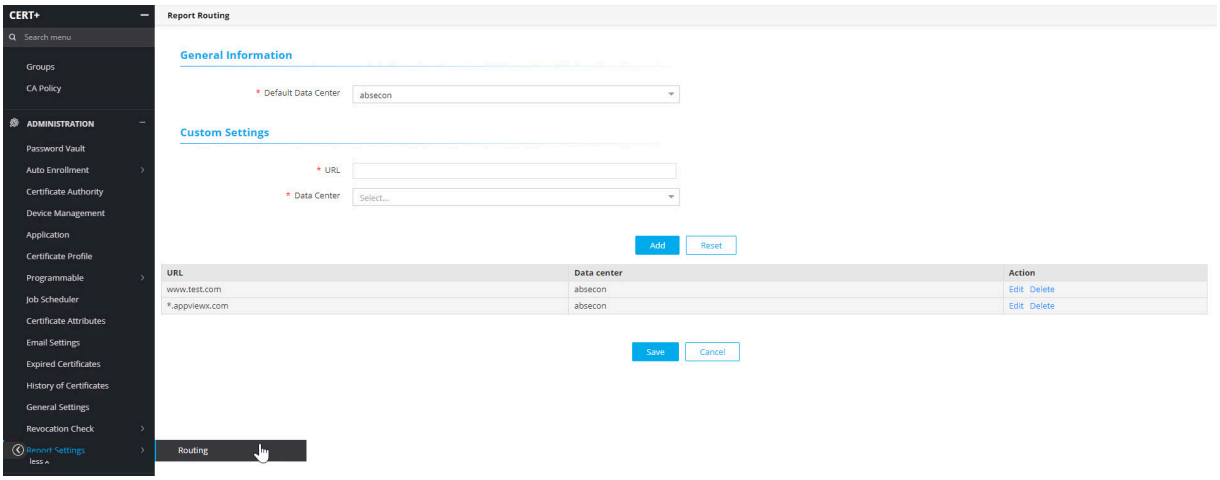
- Validation report
- Vulnerability report
- CAA report

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.

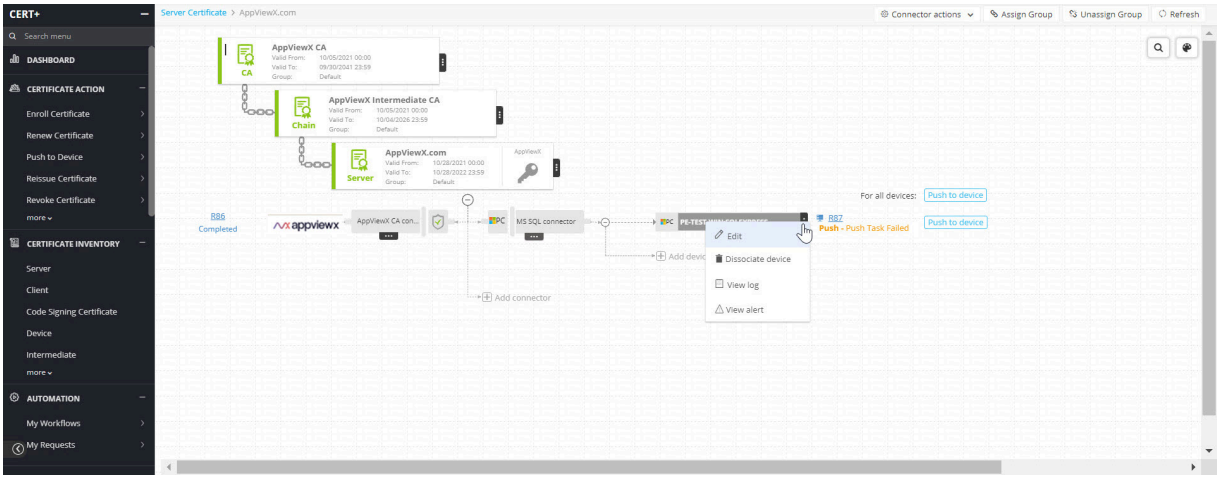
> **Note:** To perform a bulk operation on certificate URLs, you can specify a wildcard character with their domain name, for example, if you want to specify a data center to all the AppViewX certificates at one go, then use wildcard character as in *.appviewx.com and select the data center from the dropdown list.

7. Click **Add.**
8. If you want to edit the certificates, then use the **Edit** option.

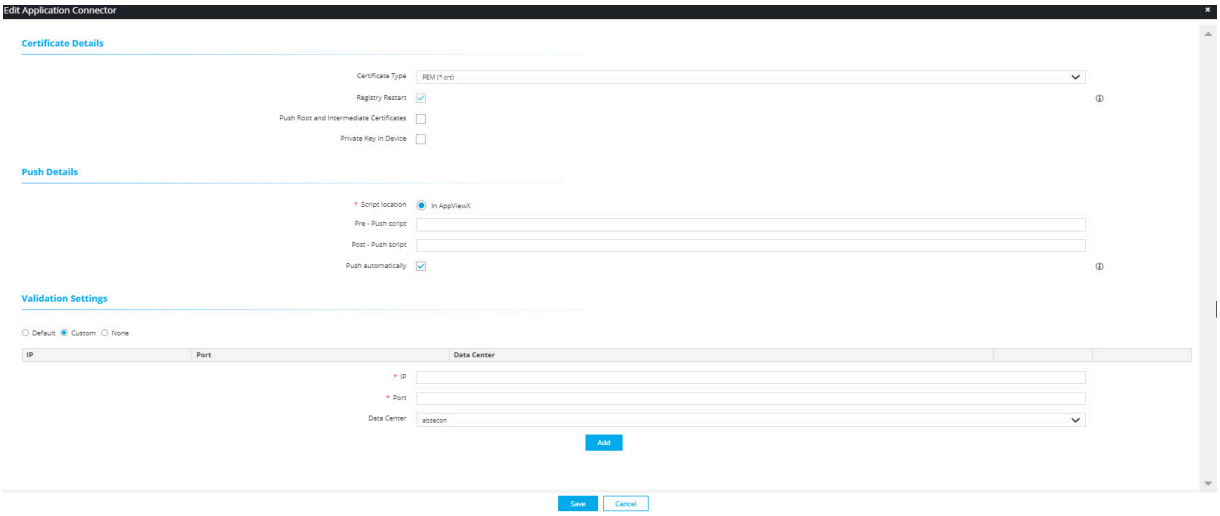
Validation Settings

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.



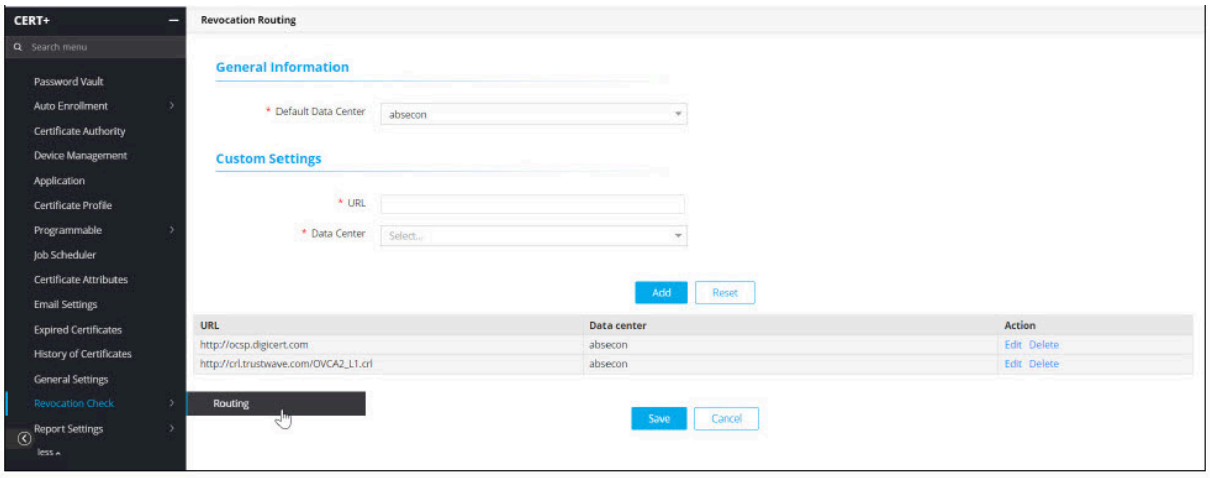
3. Select **Custom** option.
4. In the **Validation Settings** section, select the data center from the dropdown list.
   This ensures that for any validation check, this is treated as high priority.

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. If the job failed, then go to **Administration > Logging > Certificate** and check the log message.

Field	Description
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.

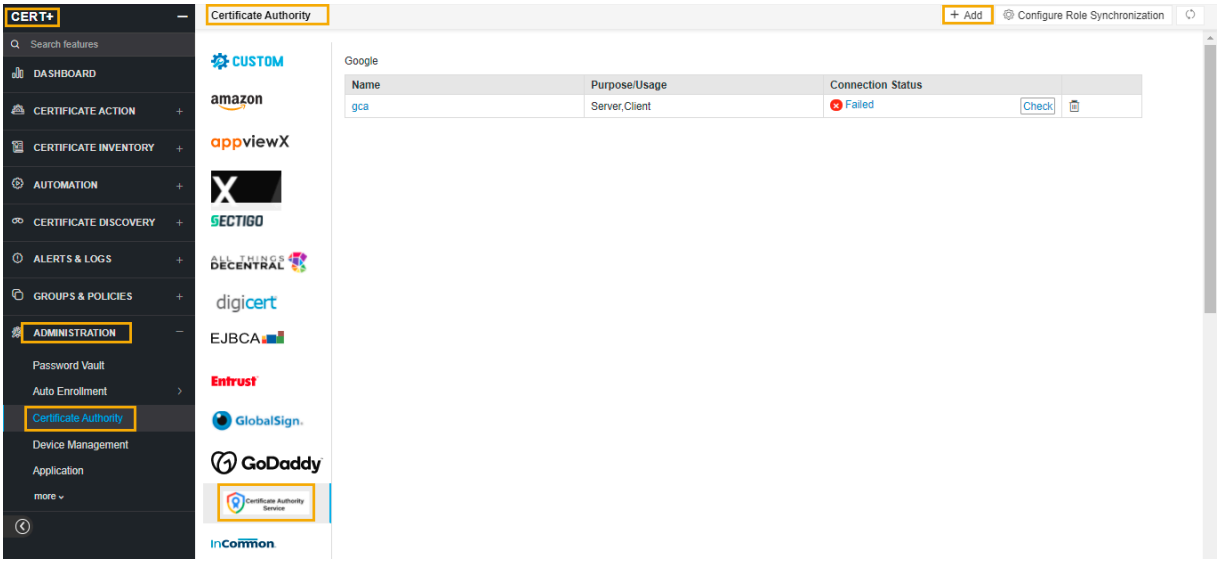
   The table is refreshed with a row entry of the newly added URL and the data center.

Configure Certificate Authority

To configure a certificate authority:

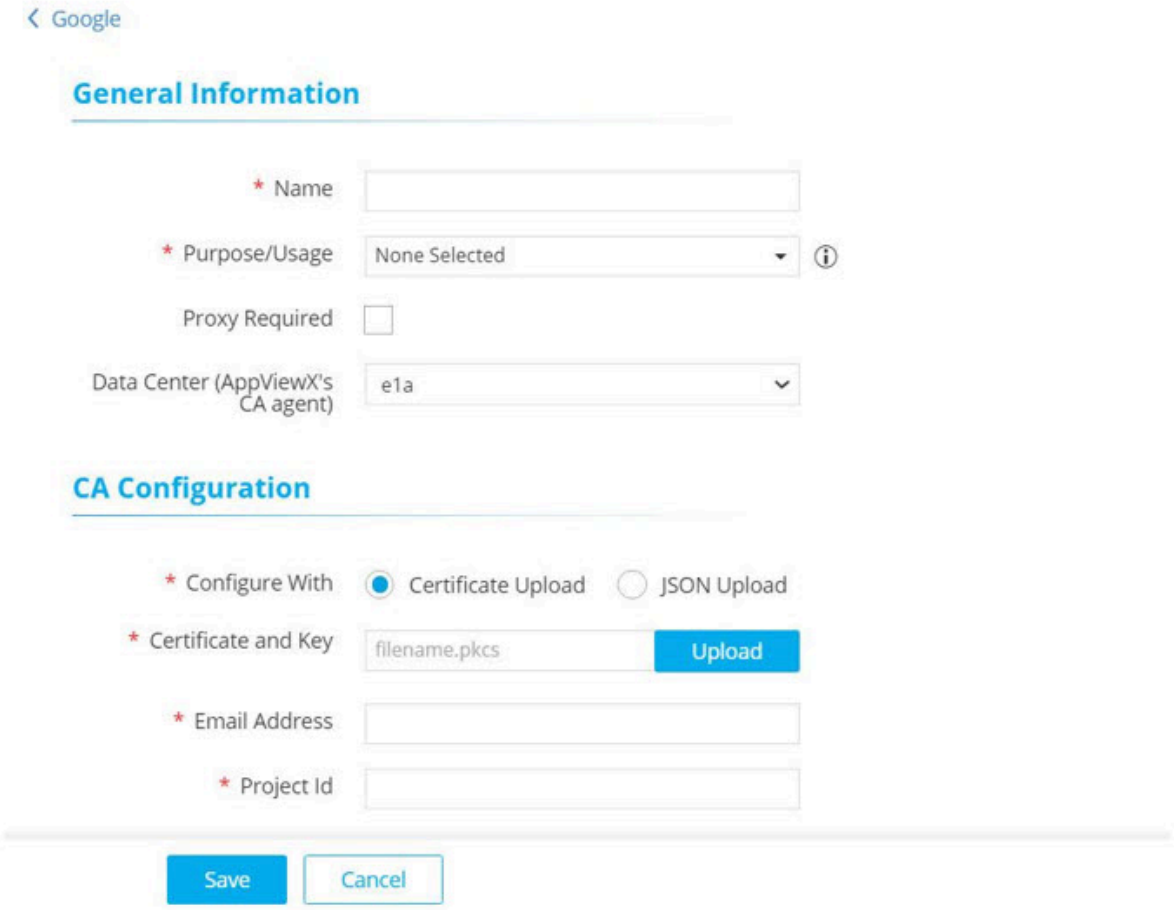
1. Click the **Menu** ( ) icon.
2. Click **CERT+**.

   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.



5. Click **+ Add** on the top-right of the page.

The CA configuration page appears.



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.

Field	Description
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.

Note: Fields marked with red asterisk (*) symbol are mandatory.

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

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

Before you Begin

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 an agent(avx_vendor_cert_acme_agent) up and running for ACME in AppViewX.
- This ACME 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.

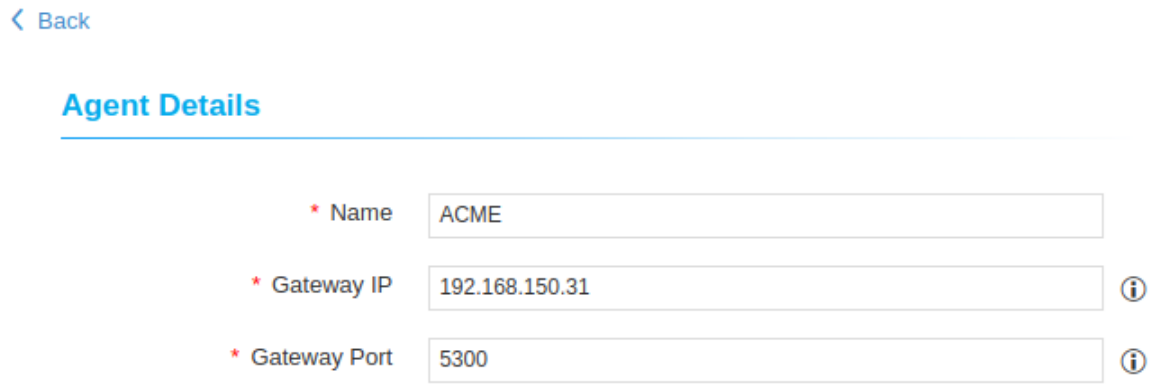
- It is highly recommended to **OFF** the approval Required flag in **Menu > Inventory > Certificate > Policy** page.
- A valid agent settings should be available in **Menu > Inventory > Certificate > Settings**.

Configuring ACME

In order to perform enrolment, CA setting details and agent details needs to be configured to proceed with.

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 **CERT+** > **ADMINISTRATION** > **AutoEnrolment** > **ACME**.
4. Select **Add** or **Configure Now**.
5. Configure the **Agent Details** as follows:

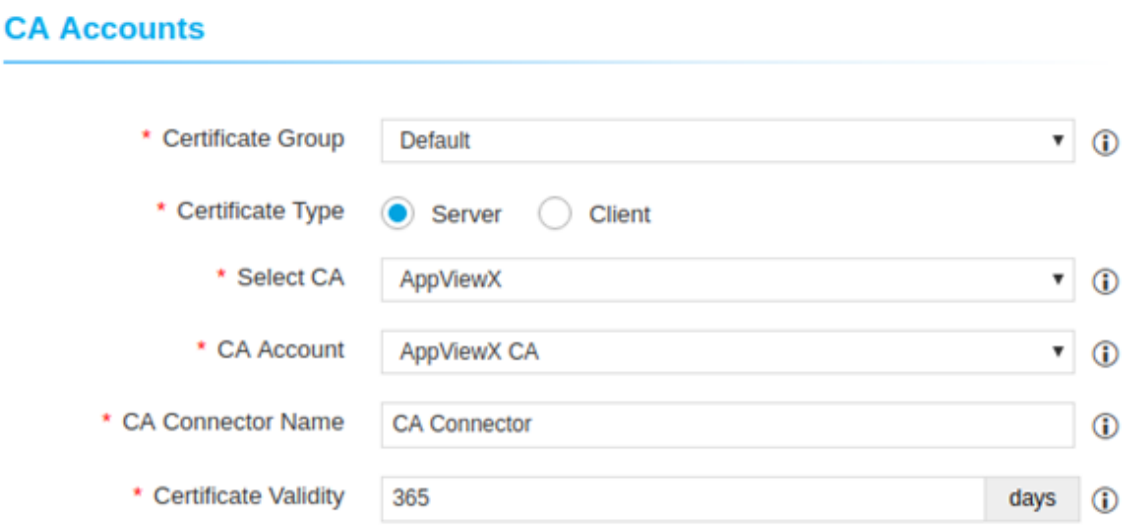
Name	Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the agent setting.	No special characters other than '.', '-','_' are allowed. Name should not start with special characters.
Gateway IP Address	Text	Yes	IP address of the appviewx node gateway.	Invalid IP address(example: xxx.xxx.xxx.xxx)
Gateway Port	Text	Yes	HTTP gateway port of the appviewx node.	Port will accept only numerical values between 0 to 65535.



6. Configure the **CA Accounts** details as follows:

Name	Type	Mandatory	Description	Validation
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.	NA
Certificate Type	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Select	Yes	Select a specific CA from which the certificate needs to be enrolled. **Note:** If the selected CA is **Entrust MPKI**, a separate section displaying **Vendor Specific Details** is displayed after the **CA Accounts** section. Under the **Vendor Specific Details** section: Select the required **CA Name** and the **Cert Profiles**.	NA
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.	NA
CA Connector Name	Text	Yes	Name of the CA connector after certificate is being enrolled.	NA

Name	Type	Mandatory	Description	Validation
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.	Certificate validity accepts only numerical values



7. Configure the **Advanced Settings** details as follows:

Name	Type	Mandatory	Description	Validation
Retry Count	Text	Yes	Specify a retry count upto which the agent will retry for the certificate to be fetched.	NA
Retry Frequency	Text	Yes	Specify a retry frequency upto which the agent will wait for each retry count.	NA

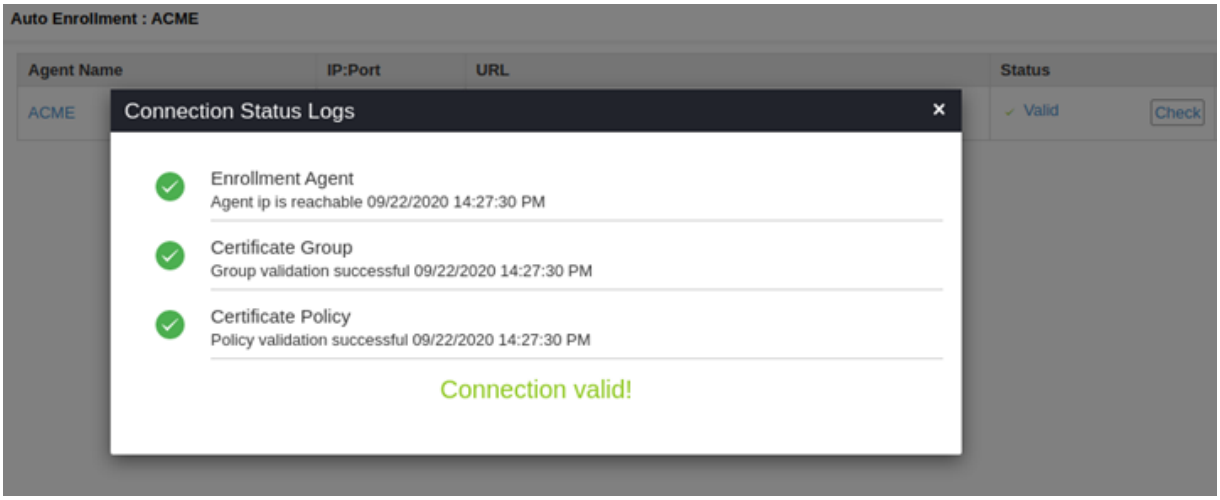
8. Click **Save**.

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 is Enrollment over Secure Transport, which is a certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire certificates and associated CA certificates. Architecturally, the EST service(agent) is located between a CA and a client. AppViewX supports the Enrolment operation via EST server in HTTPS mode.

- 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

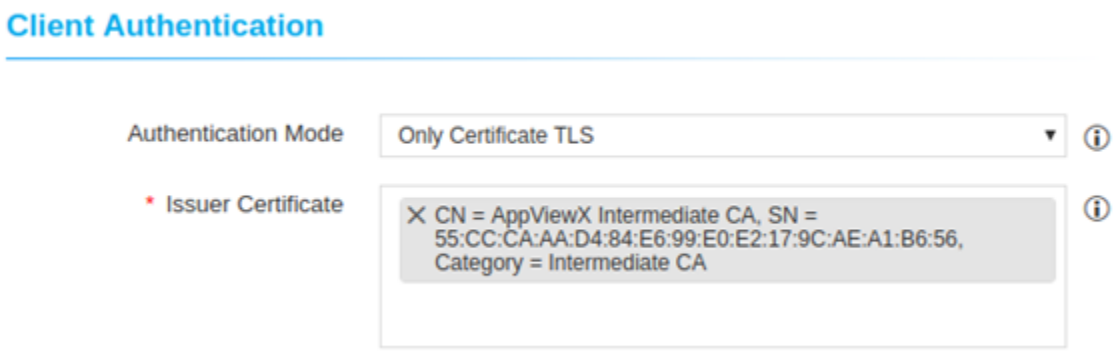
In order to perform enrolment, CA setting details and agent details needs to be configured to proceed with.

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 **CERT+** > **ADMINISTRATION** > **AutoEnrollment** > **EST.**
4. Select **Add** or **Configure Now.**
5. Configure the **Agent Details** details as follows:

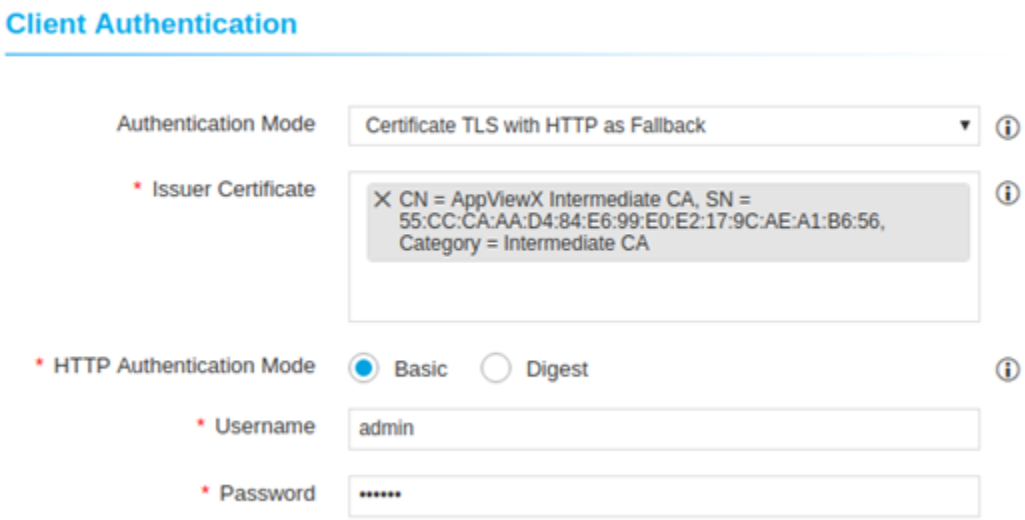
Name	Type	Mandatory	Description	Validation
Name	Text	Yes	Unique name to identify the Agent setting.	No special characters other than '.', '-','_' are allowed. Name should not start with special characters.
IP Address	Text	Yes	IP address of the appviewx node.	Invalid IP address(example: xxx.xxx.xxx.xxx)
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 **Client Authentication** details as follows:

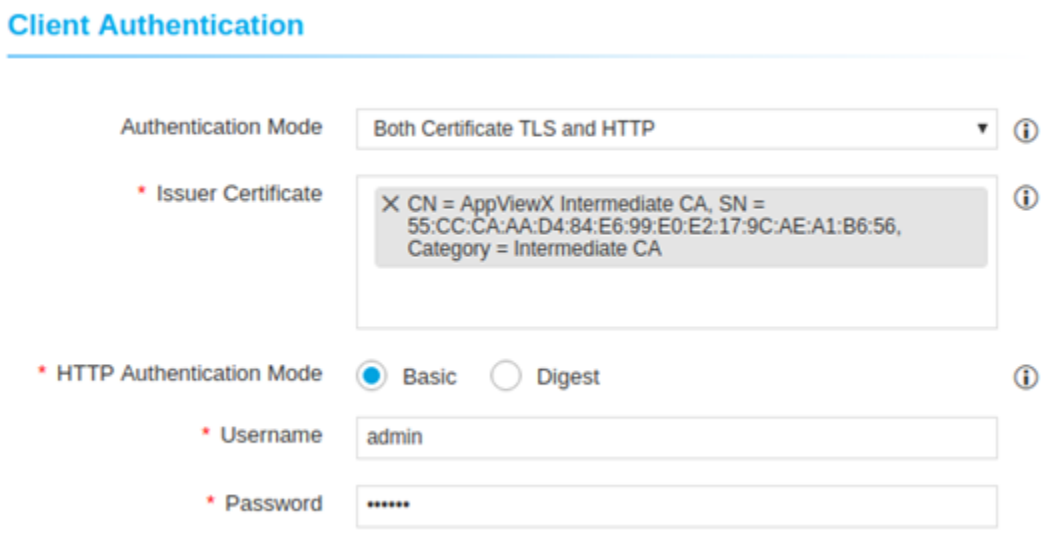
Name	Type	Mandatory	Description	Validation
Authentication Mode	Select	Yes	Select any one authentication method to be carried out during communication with clients.	NA
Issuer Certificate	Select	Yes	Select one or more issuer certificates which needs to be checked for the client certificate authentication.	NA
HTTP Authentication Mode	Select	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



Only Client Certificate Authentication Mode

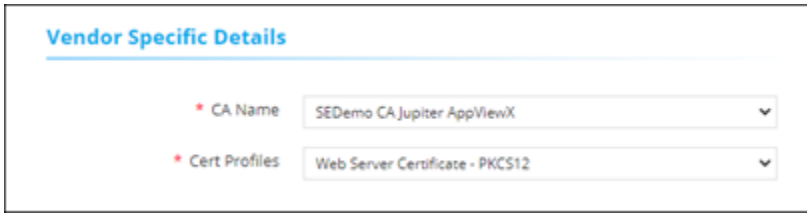


Client Certificate Authentication with HTTP Fallback Mode

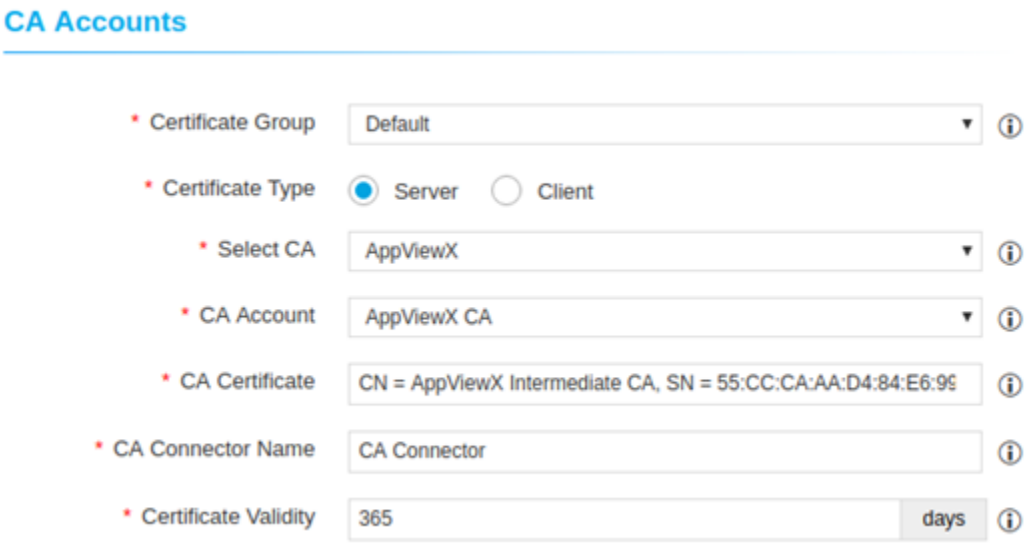


Both Client certificate and HTTP Authentication Mode

7. Configure the **CA Accounts** details as follows:

Name	Type	Mandatory	Description
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.
Certificate Type	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.
Select CA	Select	Yes	Select a specific CA from which the certificate needs to be enrolled. **Note**: If the selected CA is **Entrust MPKI**, a separate section displa **Vendor Specific Details** is displayed after the **CA Accounts** sectio  Under the **Vendor Specific Details** section: Select the required **CA** and the **Cert Profiles**.
CA Account	Select	Yes	Select a specific CA Account from the selected CA which is to be us certificate creation operations.

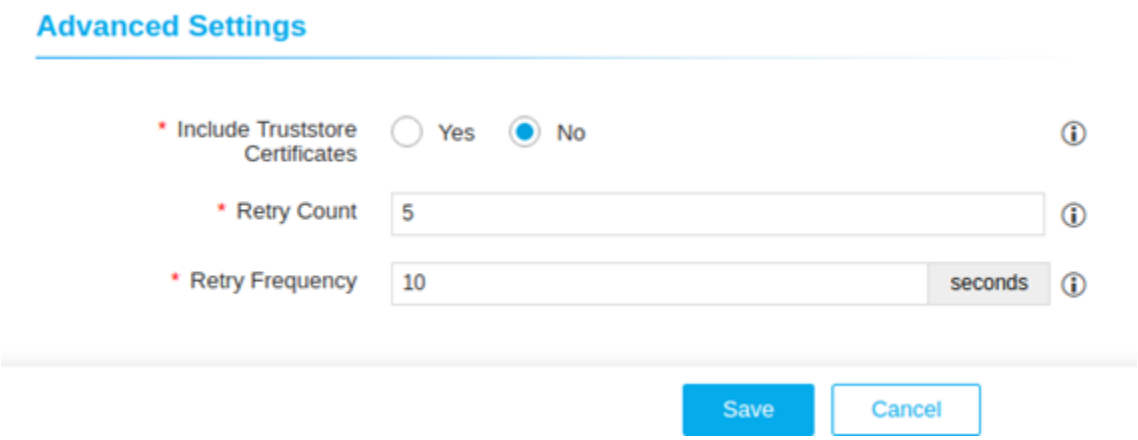
Name	Type	Mandatory	Description
Server Certificate	Select	Yes	Type 3 or more letters of the certificate keywords after which a list of certificates issued from the above selected CA account will be displa one certificate can be selected for further communications with EST machine.
CA Connector Name	Text	Yes	**Name of the CA connector after certificate is being enrolled.**
Certificate Validity	Text	Yes	Validity of the certificate to be enrolled.



8. Configure the **Advanced Settings** details as follows:

Name	Type	Mandatory	Description	Validation
Include Truststore Certificates	Select	Yes	Select whether issuer certificate needs to be sent to client machines after enrolment.	NA
Retry Count	Text	Yes	Specify a retry count upto which the agent will retry for the certificate to be fetched.	NA

Name	Type	Mandatory	Description	Validation
Retry Frequency	Text	Yes	Specify a retry frequency upto which the agent will wait for each retry count.	NA

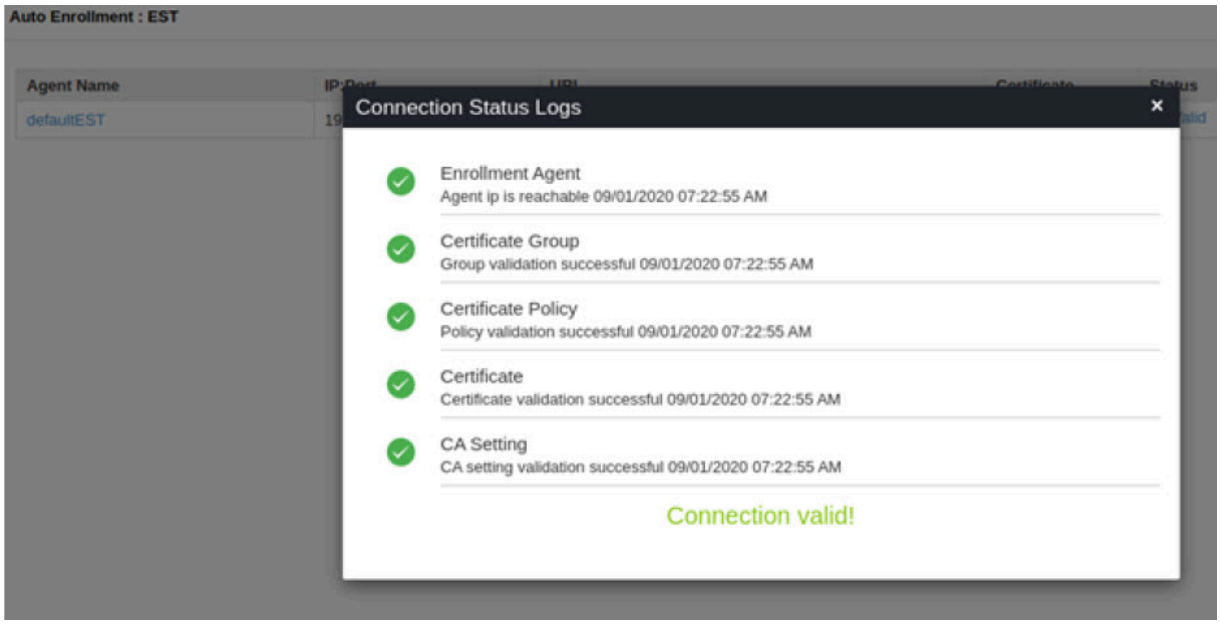


9. Click **Save**.

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

Before you Begin

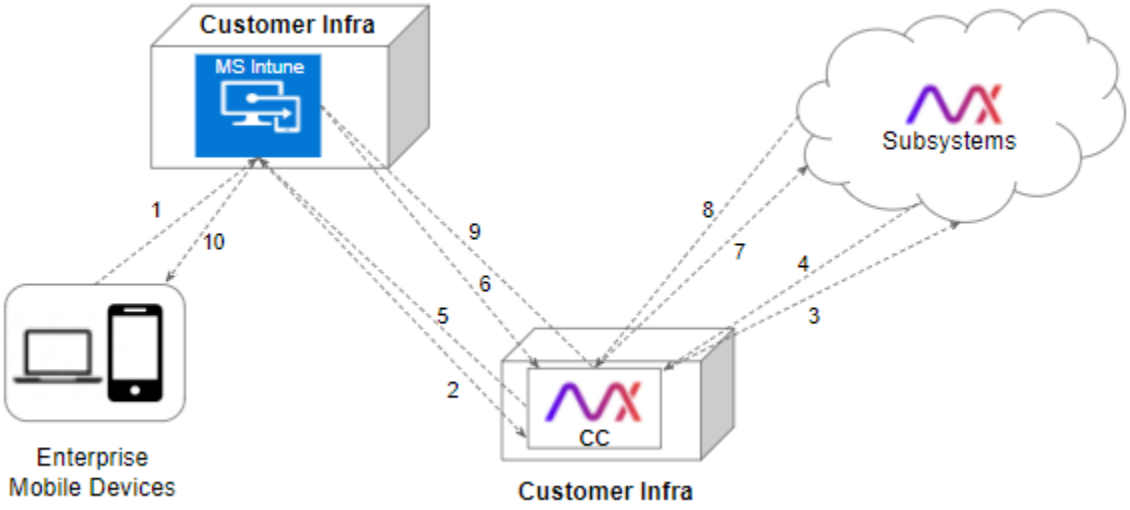
Microsoft Intune is a cloud-based management solution that provides for mobile device and operating system management. Architecturally, the Intune service(agent) is located between a CA and a client.

- 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**.

Prerequisites

Based on the above flow for the MS Intune enrollment to work the all CCs in the customer network should be able to reach MS Intune.

Explanation



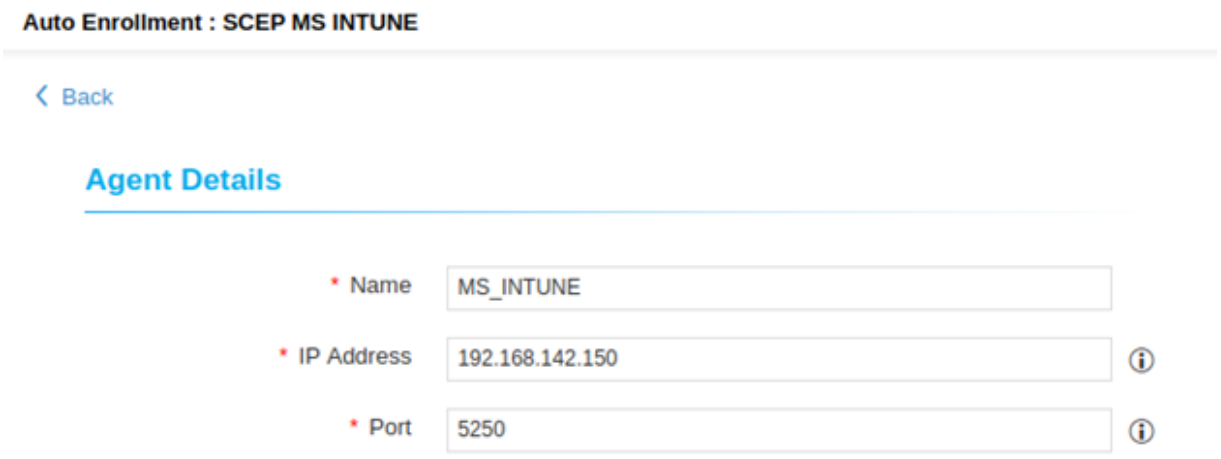
1. Mobile device requests certificate enrollment
2. MS Intune forwards the request to AppViewX Cloud Connector (CC) residing in Customer's Infrastructure (onprem or cloud).
3. CC forwards the request to AppViewX subsystems in cloud.
4. Subsystem forwards client authentication challenge request to CC.
5. CC forwards the client authentication challenge request to MS Intune.
6. MS Intune responds to the authentication challenge request on behalf of the client.
7. CC forwards authentication request response to AppViewX Subsystems.
8. AppViewX subsystem forwards the Certificate to CC.
9. CC sends the certificate back to MS Intune.
10. MS Intune assigns the certificate to device.

Configuring MS Intune

In order to perform enrolment, CA setting details and agent details needs to be configured to proceed with.

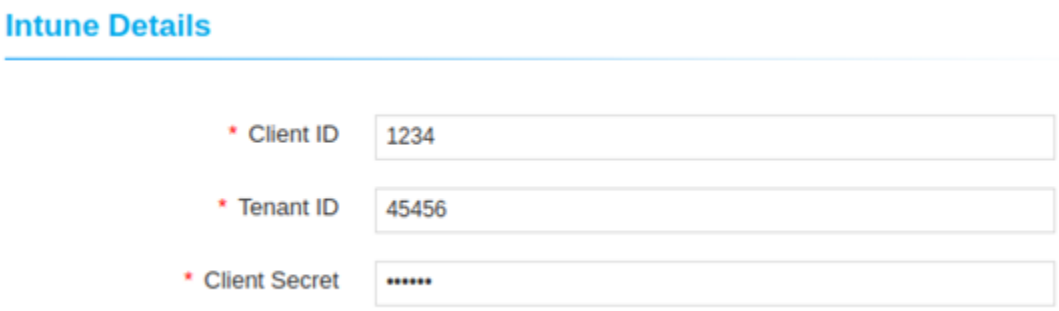
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Navigate to **CERT+** > **ADMINISTRATION** > **AutoEnrolment** > **MS INTUNE**.
4. Select **Add** or **Configure Now**.
5. Configure the **Agent Details** details as follows:

Name	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 Address	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.



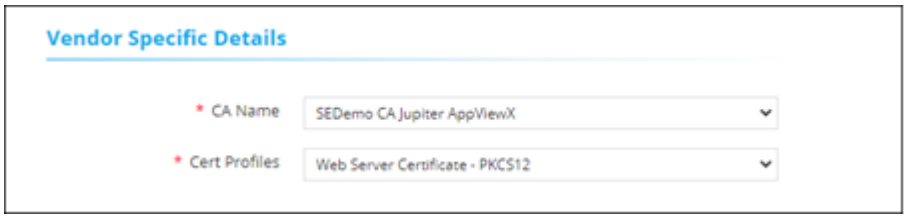
6. Configure the **Intune Details** as below:

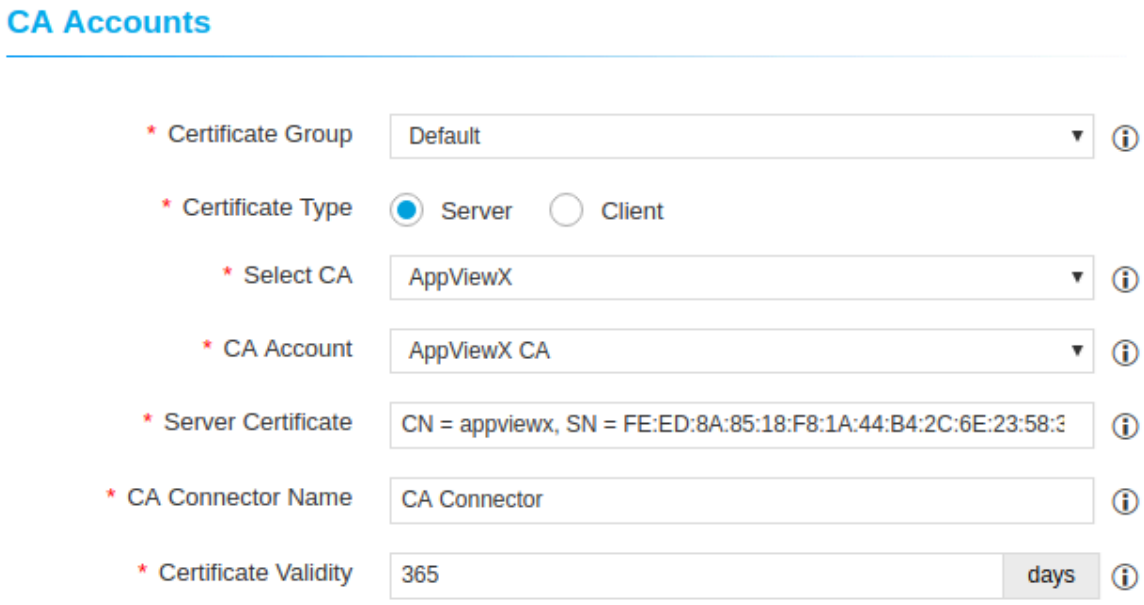
Name	Type	Mandatory	Description	Validation
Client Id	Text	Yes	Client ID of the Intune Account - this value should have been captured during Intune App Registration.	NA
Tenant Id	Text	Yes	Tenant ID is the domain name in your account ID. For example, if your account id is **admin@test.onmicrosoft.com** 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:

Name	Type	Mandatory	Description	Valida
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.	NA
Certificate Type	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Select	Yes	Select a specific CA from which the certificate needs to be enrolled.	NA

Name	Type	Mandatory	Description	Valida
			Note: If the selected CA is **Entrust MPKI**, a separate section displaying **Vendor Specific Details** is displayed after the **CA Accounts** section.  Under the **Vendor Specific Details** section: Select the required **CA Name** and the **Cert Profiles**.	
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, one certificate can be selected for further communications with SCEP 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.	Certific validity accept only numeri values



8. Configure the **Advanced Settings** as follows:

Name	Type	Mandatory	Description	Validation
Retry Count	Text	Yes	Specify a retry count upto which the agent will retry for the certificate to be fetched.	NA
Retry Frequency	Text	Yes	Specify a retry frequency upto which the agent will wait for each retry count.	NA
Certificate Poll Type	Select	Yes	Select a specific type to poll the issued certificate from agent to subsystem certificate plugin.	NA

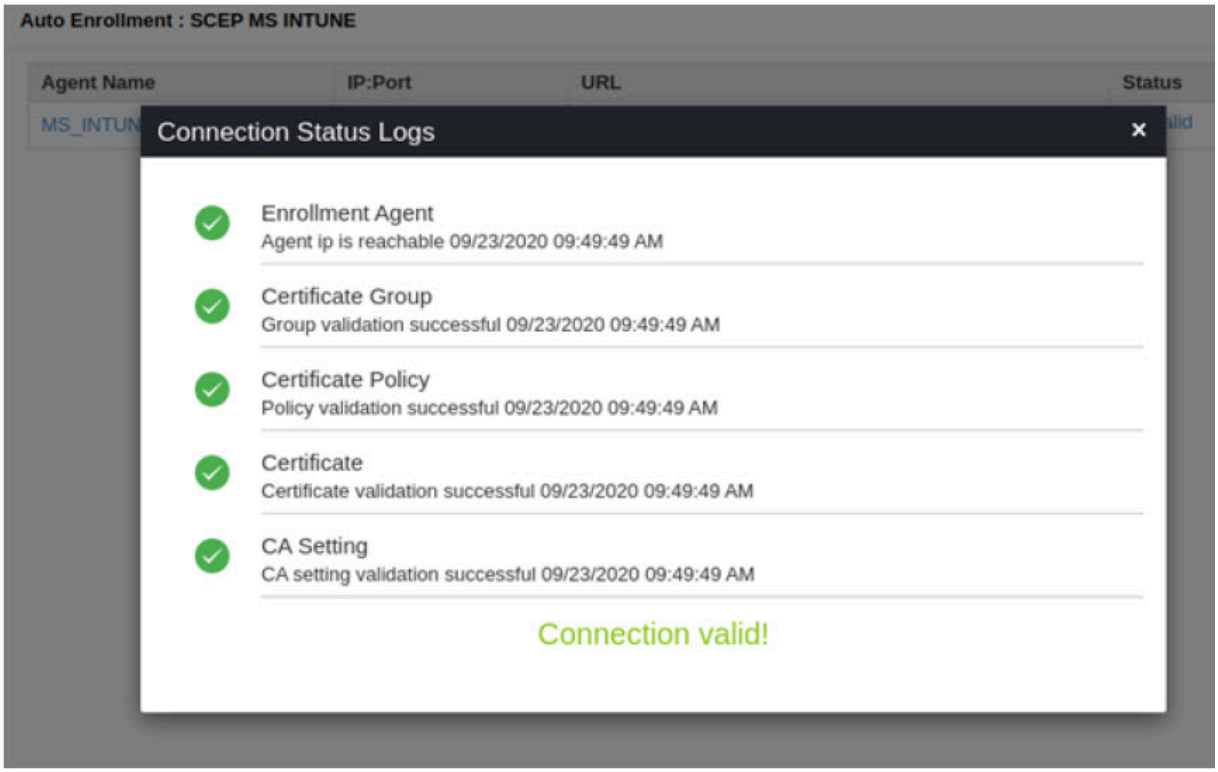
9. Click **Save.**

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

Before you Begin

SCEP is **Simple Certificate Enrollment Protocol**, which is a certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire certificates and associated CA certificates. Architecturally, the SCEP service(agent) is located between a CA and a client. AppViewX supports the Enrolment operation via the SCEP server in HTTP mode.

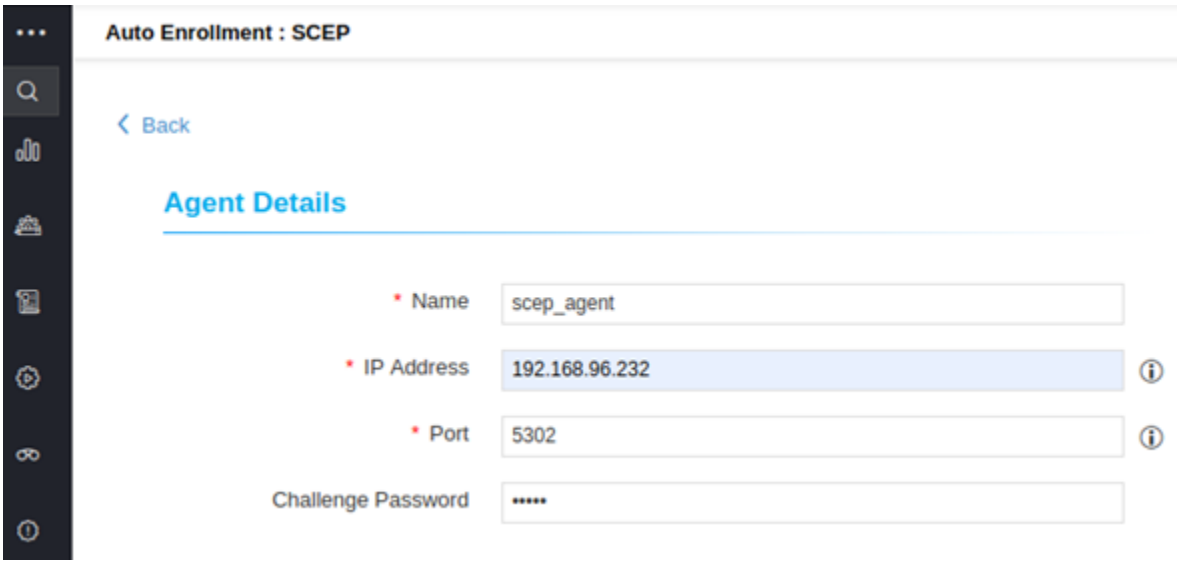
- There should be an agent(avx_vendor_cert_scep_agent) up and running for SCEP in appviewx.
- This SCEP plugin can either be in HTTPS or HTTP, but it needs an HTTP gateway running in order to communicate with the client.
- In order to make that HTTP gateway up and running go to /home/appviewx/appviewx/avxgw/avxgw-profile.json. 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

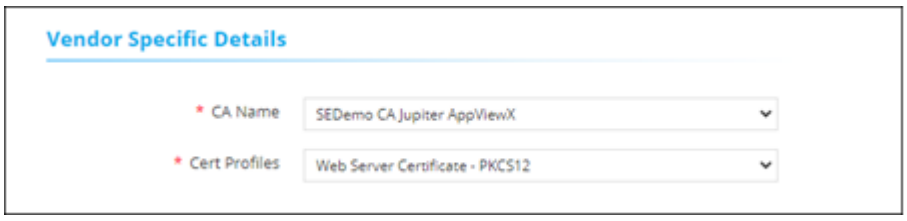
In order to perform enrolment, CA setting details and agent details needs to be configured to proceed with.

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 **CERT+** > **ADMINISTRATION** > **AutoEnrolment** > **SCEP.**
4. Select **Add** or **Configure Now.**
5. Configure the **Agent Details** details as follows:

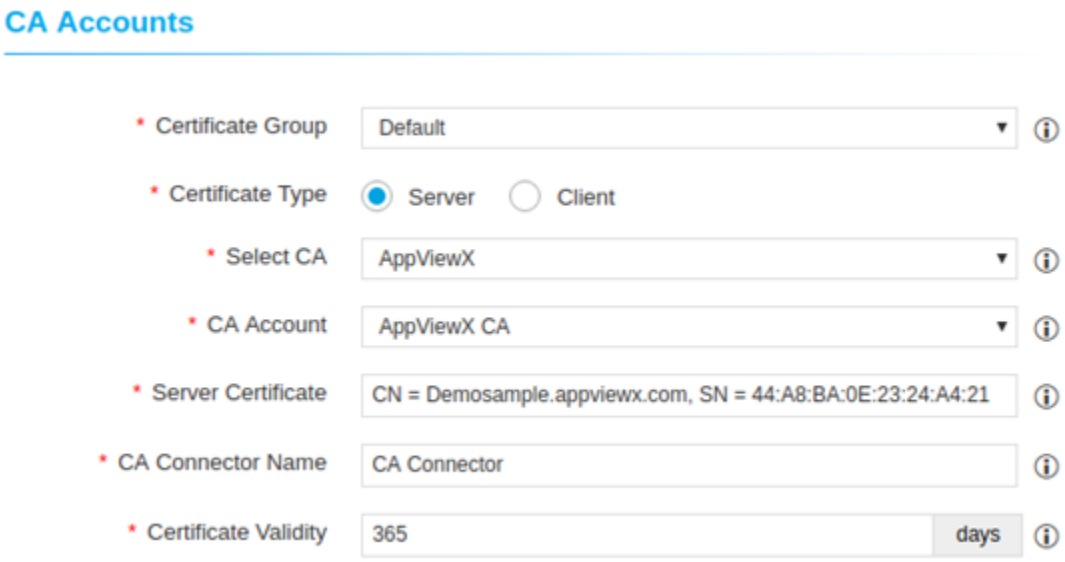
Name	Type	Mandatory	Description	Validation
Name	Text	Yes	A unique name to identify the agent setting.	No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
IP Address	Text	Yes	The IP address of the appviewx node.	Invalid IP address(example: xxx.xxx.xxx.xxx)
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:

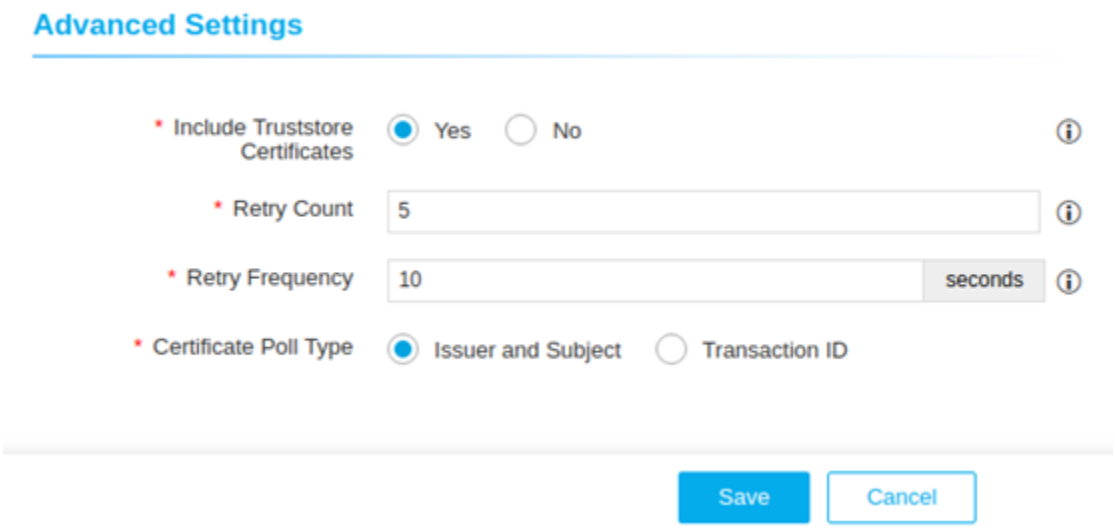
Name	Type	Mandatory	Description	Valida
Certificate Group	Select	Yes	Select a specific group under which certificate needs to be enrolled.	NA
Certificate Type	Select	Yes	Select a specific certificate type (Server / Client) to be enrolled.	NA
Select CA	Select	Yes	Select a specific CA from which the certificate needs to be enrolled. **Note:** If the selected CA is **Entrust MPKI**, a separate section displaying **Vendor Specific Details** is displayed after the **CA Accounts** section.  Under the **Vendor Specific Details** section: Select the required **CA Name** and the **Cert Profiles**.	NA

Name	Type	Mandatory	Description	Valida
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, one certificate can be selected for further communications with SCEP 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.	Certific validity accepts only numeri values



7. Configure the **Advanced Settings** details as follows:

Name	Type	Mandatory	Description	Validation
Include Truststore Certificates	Select	Yes	Select whether issuer certificate needs to be sent to client machines after enrolment.	NA
Retry Count	Text	Yes	Specify a retry count upto which the agent will retry for the certificate to be fetched.	NA
Retry Frequency	Text	Yes	Specify a retry frequency upto which the agent will wait for each retry count.	NA
Certificate Poll Type	Select	Yes	Select a specific type to poll the issued certificate from agent to subsystem certificate plugin.	NA



8. Click **Save.**

Validating SCEP

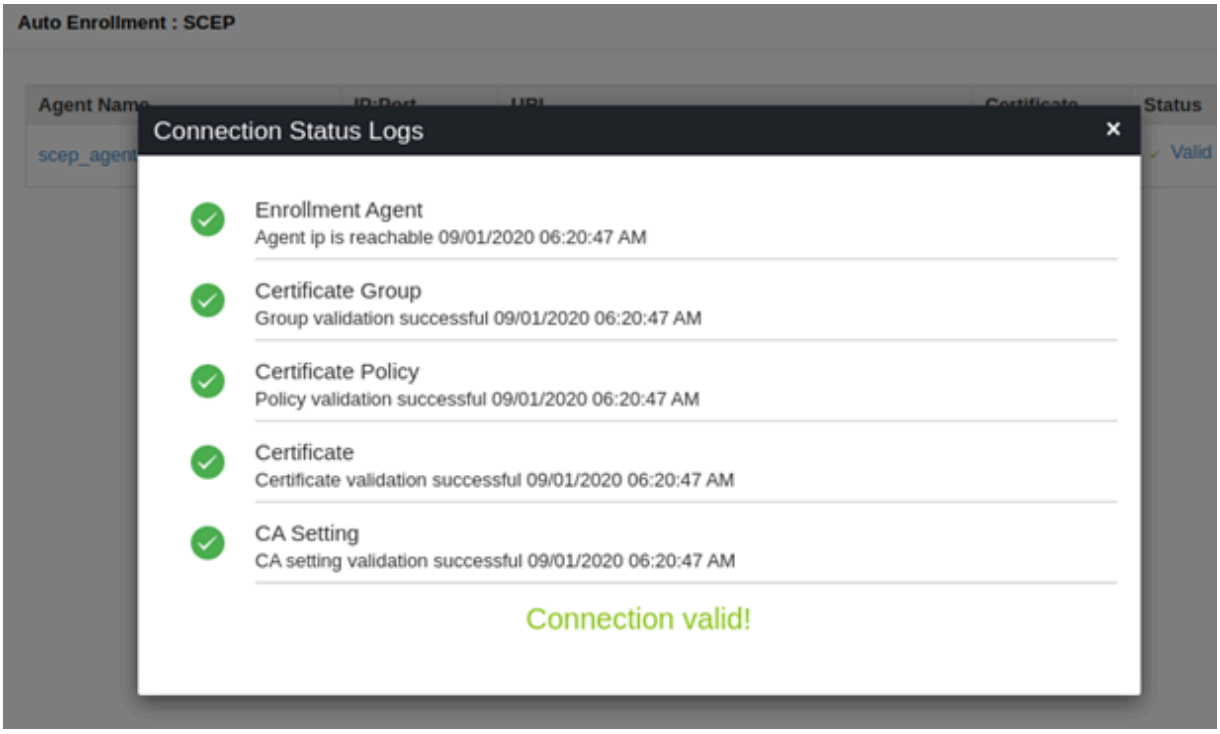
Once the SCEP settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** button.
3. Navigate to **CERT+ > ADMINISTRATION**.

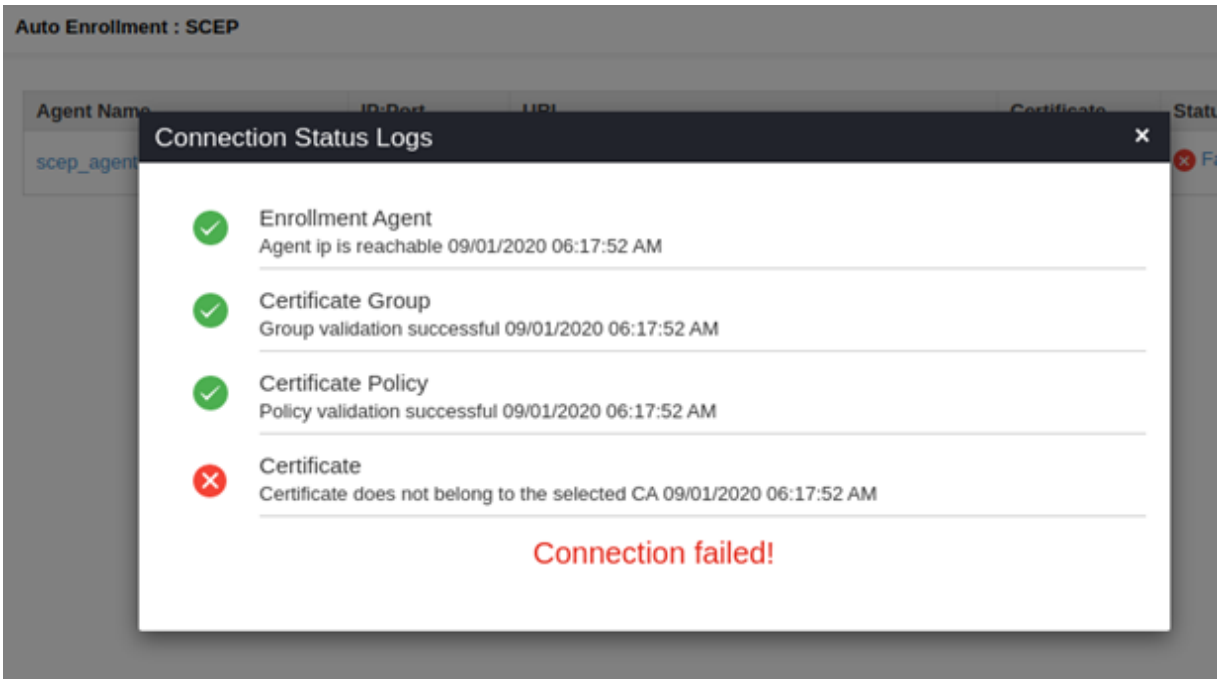
4. Under the **Administration** section, click **Auto-Enrollment** and then select **SCEP**.
5. On the **SCEP** page, click **Check** to validate the SCEP setting that has been created.

   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
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.