appviewx

CERT+ SaaS User Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

Trademarks

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
4.0	Updated version of document for release 2022.1.0 FP2	December 2022
3.0	Updated version of document for release 2022.1.0 FP2 Beta	November 2022
2.0	Updated version of document for release 2022.1.0 FP1	September 2022
1.0	Initial release of document for release 2022.1.0	June 2022

About this Guide

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

Audience

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

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: Getting Started

- About AppViewX
- Getting started with CERT+
- What's In It for you?
- Pre-requisites

About AppViewX

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

CERT+ Overview

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

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

Getting started with CERT+

AppViewX CERT+ CLM

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

Key Features of the CERT+:

- Certificate Discovery
- Inventory and Management
- Dashboard for Visibility and Monitoring
- Certificate Actions for Enrollment and Provisioning

- Alerts & Logs
- Groups & Policies
- Administration

Certificate Discovery

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

Inventory and Management

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

Dashboard for Visibility and Monitoring

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

Certificate Actions for Enrollment and Provisioning

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

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

Alerts & Logs

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

Groups & Policies

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

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

Administration

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

CLM Automation

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

What’s In It for you?

Overview

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

Discovery and Visibility

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

CLM Automation

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

Cloud and DevOps

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

Secure Key Management

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

Certificate and Key Compliance

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

IoT and Enterprise Mobility Certificate Management

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

SSH Key Lifecycle Automation

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

Pre-requisites

Web Browser Requirement

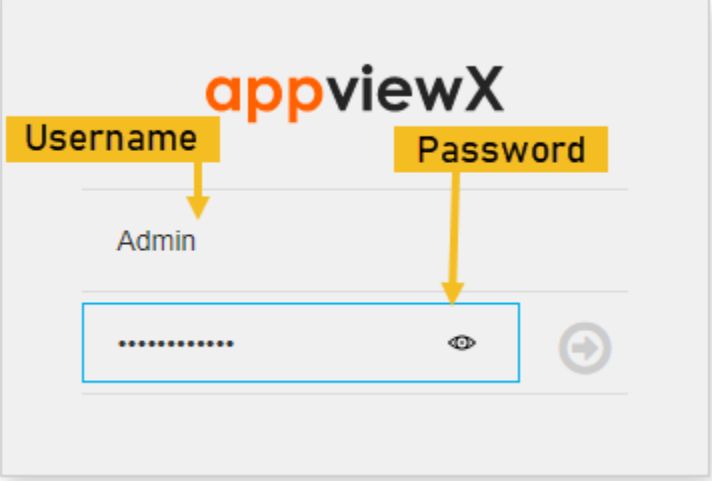
Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	v74.0.1 (64-bit) or later
Google Chrome	v85.0.4183.83 (64-bit) or later

Accessing the CERT+

Steps to access the CERT+,

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

   The AppViewX Landing page appears.



2. Click menu button located in the upper left corner of the screen.

3. Click **CERT+** on the left navigation bar.

CERT+ Home Page

The CERT+ home page contains necessary features for the certificate lifecycle management as shown on the image.

The following table describes the options available in the CERT+ home page:

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Menu button</td><td>Displays the left navigation pane of the AppViewX.</td></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: Onboard Certificates

Overview

A certificate is often distributed across load balancers, firewalls, web servers, containers, and multi-cloud environments and without proper visibility, a certificate-related outage becomes inevitable. During any certificate expiry or revocation event, the hardest part of mitigating an outage is not identifying the certificate, but it is often locating it on-time. With AppViewX, you can enhance the visibility and accuracy of your certificate infrastructure with minimal manual intervention.

Prechecks or Preconditions

- To discover certificates from managed Devices, the device must be managed under the AppViewX Device Inventory.
- To discover certificates from a CA, the CA account should be determined under the AppViewX Certificate Authority settings. Network Access to be considered

AppViewX discovery agent role and usage

Refer to Roles section in the CERT+ admin guide

Certificate Discovery

Overview

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

Discovery

- Network Scan
- Scan Subnet
- Scan Range of IP Addresses
- Scan URL
- Managed Device Scan
- Certificate Authority Scan
- Cloud Scan
- Scanning Uploaded Certificates

Network Scan

You can perform an unauthenticated discovery when there are no servers or applications onboarded into AppViewX, but certificates hosted in your network. This form of discovery does not require credentials and you can run the discovery through network scans. This allows you to discover hosted certificates in your organization and its source (IP and Port).

Scan Subnet

Based on user inputs for a subnet, CERT+ performs an SSL handshake with IP addresses across the subnet to retrieve certificates. By default, standard ports are scanned. If required, you can scan any other specific port or perform an All Port Scan.

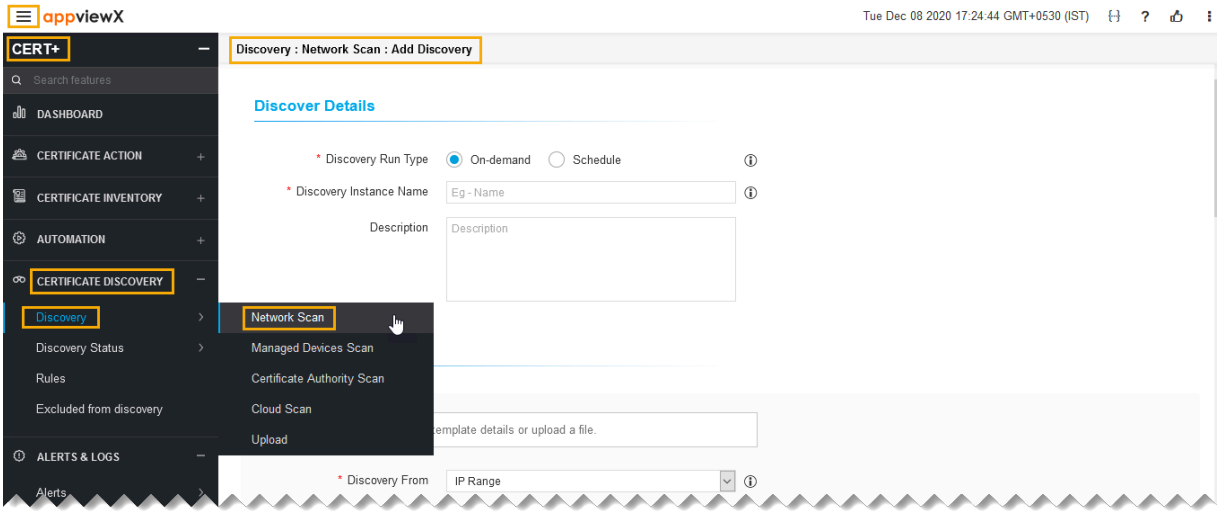
To discover a certificate via subnet,

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+**.

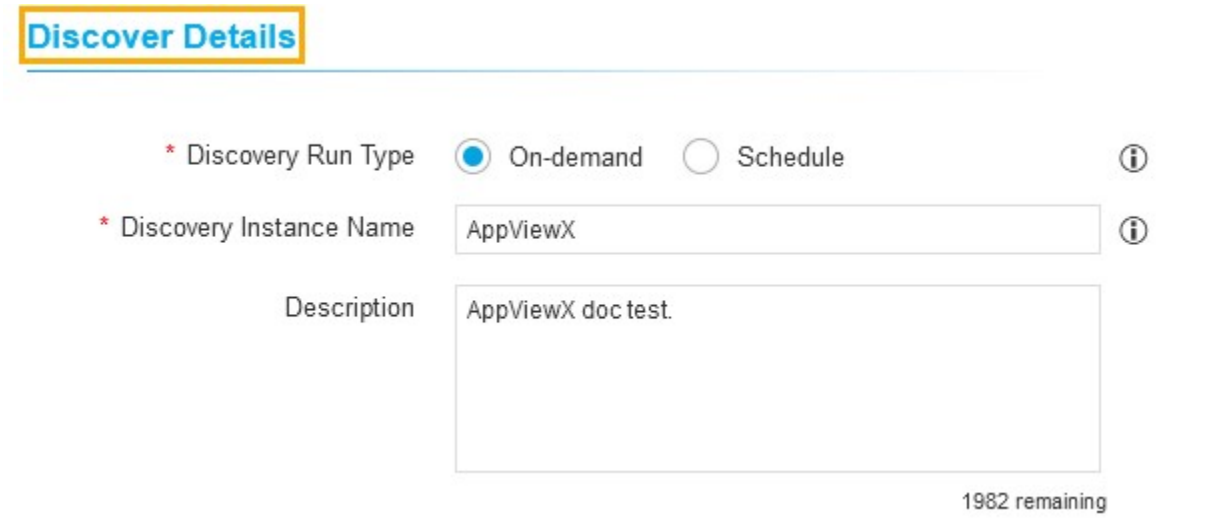
The **CERT+** left navigation pane appears.

4. Expand **CERTIFICATE DISVOERY**.
5. Click **Discovery**, and then select **Network Scan**.

   The **Add Discovery** page appears.

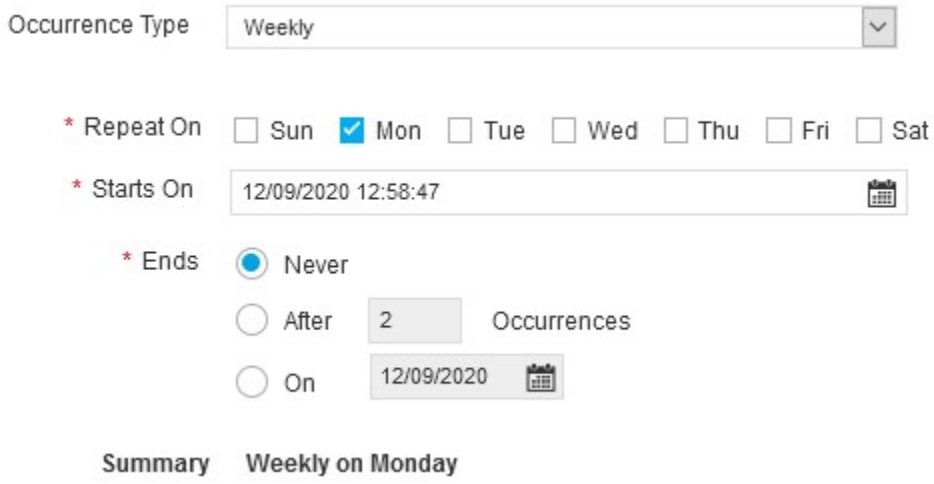


6. In the **Discover Details** section, select/enter the details as follows.



The following table describes the options available in the **Discover Details** section:

Field	Description
*Discovery Run Type	Click the check box to select the desired discovery run type. The possible types are:

Field	Description
	• **On-demand** - The user can trigger a discovery manually whenever he/she wants. • **Schedule** - By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details. 

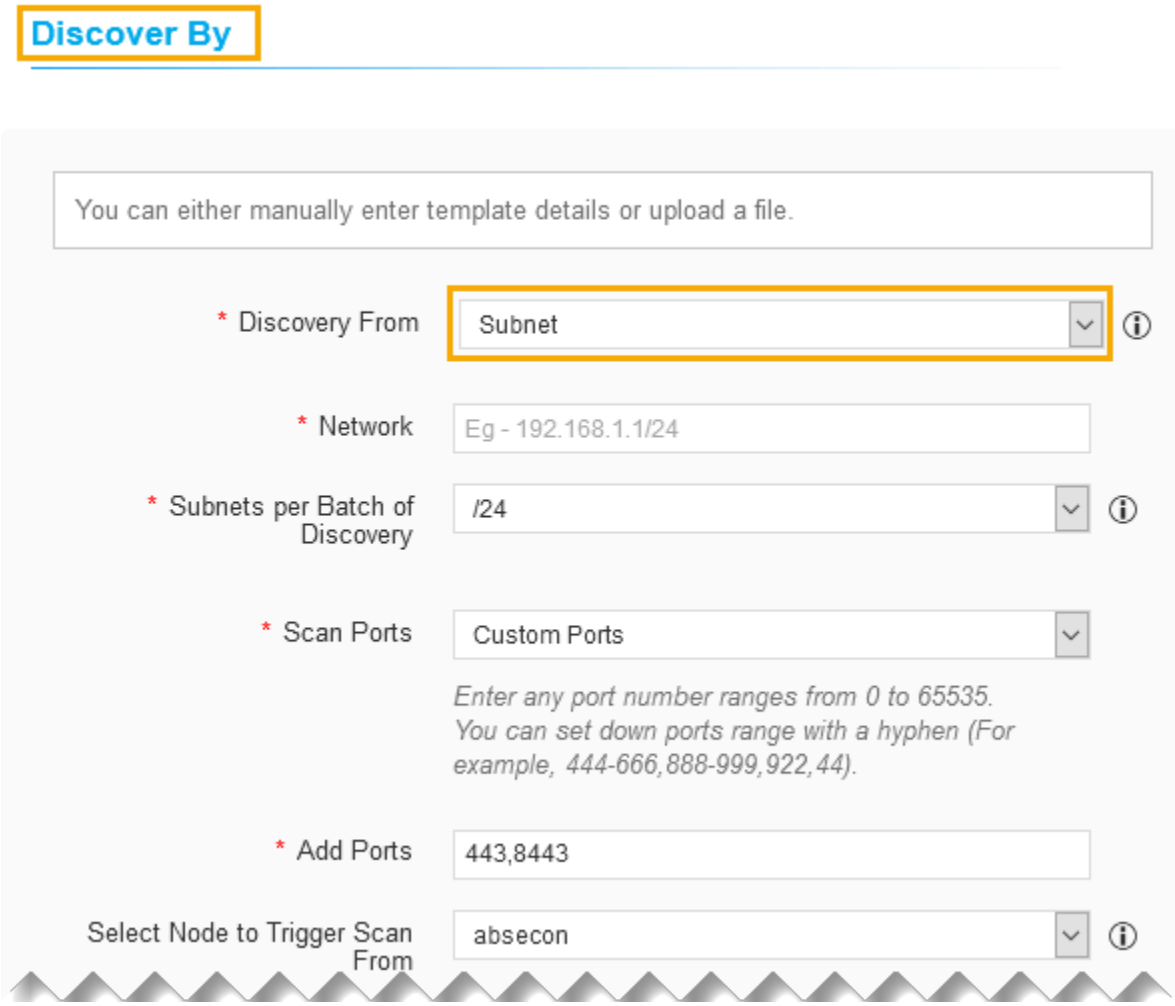
Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
***Repeat On**	Select a day in the week to schedule the weekly discovery.
***Starts On**	Select the date to start the scheduled discovery.
***Ends**	Select the desired last discovery.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>• Never - Continues to discover the certificate.
• After - Stops the discovery process after a number of occurrences entered in the field.
• On - Stops the discovery process for the selected period from the calendar.</td></tr>
</table>

Note: AppViewX will trigger the discovery certificates process for that instance.
</td></tr>
<tr><td>Discovery Instance Name</td><td>Enter the name of the discovery instance.</td></tr>
<tr><td>Description</td><td>Enter the required details in this field.

Note: You can enter a maximum of 2000 words in the field.</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

7. In the **Discover By** section, select/enter the details as follows.



The following table describes the options available in the **Discover By** section:

Field	Description
***Discover From**	Select the Subnet to discover a certificate from the dropdown list. The possible options are: • IP Range • Subnet • URL.
***Network**	Enter IP address. For example, 192.168.1.1/24
***Subnets per Batch of Discovery**	Select a value from the dropdown list to split the subnet into multiple batches for the discovery process. The possible values are:

Field	Description
	• /16 • /24 • /26 • /28 • /30 • /32.
***Scan Ports**	Select the desired scan ports from the dropdown list. The possible ports are: • All ports • Standard Ports • Custom Ports.
***Add Ports**	Enter any port number ranges from 0 to 65535. **Note:** You can set down port range with a hyphen (For example, 444-666,888-999,922,44).
Select Node to Trigger Scan From	Select the CLM node from where the discovery node is performed.
SNI Hostname(s)	Enter the hostnames in this field. **Note:** Multiple hostname values are supported by using the comma (,) as a delimiter.
TLS version(s)	Select the desired TLS versions from the desired name. The possible versions are: • Select All • TLSv1.3 • TLSv1.2 • TLSv1.1 • SSLv3

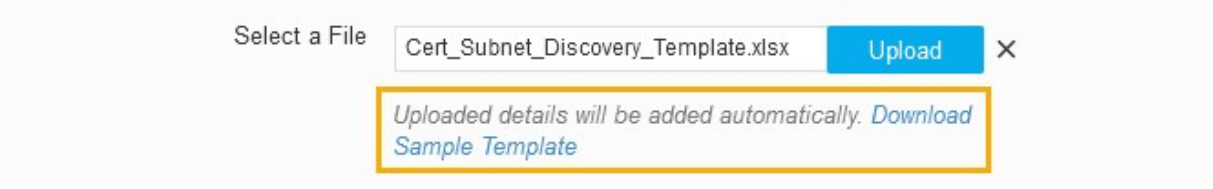
Field	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

8. Click **Add**.

   The popup message appears as **Network** details added.

9. (or) you can fill all the details for **Discover By** section by uploading network details via an excel sheet.

   To update network details via excel sheet.

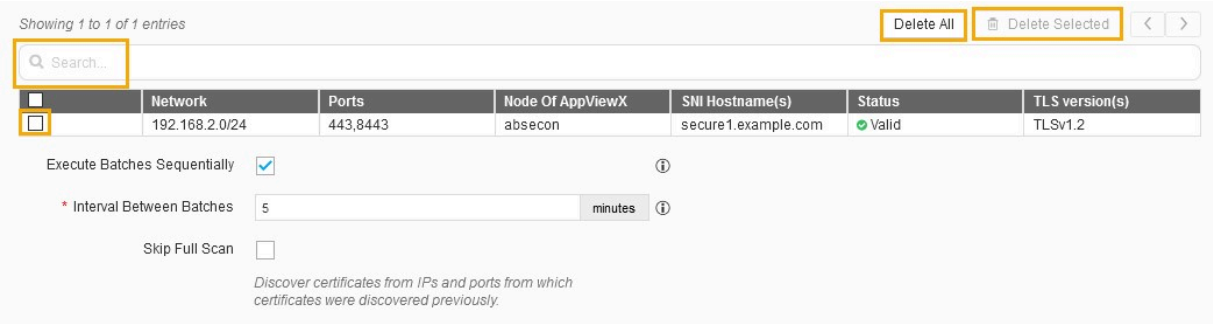


   a. Click the Download Sample Template link, to download a sample file.

   b. Fill all the necessary details in the excel sheet.

   c. Click the **Browse** button.

10. Added network details are listed.



   a. You use the search field to select the networks from the list.

   b. Use **Delete All**, if you want to delete all the network details.

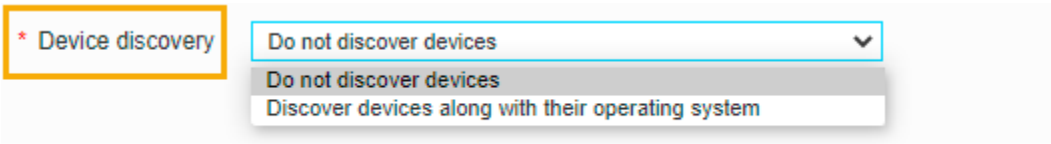
   c. Select desired check box, and then click Delete Selected to delete specific networks.

11. Select the **Execute Batches Sequentially** checkbox if required.

    a. (Recommended) If enabled, based on the value provided in Interval Between Batches field AppViewX will give the duration gap between each batch execution.

    b. If disabled, Scanning Intensity can be decided. An increase in scanning intensity will increase the scanning speed and network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.

12. Select the **Skip Full Scan** check box if required.



a. If enabled, certificates will be discovered from IPs and ports from which certificates were discovered previously.

13. In the **Device discovery** option, select the required discovery from the dropdown list.
    a. Do not discover devices - Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed.

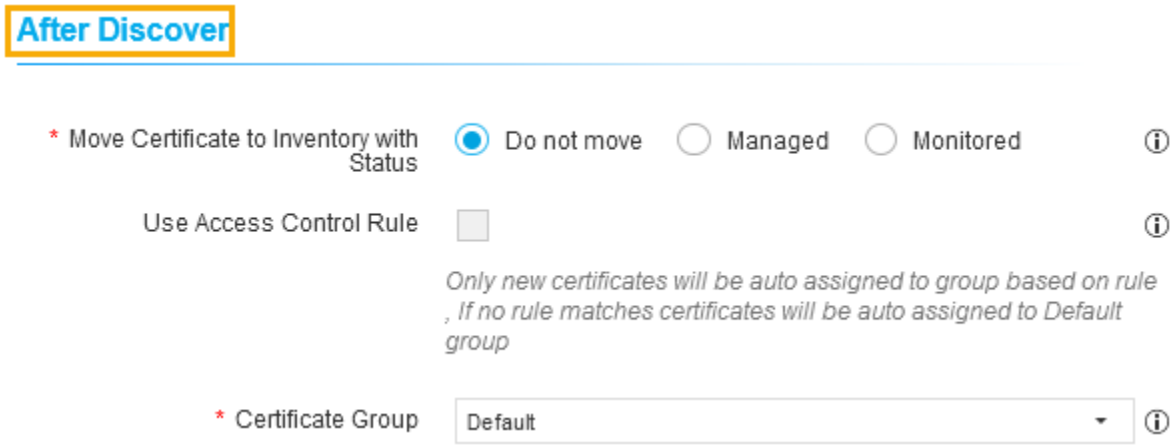
    b. **Note:** To discover the Operating System version, AppViewX requires Sudo access.

    Discover devices along with their operating systems - AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed.

14. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

    In the **Discovery Rules** section, select the Associate Rule from the dropdown list.

15. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the **After Discover** section.

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are: • Do not move - Newly discovered certificates and associated objects will not be moved to inventory. • Managed - New discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - New discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.
Note: The asterisk (*) symbol indicates a mandatory field.	

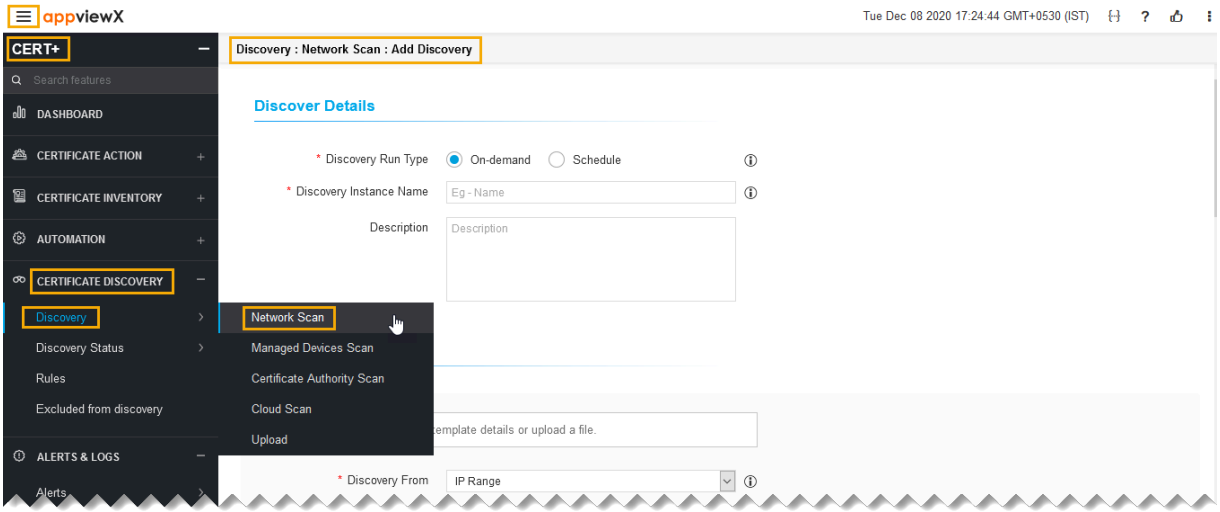
16. Click **Discover** or **Schedule** to perform an On-Demand (or) Schedule certificate discovery respectively.

Scan Range of IP Addresses

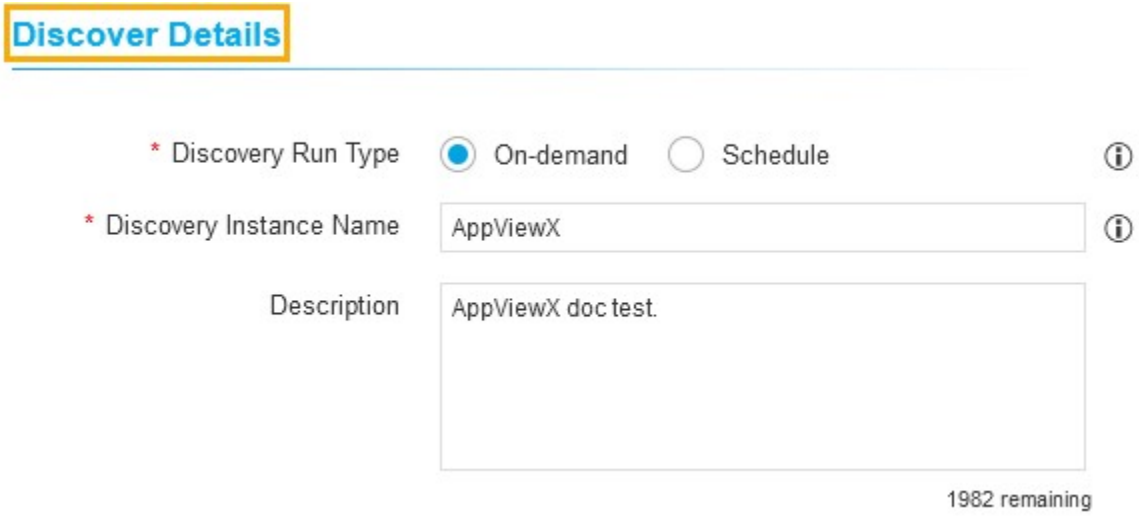
Based on user inputs for an IP range, CERT+ performs an SSL handshake with IP addresses in a range to retrieve certificates. By default, standard ports (443 and 8443) are scanned. If it is required, you can scan any other specific port or perform an All Port Scan.

To discover a certificate by IP range,

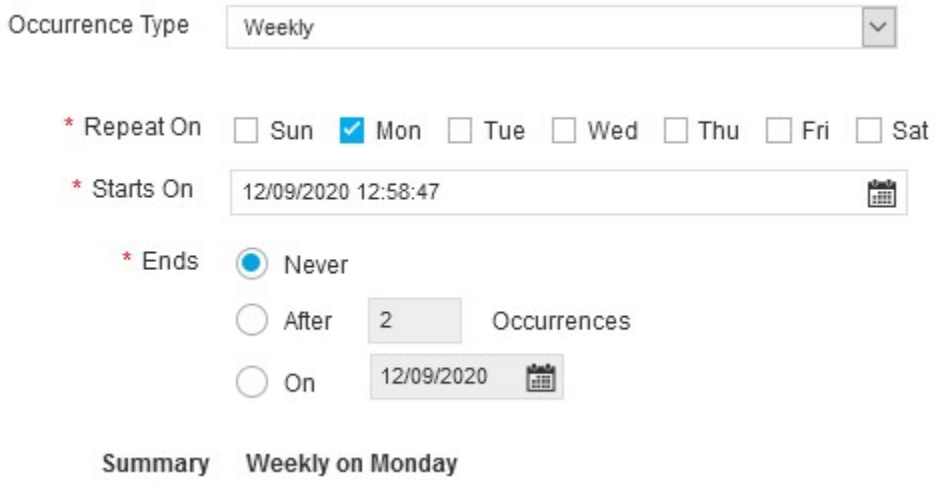
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE DISCOVERY**.
5. Click **Discovery**, and then select **Network Scan**.
   The **Add Discovery** page appears.



6. In the **Discover Details** section, select/enter the details as follows.



The following table describes the options available in the Discover Details section:

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. The possible types are: • **On-demand** - The user can trigger a discovery manually whenever he/she wants. • **Schedule** -By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details. 

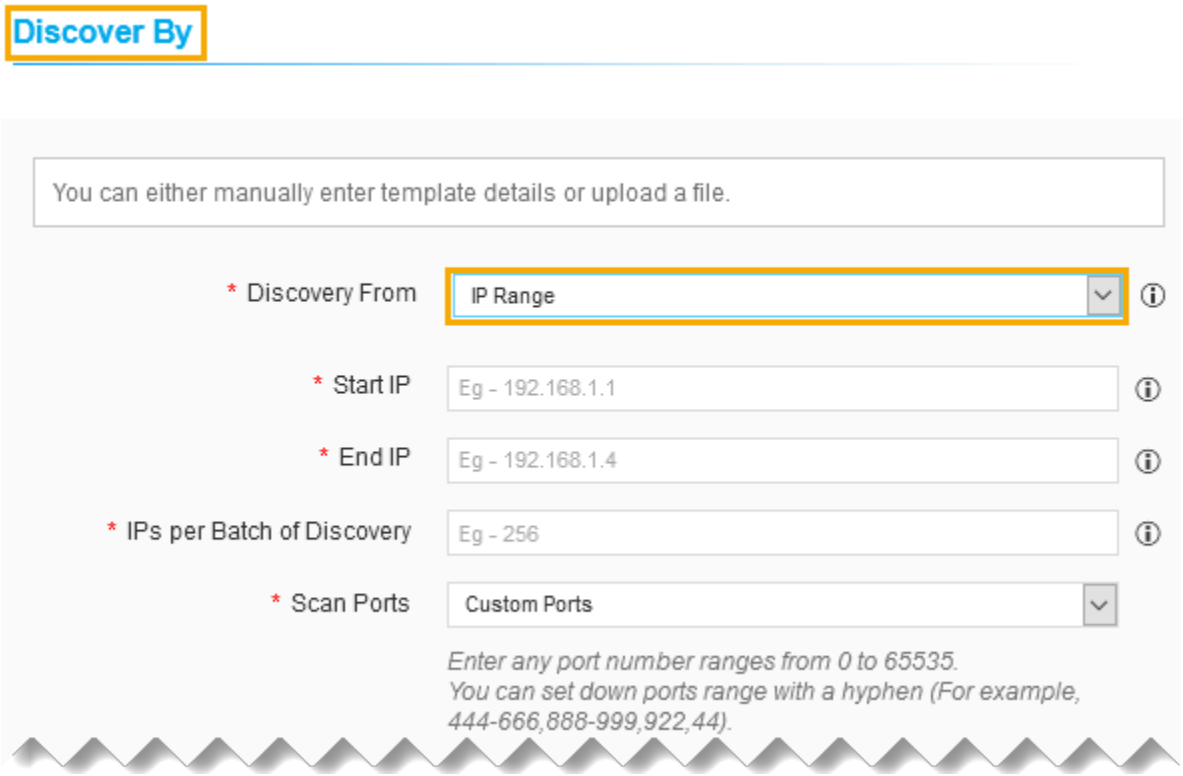
Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
***Repeat On**	Select a day in the week to schedule the weekly discovery.
***Starts On**	Select the date to start the scheduled discovery.
***Ends**	Select the desired last discovery.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>• Never - Continues to discover the certificate.
• After - Stops the discovery process after a number of occurrences entered in the field.
• On - Stops the discovery process for the selected period from the calendar.</td></tr>
</table>

Note: AppViewX will trigger the discovery certificates process for that instance.
</td></tr>
<tr><td>Discovery Instance Name</td><td>Enter the name of the discovery instance.</td></tr>
<tr><td>Description</td><td>Enter the required details in this field.

Note: You can enter a maximum of 2000 words in the field.</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

7. In the **Discover By** section, select/enter the details as follows.



The following table describes the options available in the Discover By section:

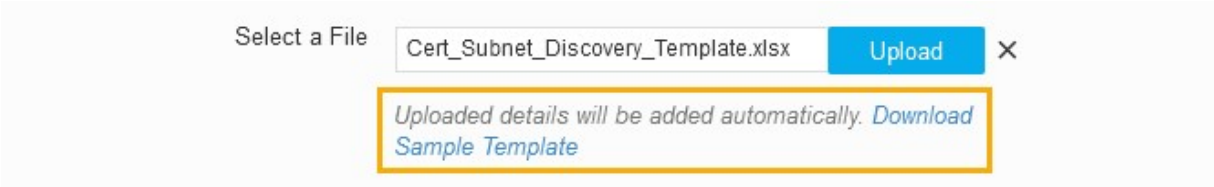
Field	Description
***Discovery From**	Select the IP Range to discover a certificate from the dropdown list. The possible options are: • IP Range • Subnet.
***Start IP**	Enter the start IP address. For example, 192.168.1.1
***End IP**	Enter the end IP address. For example, 192.168.1.4
***IPs per Batch of Discovery**	Enter the number of IP addresses that must be scanned in a batch. **Note:** • This can be used to throttle scan traffic. • Enter IP addresses that do not exceed more than 256. • /32.

Field	Description
***Scan Ports**	Select the desired scan ports from the dropdown list. The possible ports are: • All ports • Standard Ports • Custom Ports.
***Add Ports**	Enter any port number ranges from 0 to 65535. **Note:** You can set down port range with a hyphen (For example, 444-666,888-999,922,44).
Select Node to Trigger Scan From	Select the CLM node from where the discovery node is performed.
SNI Hostname(s)	Enter the hostnames in this field. **Note:** Multiple hostname values are supported by using the comma (,) as a delimiter.
TLS version(s)	Select the desired TLS versions from the desired name. The possible versions are: • Select All • TLSv1.3 • TLSv1.2 • TLSv1.1 • SSLv3.
Note: The asterisk (*) symbol indicates a mandatory field.	

8. Click **Add**.

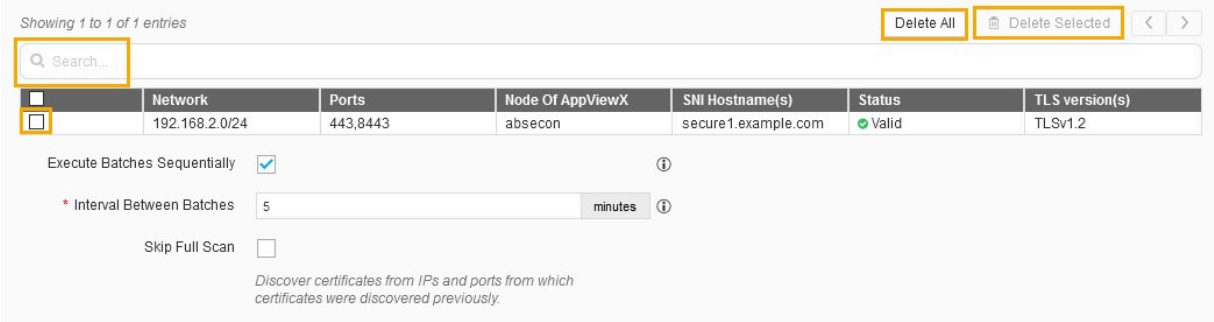
   The popup message appears as **Network details added**.

9. (or) you can fill all the details for Discover By section by uploading network details via an excel sheet. To update network details via excel sheet,

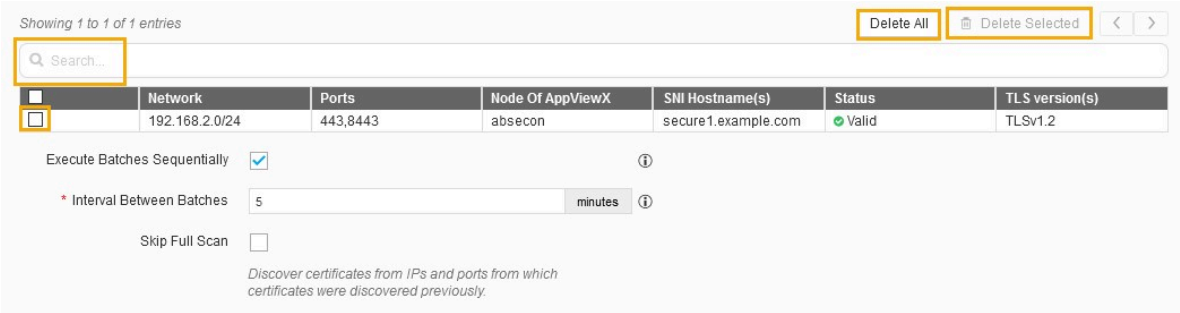


   a. Click the Download Sample Template link, to download a sample file.
   b. Fill all the necessary details in the excel sheet.
   c. Click the **Browse** button.

10. Added network details are listed.

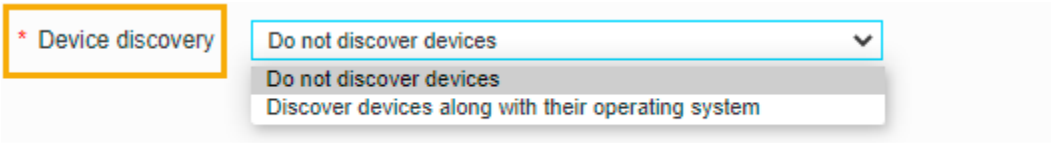


11. You use the search field to select the networks from the list.
   a. Use **Delete All**, if you want to delete all the network details.
   b. Select desired check box, and then click **Delete Selected** to delete specific networks.



12. Select the **Execute Batches Sequentially** checkbox if required.
   a. If enabled, Based on the minute's value provided in Interval Between Batches field AppViewX will give the duration gap between each batch execution.
   b. If disabled, Scanning Intensity can be decided. An increase in scanning intensity will increase the scanning speed and network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.

13. Select the **Skip Full Scan** check box if required. If enabled, Certificates will be discovered from IPs and ports from which certificates were discovered previously.
14. In the **Device discovery** option, select the required discovery from the dropdown list.



a. Do not discover devices - Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed.

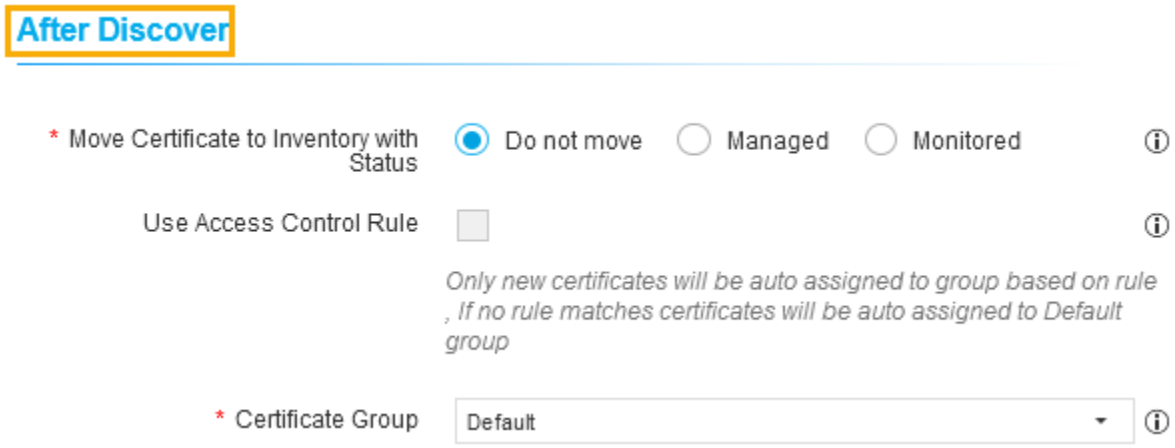
b. **Note:** To discover the Operating System version, AppViewX requires Sudo access.

Discover devices along with their operating systems - AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed.

15. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

In the **Discovery Rules** section, select the Associate Rule from the dropdown list.

16. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the After Discover section:

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are: • Do not move - New discovered certificates and associated objects will not be moved to inventory. • Managed - New discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - New discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.
Note: The asterisk (*) symbol indicates a mandatory field.	

17. Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Scan URL

The certificate public key is retrieved or stored during the handshake to the URL.

To discover a certificate via URL,

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.

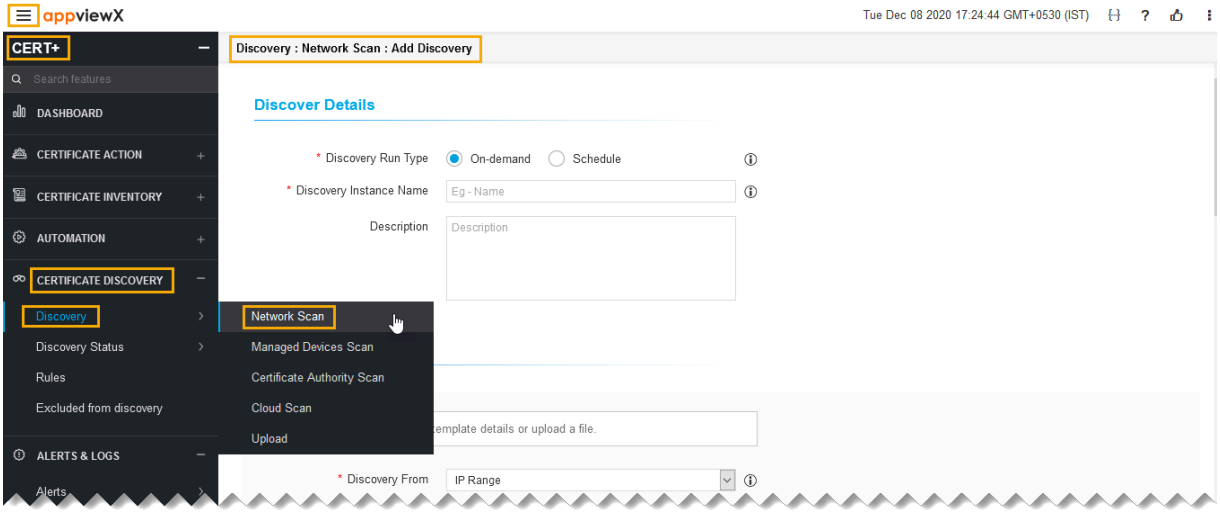
3. Click **CERT+**.

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

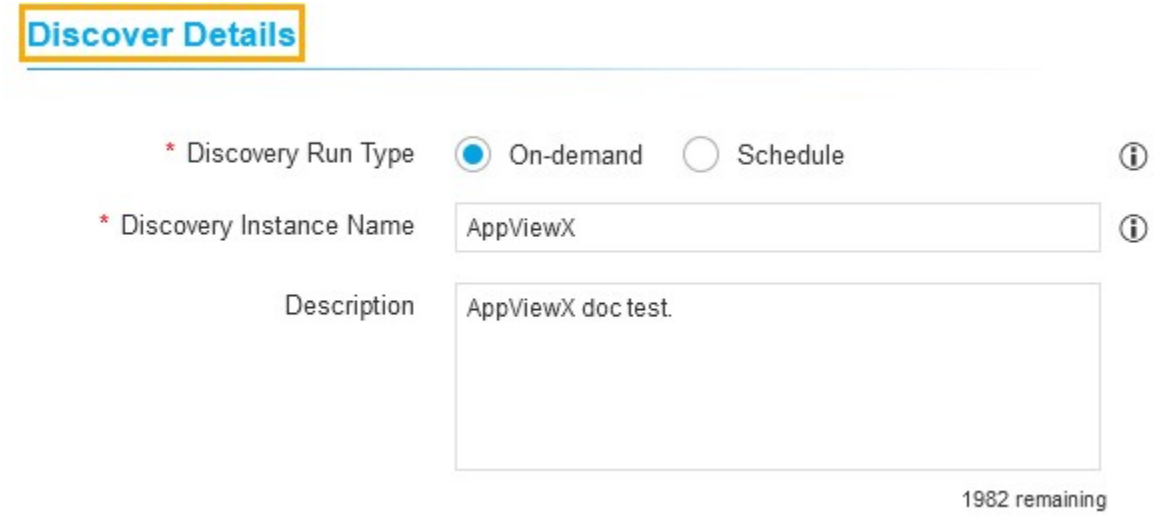
4. Expand **CERTIFICATE DISCOVERY**.

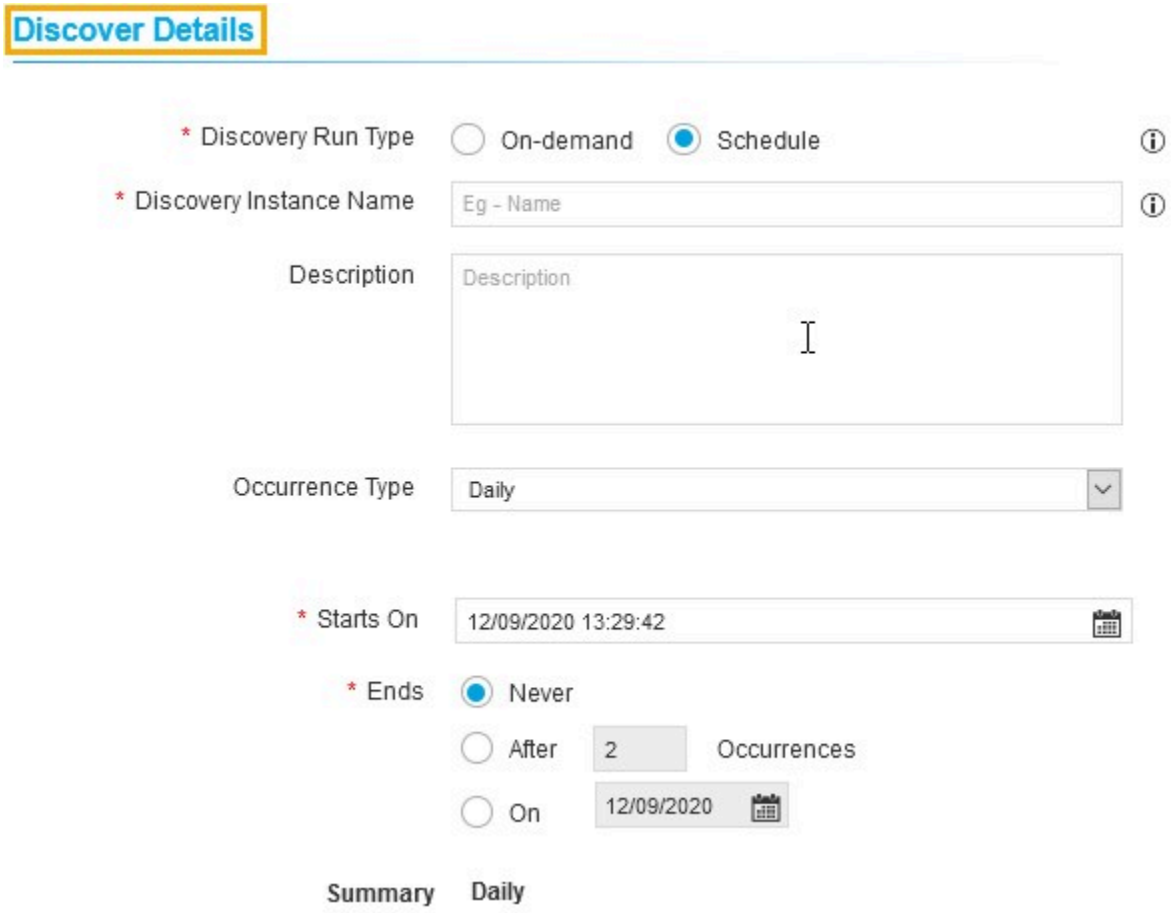
5. Click **Discovery**, and then select **Network Scan**.

   The **Add Discovery** page appears.



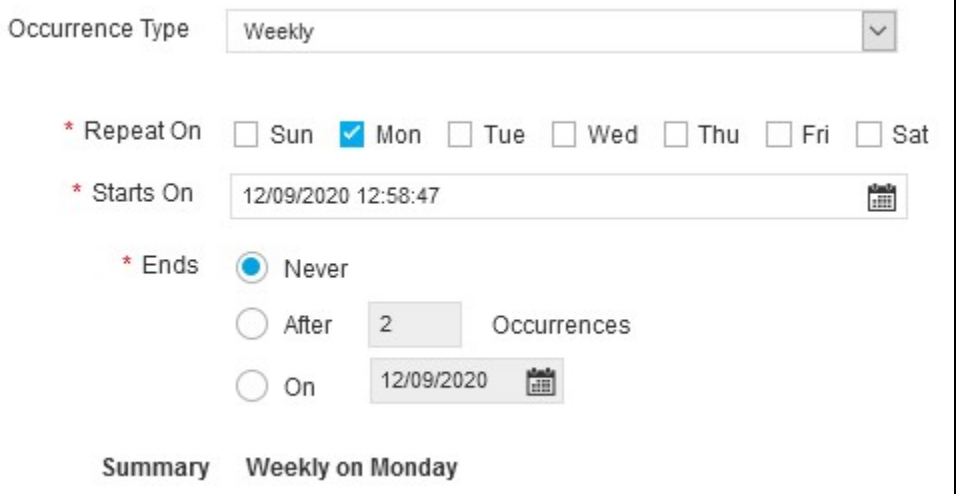
6. In the **Discover Details** section, select/enter the details as follows.





The following table describes the options available in the Discover Details section:

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. The possible types are: • **On-demand** - The user can trigger a discovery manually whenever he/she wants. • **Schedule** -By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details.

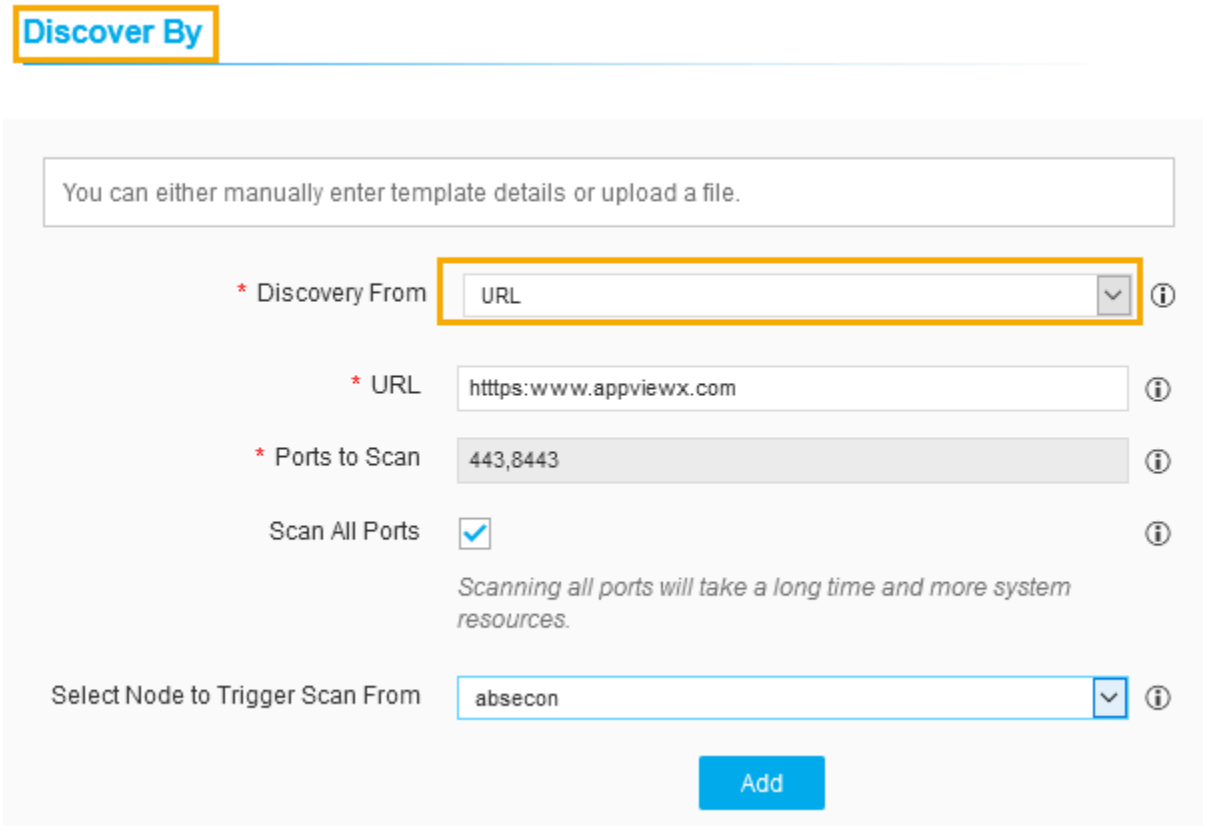
Field	Description
	

Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
***Repeat On**	Select a day in the week to schedule the weekly discovery.
***Starts On**	Select the date to start the scheduled discovery.
***Ends**	Select the desired last discovery. • Never - Continues to discover the certificate. • After - Stops the discovery process after a number of occurrences entered in the field. • On - Stops the discovery process for the selected period from the calendar.

Note: AppViewX will trigger the discovery certificates process for that instance.

Field	Description
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** You can enter a maximum of 2000 words in the field.
Note: The asterisk (*) symbol indicates a mandatory field.	

7. In the **Discover By** section, select/enter the details as follows.

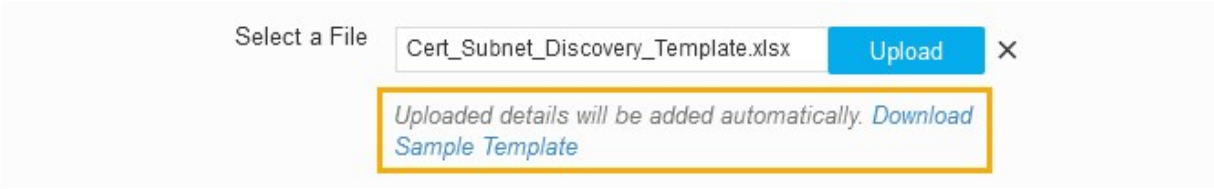


The following table describes the options available in the Discover By section:

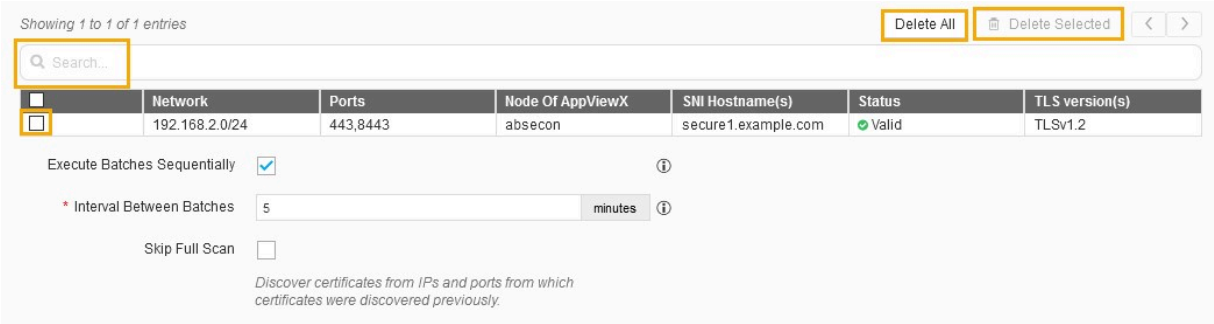
Field	Description
***Discovery From**	Select the IP Range to discover a certificate from the dropdown list. The possible options are: • IP Range • Subnet.
***Start IP**	Enter the start IP address. For example, 192.168.1.1
***End IP**	Enter the end IP address. For example, 192.168.1.4
***IPs per Batch of Discovery**	Enter the number of IP addresses that must be scanned in a batch. **Note:** • This can be used to throttle scan traffic. • Enter IP addresses that do not exceed more than 256. • /32.
***Scan Ports**	Select the desired scan ports from the dropdown list. The possible ports are: • All ports • Standard Ports • Custom Ports.
***Add Ports**	Enter any port number ranges from 0 to 65535. **Note:** You can set down port range with a hyphen (For example, 444-666,888-999,922,44).
Select Node to Trigger Scan From	Select the CLM node from where the discovery node is performed.
SNI Hostname(s)	Enter the hostnames in this field.

Field	Description
	Note: Multiple hostname values are supported by using the comma (,) as a delimiter.
TLS version(s)	Select the desired TLS versions from the desired name. The possible versions are: • Select All • TLSv1.3 • TLSv1.2 • TLSv1.1 • SSLv3.
Note: The asterisk (*) symbol indicates a mandatory field.	

8. Click **Add**.
   The popup message appears as **Network details added**.
9. (or) you can fill all the details for Discover By section by uploading network details via an excel sheet.
   To update network details via excel sheet,

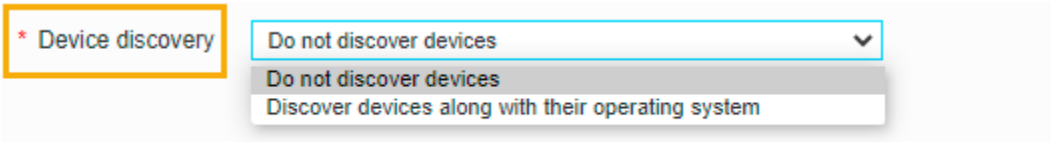


   a. Click the Download Sample Template link, to download a sample file.
   b. Fill all the necessary details in the excel sheet.
   c. Click the **Browse** button.
10. Added network details are listed.



11. You use the search field to select the networks from the list.
    a. Use **Delete All**, if you want to delete all the network details.
    b. Select desired check box, and then click **Delete Selected** to delete specific networks.

12. Select the **Execute Batches Sequentially** checkbox if required.
    a. If enabled, Based on the minute's value provided in Interval Between Batches field AppViewX will give the duration gap between each batch execution.
    b. If disabled, Scanning Intensity can be decided. An increase in scanning intensity will increase the scanning speed and network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
13. Select the **Skip Full Scan** check box if required. If enabled, Certificates will be discovered from IPs and ports from which certificates were discovered previously.
14. In the **Device discovery** option, select the required discovery from the dropdown list.



a. Do not discover devices - Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed.

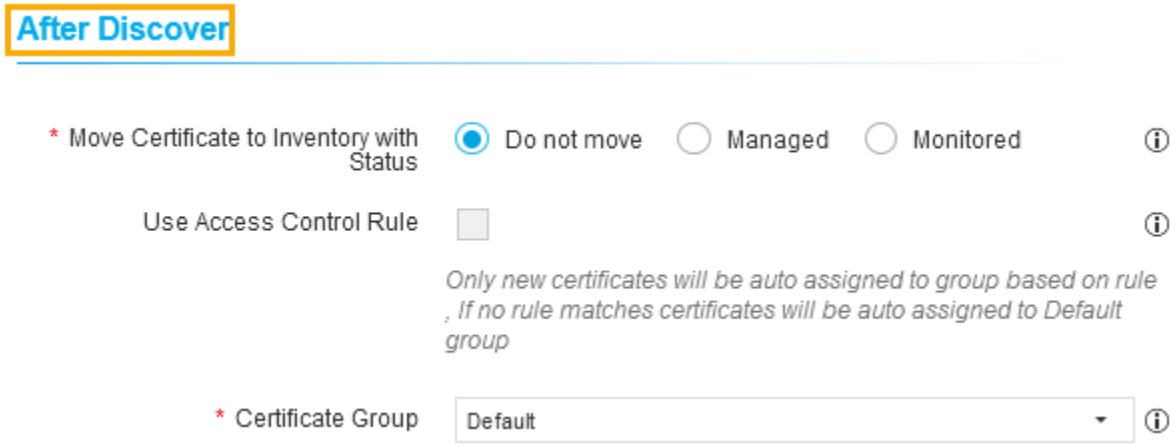
b. **Note:** To discover the Operating System version, AppViewX requires Sudo access.

Discover devices along with their operating systems - AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed.

15. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

In the **Discovery Rules** section, select the Associate Rule from the dropdown list.

16. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the After Discover section:

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are: • Do not move - New discovered certificates and associated objects will not be moved to inventory. • Managed - New discovered certificates and associated objects will be moved to inventory with status Managed.

Field	Description
	• Monitored - New discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.
Note: The asterisk (*) symbol indicates a mandatory field.	

17. Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Managed Device Scan

AppViewX can discover certificates from Managed Devices, this includes ADCs-Load balancers, Servers, Firewalls, WAFs. AppViewX can discover certificates from load balancers and provide in-depth information on certificates discovered from the SSL profile and the virtual server.

• Prerequisite

Prerequisite

To discover certificates from Managed devices, the device should be managed under the AppViewX Inventory. For onboarding devices into AppViewX inventory, refer to CERT+ Admin Guide.

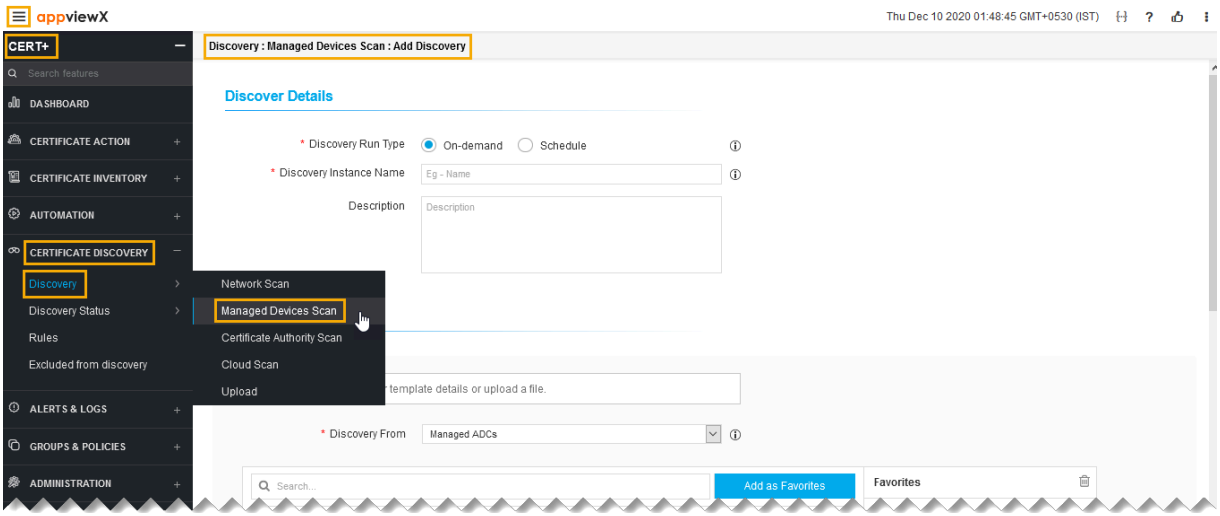
To discover certificates from Managed Devices,

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

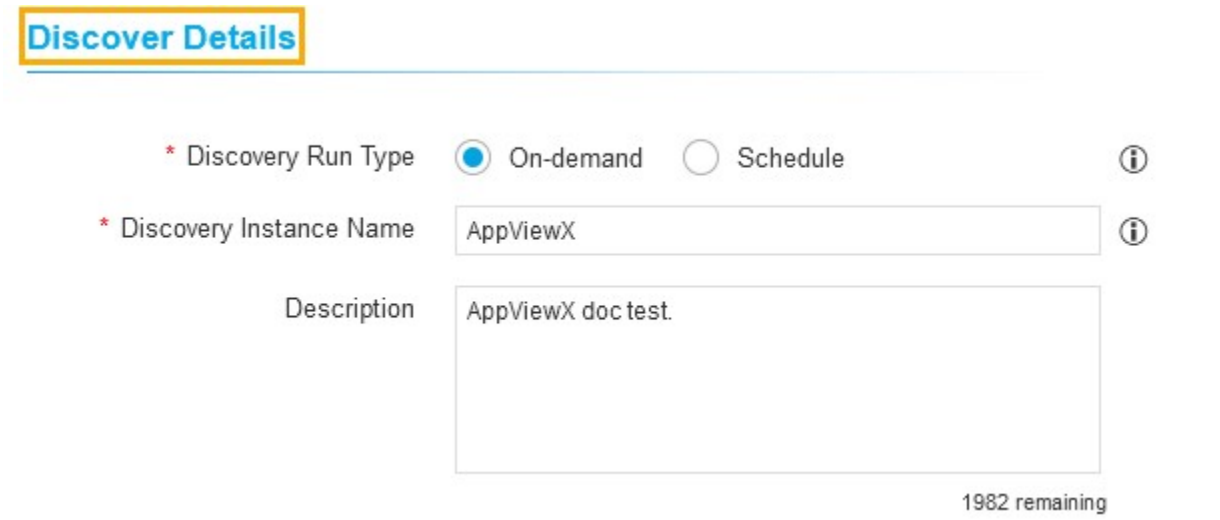
   The left navigation pane appears.
3. Click **CERT+**.

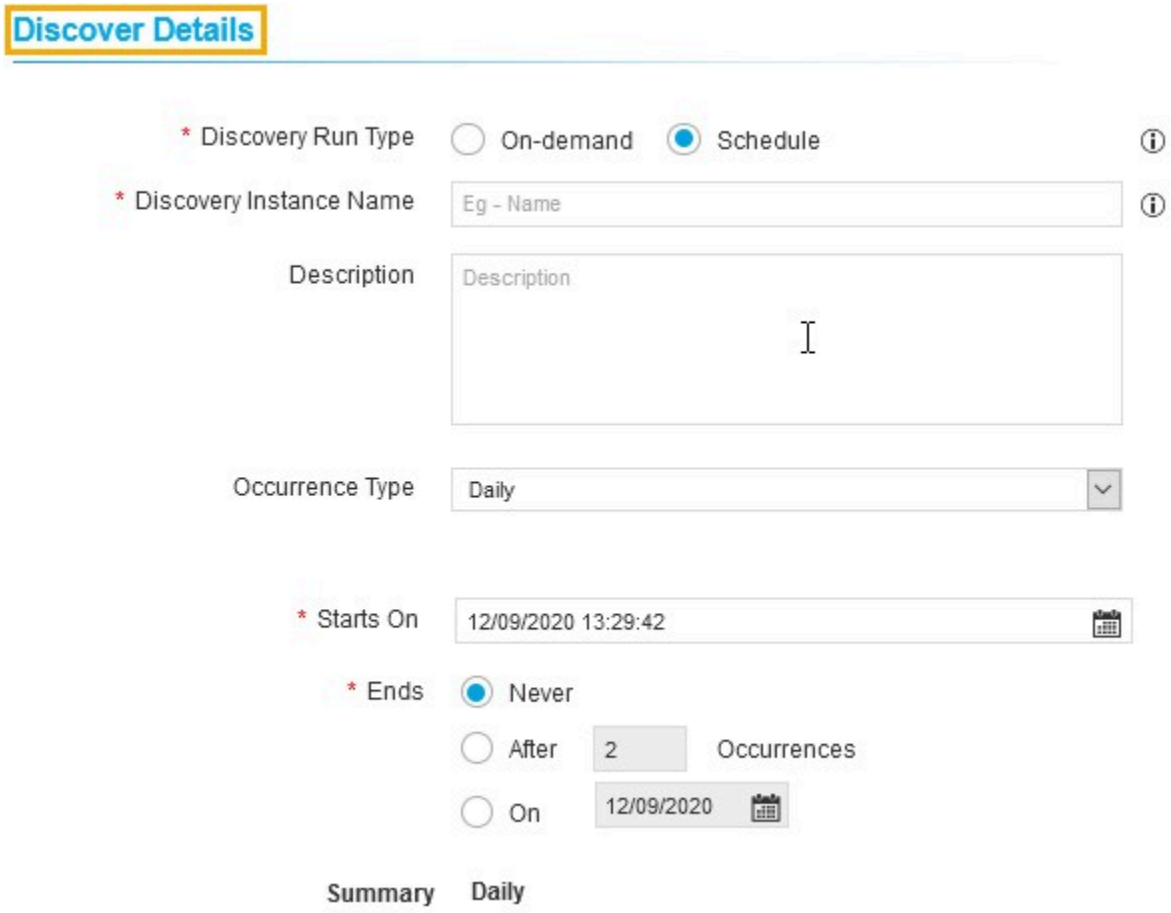
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Discovery**, and then select **Managed Devices** Scan.

   The **Add Discovery** page appears.



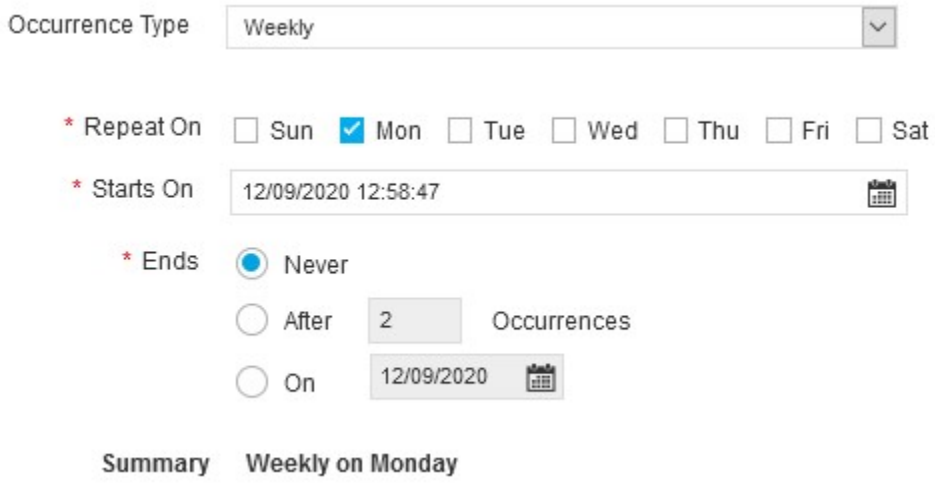
6. In the Discover Details section, select/enter the details as follows.





The following table describes the options available in the Discover Details section:

Field	Description
***Discovery Run Type**	Click the checkbox to select the desired discovery run type. The possible types are: • On-demand - If performing an On-Demand discovery. • Schedule - By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details.

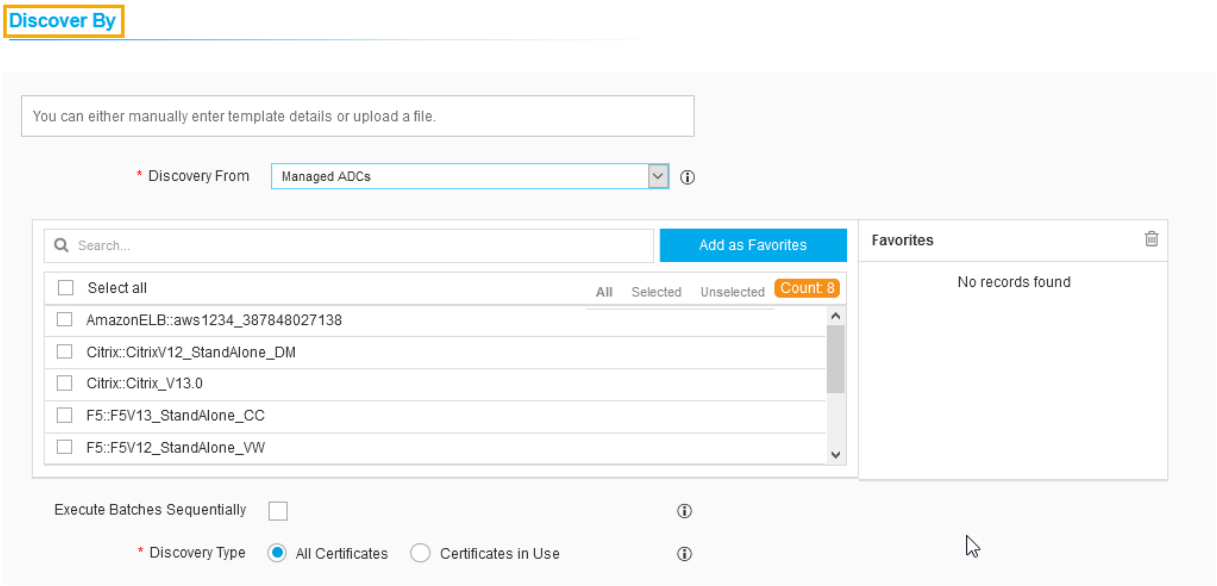
Field	Description
	

Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
*Repeat On	Select a day in the week to schedule the weekly discovery.
*Starts On	Select the date to start the scheduled discovery.
*Ends	Select the desired last discovery. • Never - Continues to discover the certificate. • After - Stops the discovery process after the number of occurrences entered in the field. • On - Stops the discovery process for the selected period from the calendar.

Note: AppViewX will trigger the discovery certificates process for that instance.

Field	Description
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** You can enter a maximum of 2000 words in the field.
Note: The asterisk (*) symbol indicates a mandatory field.	

7. In the **Discover By** section, select/enter the details as follows.



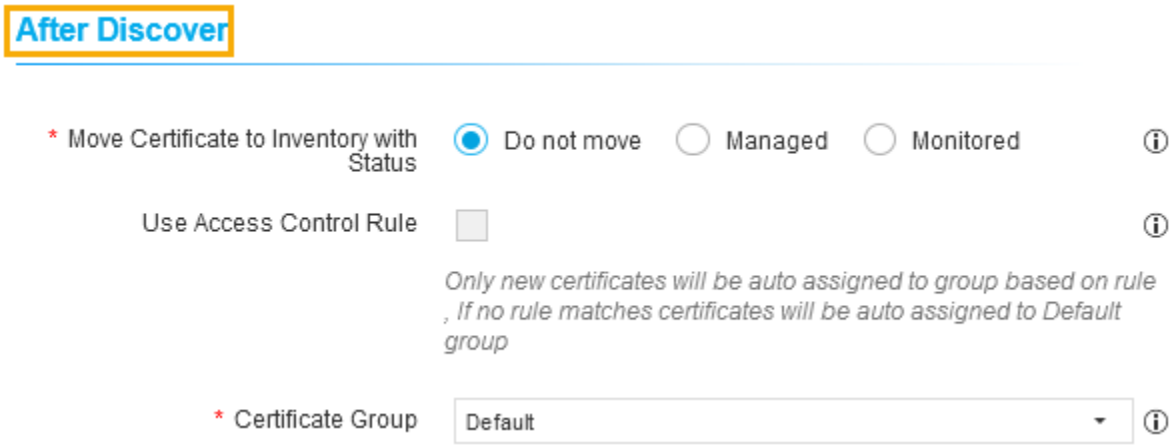
The following table describes the options available in the Discover By section:

Field	Description
***Discover From**	Select the source from the dropdown list to discover a certificate. The possible sources are: • Managed WAFs • Managed ADCs • Managed Servers

Field	Description
	• Managed MDMs • Managed Firewalls.
Devices Window	A list of all the managed devices will be shown in the devices window. Select devices to discover certificates from. • Add as Favorites - You search the desired device and add as favorites. • All - You can see all the devices from the list. • Select - You can see all the selected devices from the list. Unselect - You can see all the unselected devices from the list. • Delete - You can delete the favorite CAs from the list.
Note: The asterisk (*) symbol indicates a mandatory field.	

8. Select the Execute Batches Sequentially checkbox if required.
   a. If enabled, Based on the minutes value provided in **Interval Between Batches** field AppViewX will give the duration gap between each batch execution.
   b. If disabled, **Scanning Intensity** can be decided. An increase in scanning intensity will increase the scanning speed and network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
9. Click the check box to select the **Certificate Type**.
   a. **All Certificates**
   b. **Certificate in Use** - Certificates associated with a service that must be discovered
10. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

    In the **Discovery Rules** section, select the **Associate Rule** from the dropdown list.
11. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the After Discover section:

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are: • Do not move - Newly discovered certificates and associated objects will not be moved to inventory. • Managed - Newly discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - Newly discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.

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

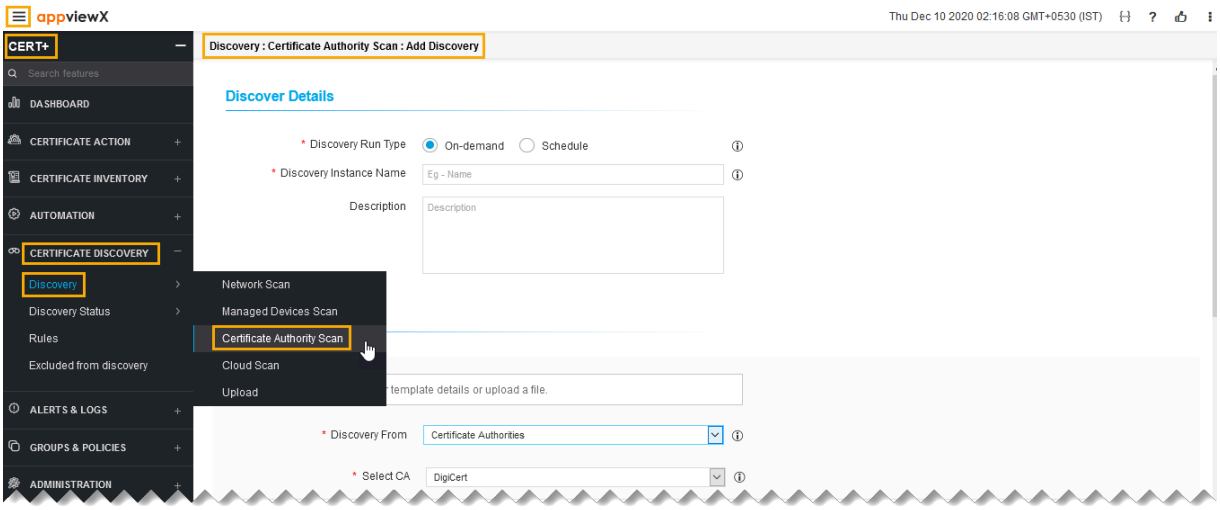
12. Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Certificate Authority Scan

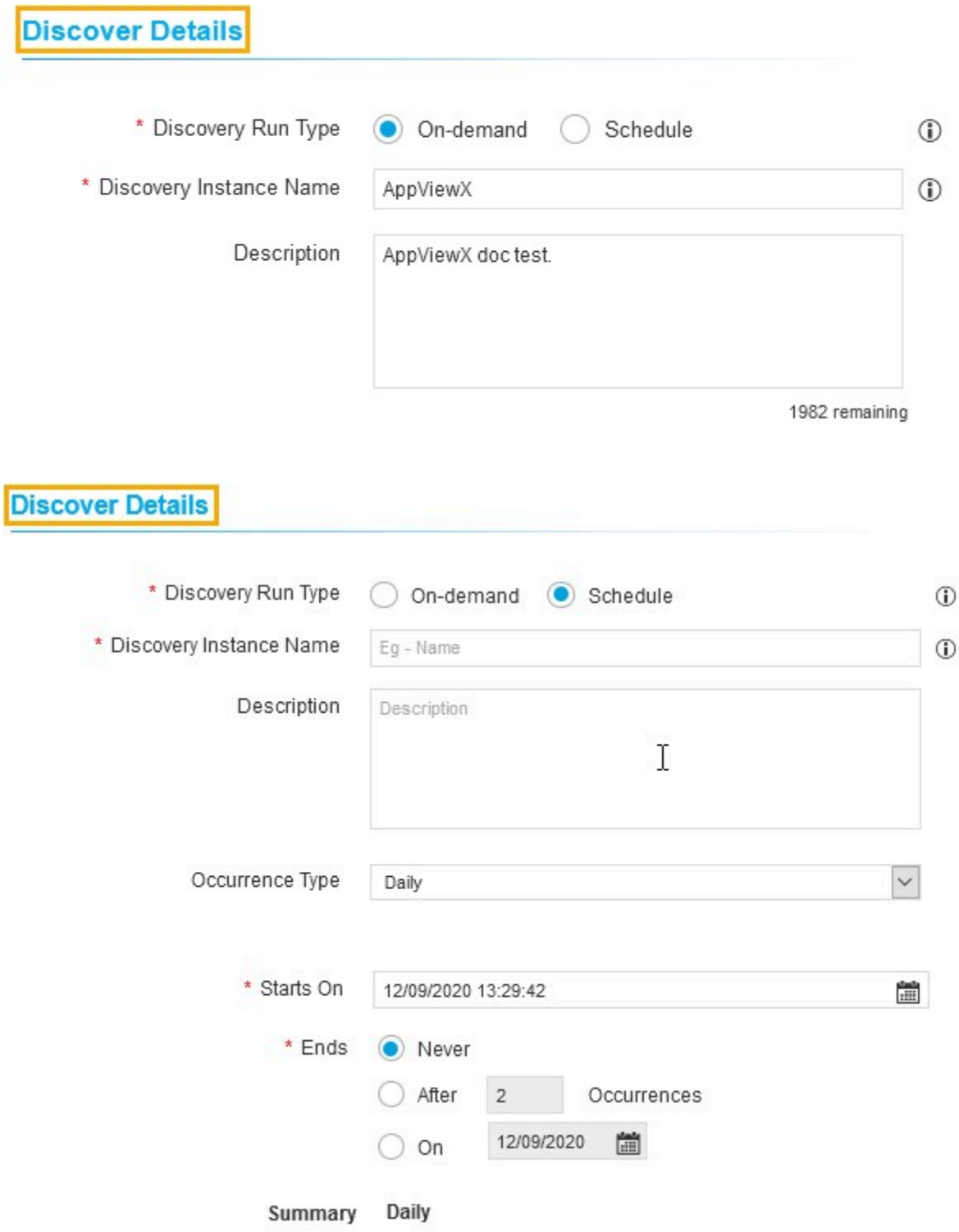
AppViewX can communicate with CA and scan certificates. To discover certificates from a CA, the CA account must be determined under the AppViewX Inventory settings.

To discover a certificate from CA,

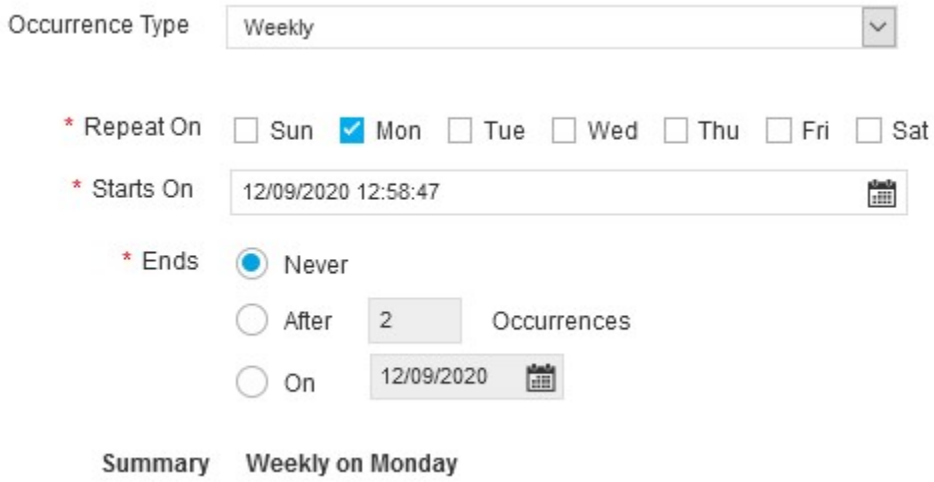
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE DISCOVERY**.
5. Click **Discovery**, and then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



6. In the **Discover Details** section, select/enter the details as follows.



The following table describes the options available in the **Discover Details** section:

Field	Description
***Discovery Run Type**	Click the checkbox to select the desired discovery run type. The possible types are: • On-demand - The user can trigger a discovery manually whenever he/she wants. • Schedule - By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details. 

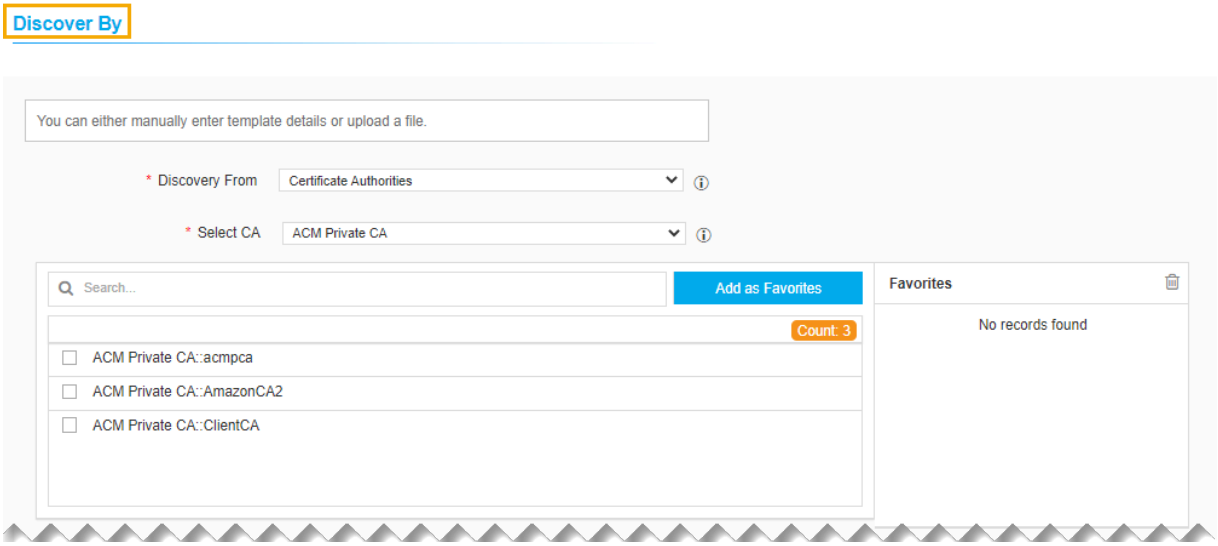
Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
***Repeat On**	Select a day in the week to schedule the weekly discovery.
***Starts On**	Select the date to start the scheduled discovery.
***Ends**	Select the desired last discovery.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>• Never - Continues to discover the certificate.
• After - Stops the discovery process after a number of occurrences entered in the field.
• On - Stops the discovery process for the selected period from the calendar.

Note: AppViewX will trigger the discovery certificates process for that instance.</td></tr>
</table>
</td></tr>
<tr><td>Discovery Instance Name</td><td>Enter the name of the discovery instance.</td></tr>
<tr><td>Description</td><td>Enter the required details in this field.

Note: You can enter a maximum of 2000 words in the field.</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

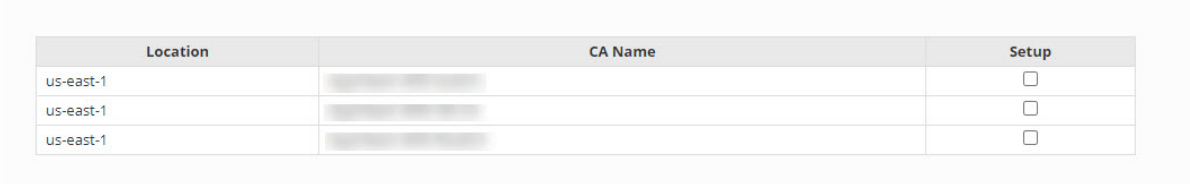
7. In the **Discover By** section, select/enter the details as follows.



Field	Description
***Discovery From**	Select the source from the dropdown list to discover a certificate.
***Select CA**	Select the CA from the dropdown list.
CA Window	List of all the managed CAs will be shown in the CA window. Select CAs to discover certificates from. • Add as Favorites - You search the desired CA and add as favorites. • All - You can see all the CAs from the list. • Select - You can see all the selected CAs from the list. • Unselect - You can see all the unselected CAs from the list. • Delete - You can delete the favorite CAs from the list.

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

When the **Amazon Private CA** is selected from the **Select CA** dropdown list and a managed private CA account is selected from the CA Window, the issuer details for the selected account are displayed below the **CA Window**, as shown in the image below:



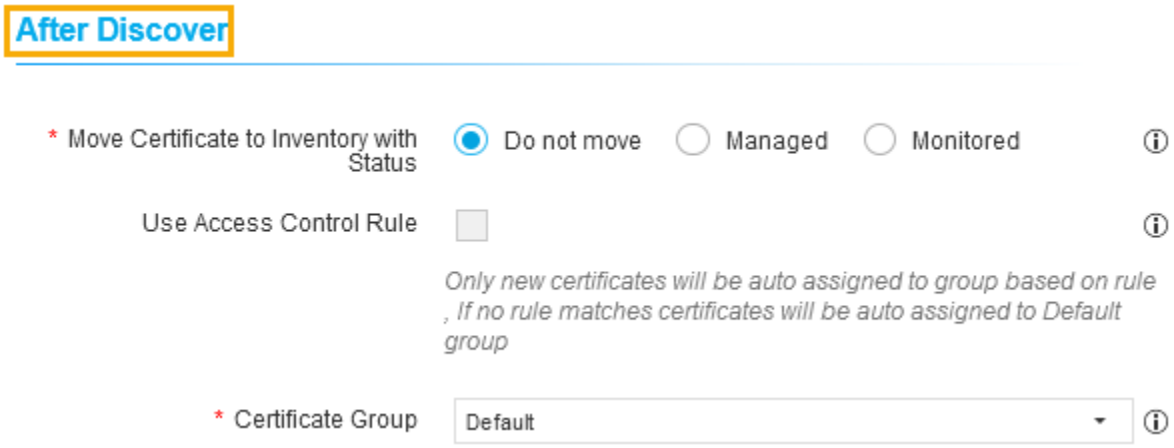
Note: All details of the private CA account, including the S3 bucket associated with the account, are fetched from the request for adding the Private CA account. [Explained in the CERT+ SaaS Admin Guide.]

8. To select the required issuer(s) for the selected Private CA account to perform the certificate authority scan, from the **Setup** column, select the checkbox corresponding to the issuer(s).

9. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

   In the **Discovery Rules** section, select the **Associate Rule** from the dropdown list.

10. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the After Discover section:

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are: • Do not move - Newly discovered certificates and associated objects will not be moved to inventory. • Managed - Newly discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - Newly discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box.

Field	Description
	Note: If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.
Note: The asterisk (*) symbol indicates a mandatory field.	

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

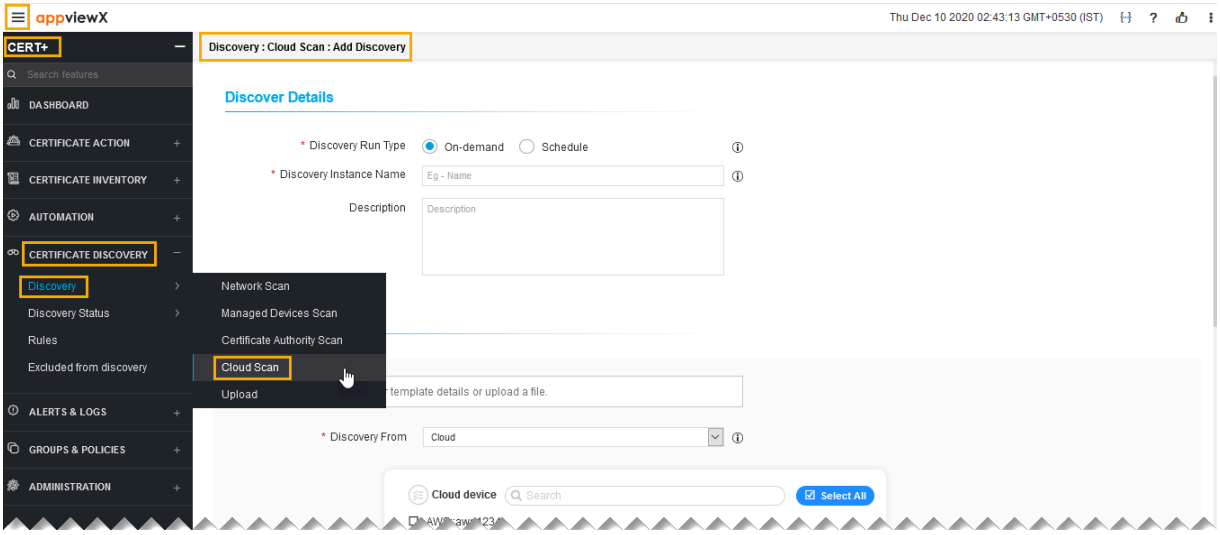
    Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Cloud Scan

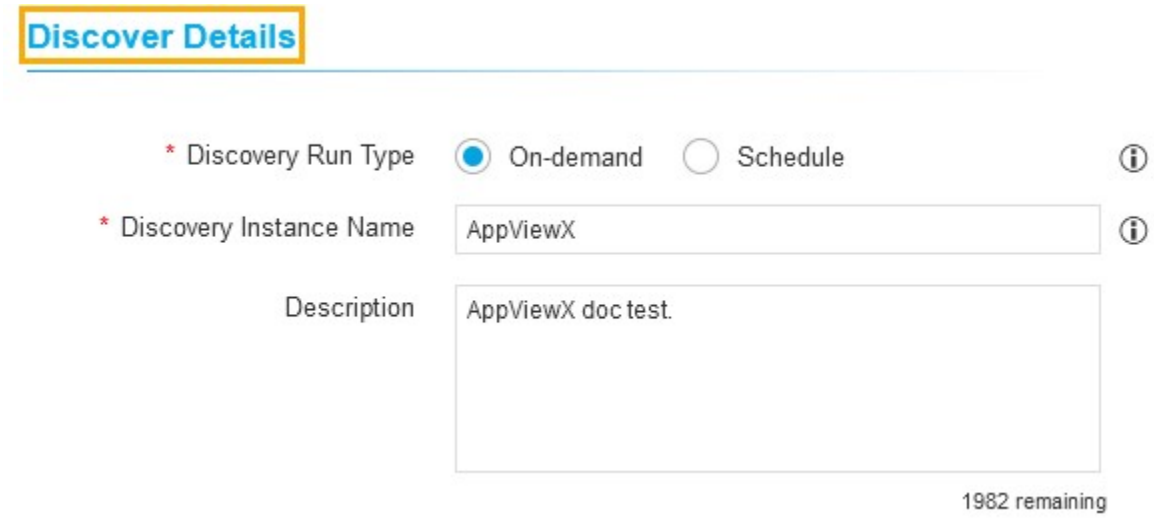
To discover certificates from a cloud, the cloud account must be determined under the AppViewX Inventory settings.

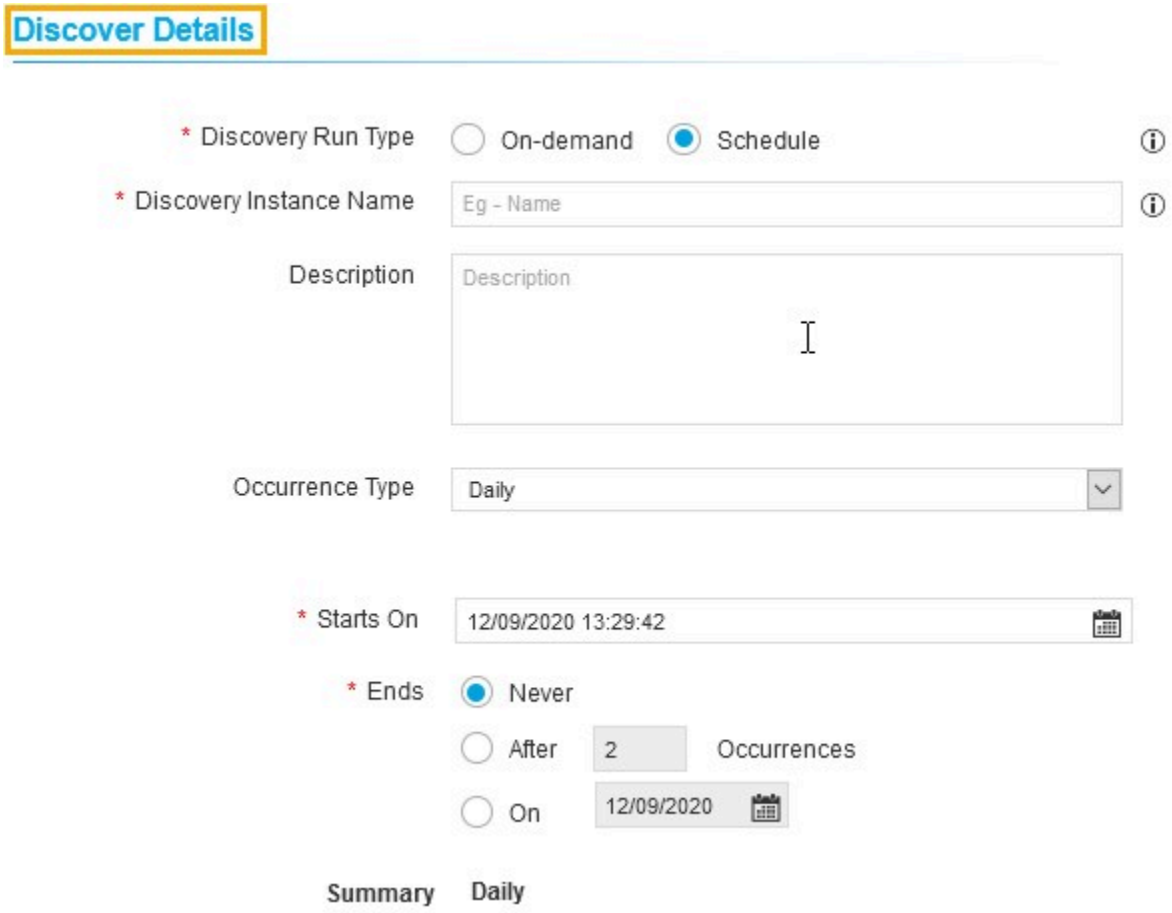
To discover a certificate from cloud,

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 **CERT+**.
   The CERT+ left navigation pane appears.
4. Expand **CERTIFICATE DISCOVERY**.
5. Click **Discovery**, and then select **Cloud Scan.**
   The **Add Discovery** page appears.



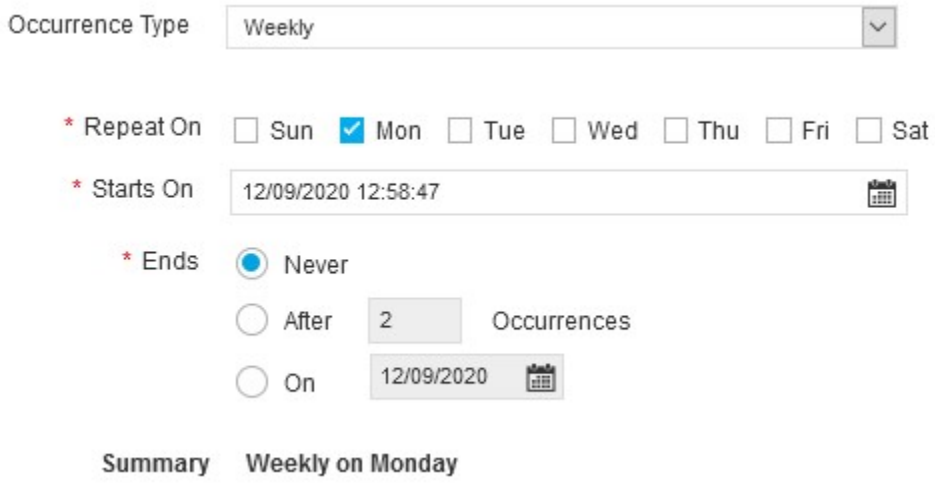
6. In the **Discover Details** section, select/enter the details as follows.





The following table describes the options available in the **Discover Details** section:

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. The possible types are: • On-demand - The user can trigger a discovery manually whenever he/she wants. • Schedule - By scheduling the discovery, the user can automate the process for a defined time/ frequency. If you select Scheduled discovery fill the below details.

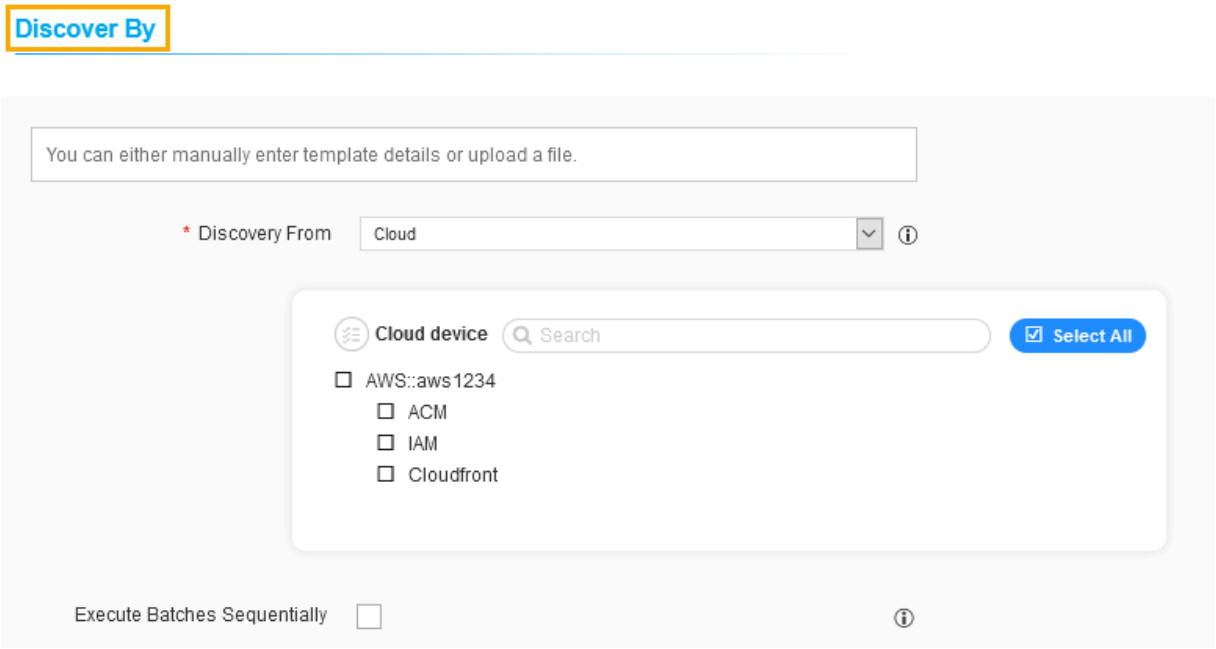
Field	Description
	

Field	Description
Occurrence Type	Select the type of occurrence from the dropdown list. The possible occurrences are: • Daily • Weekly • Monthly • Yearly.
***Repeat On**	Select a day in the week to schedule the weekly discovery.
***Starts On**	Select the date to start the scheduled discovery.
***Ends**	Select the desired last discovery. • Never - Continues to discover the certificate. • After - Stops the discovery process after a number of occurrences entered in the field. • On - Stops the discovery process for the selected period from the calendar.

Note: AppViewX will trigger the discovery certificates process for that instance.

Field	Description
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** You can enter a maximum of 2000 words in the field.
Note: The asterisk (*) symbol indicates a mandatory field.	

7. In the **Discover By** section, select/enter the details as follows.



The following table describes the options available in the Discover By section:

Field	Description
***Discover From**	Select the source from the dropdown list to discover a certificate.
Cloud Device Window	A list of all the managed cloud devices will be shown in the window. Select devices to discover certificates from.

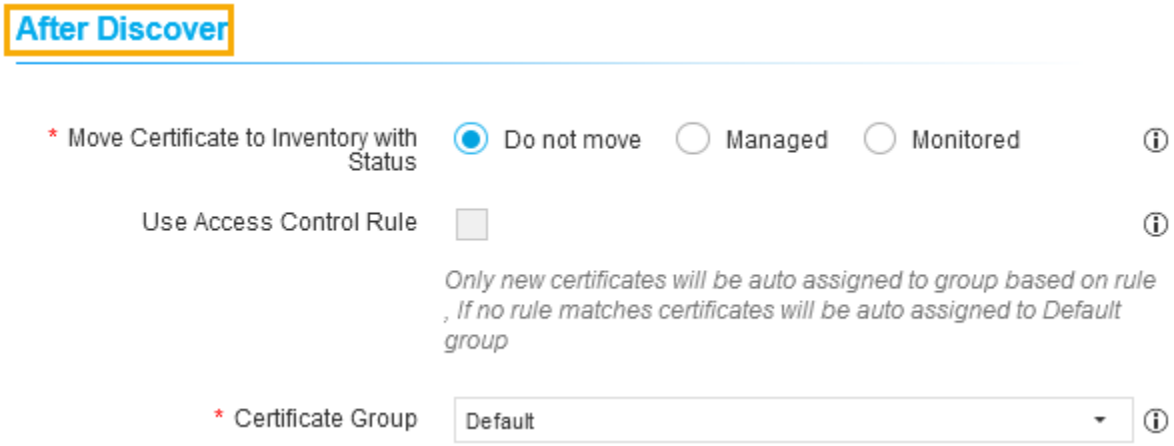
Field	Description
	Note: The asterisk (*) symbol indicates a mandatory field.

8. Select the Execute Batches Sequentially checkbox if required.
   a. If enabled, Based on the minutes value provided in Interval Between Batches field AppViewX will give the duration gap between each batch execution.
   b. If disabled, Scanning Intensity can be decided. An increase in scanning intensity will increase the scanning speed and network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.

9. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

   In the Discovery Rules section, select the Associate Rule from the dropdown list.

10. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the After Discover section:

Field	Description
***Move Certificate to Inventory with Status**	Click the check box to select the desired move certificate to inventory with status. The possible options are:

Field	Description
	• Do not move - Newly discovered certificates and associated objects will not be moved to inventory. • Managed - Newly discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - Newly discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the check box. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by rule in access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.
Note: The asterisk (*) symbol indicates a mandatory field.	

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

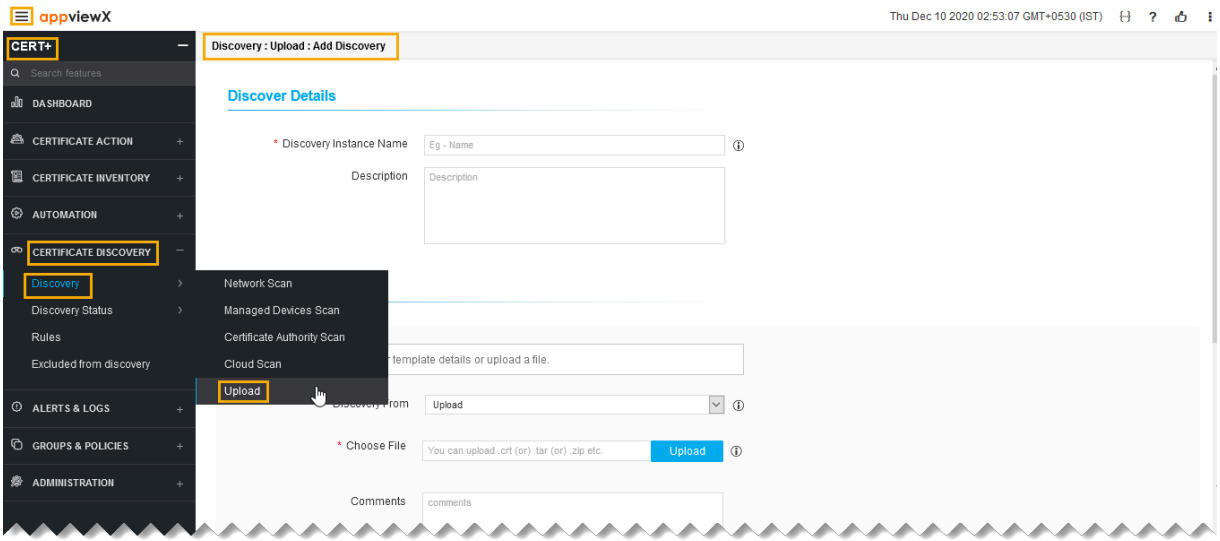
Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Scanning Uploaded Certificates

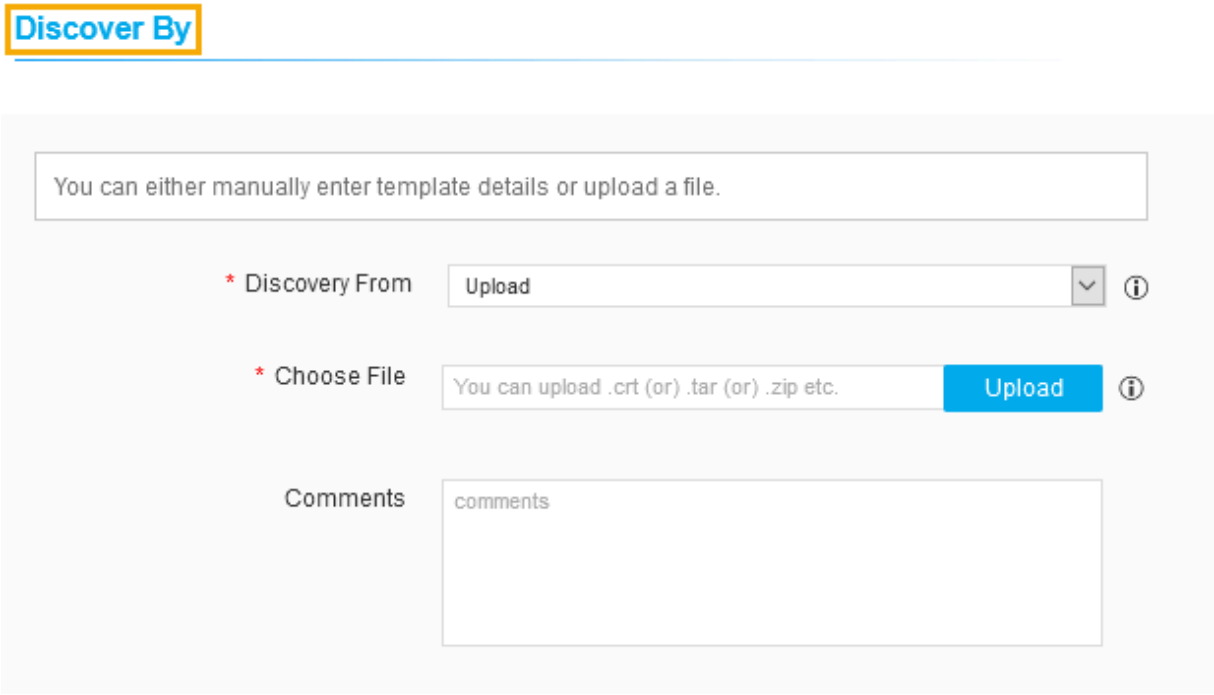
You can upload individual certificates or you can zip a group of certificates and then add them. For Windows-related servers and CA communication, an agent should be installed and configured in AppViewX.

To scan the uploaded certificate,

1. 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 **CERTIFICATEDISCOVERY**.
5. Click **Discovery**, and then select **Upload**.
   The **Add Discovery** page appears.



6. In the **Discover Details** section, enter the **Discovery Instance Name** and **Description**.
7. In the **Discover By** section, select/enter the details as follows.



The following table describes the options available in the **Discover By** section:

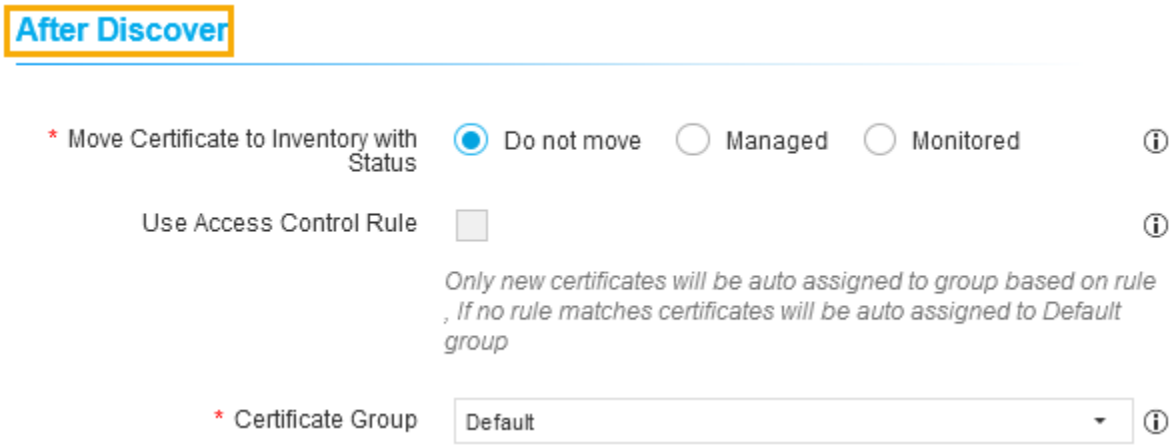
Field	Description
***Discover From**	Select the source from the dropdown list to discover a certificate.
***Choose File**	Click Upload and select the certificate you want to upload into the system, then click Open. • You can also upload encrypted keys in the <.zip>, <.tar>, or <tar.gz> file To upload certificates in bulk, you can create a <.zip>, <.tar>, or <tar.gz> file containing all the certificates and then click upload. • You can upload any of the following file types in the <.zip>, <.tar>, or <tar.gz> file: <.crt>, <.cer>, <.der>, <.p7b>, <.p7c>, <.pem>, <.pfx>, <.jks>, <.p12>.

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

8. **Note:** Set of filters created as a rule in the Rules menu. The selection of rules will apply respective filters on discovered certificates.

In the **Discovery Rules** section, select the **Associate Rule** from the dropdown list.

9. In the **After Discover** section, select/enter the details as follows.



The following table describes the options available in the **After Discover** section:

Field	Description
***Move Certificate to Inventory with Status**	Click the checkbox to select the desired move certificate to inventory with status. The possible options are: • Do not move - Newly discovered certificates and associated objects will not be moved to inventory. • Managed - New discovered certificates and associated objects will be moved to inventory with status Managed. • Monitored - New discovered certificates and associated objects will be moved to inventory with status Monitored. **Note:** If the discovered certificates already exist in the inventory, the associated object will be moved with the same status.
Use Access Control Rule	Select the checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.

Field	Description
***Certificate Group**	Select the **certificate group** from the dropdown list. Discovered certificates will be associated with this provided group.

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

10. Click **Discover** or **Schedule** to perform an On-Demand or Schedule certificate discovery respectively.

Discovery Status

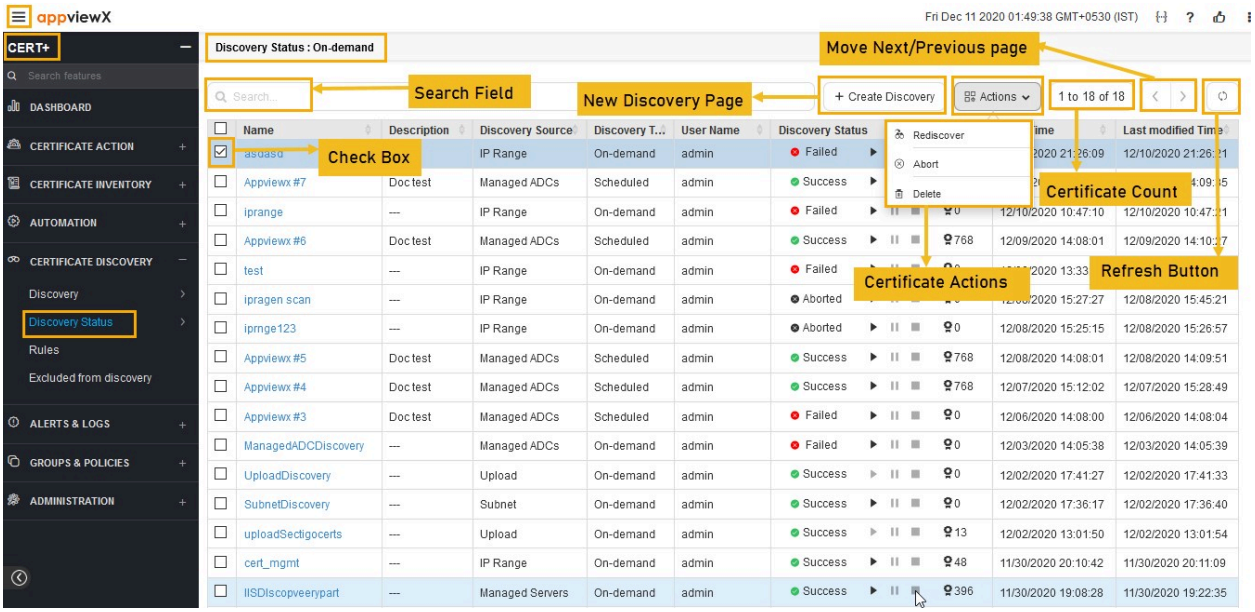
- Overview
- Excluding Unmanaged Certificate
- Filtering Discovered Certificates
- Exporting Discovered Certificates
- Aborting Certificate Discovery
- On-Demand Discovery Process
- Scheduled Discovery Process

Overview

The Discovery status provides a summary of a Discovery launched from a schedule and On-demand. Filters can be applied to certificates during discovery to filter them.

For example, certificates that are necessary to be part of this discovery instance can be ignored but can be rediscovered later, or if it has to be excluded from discovery can be set to excluded so it will not be rediscovered.

Certificates can be set to monitored or managed states individually based on their use.



The following table describes the options available in the Discovery Status home page:

Options	Description
Search Field	Searches for the given keyword(s) in the field and results in the dashboard that matches the search keyword(s).
Check Box	Allows you to select a certificate from the list.
Create Discovery	You can create a new discovery based on requirements.
Certificate Actions	Allows to rediscover, abort, and delete the certificates.
Certificate Count	Displays the number of certificates available in the list.
Next/Previous page	Arrow mark allows you to move next and previous page.
Refresh Button	Refreshes the related tabs.

Excluding Unmanaged Certificate

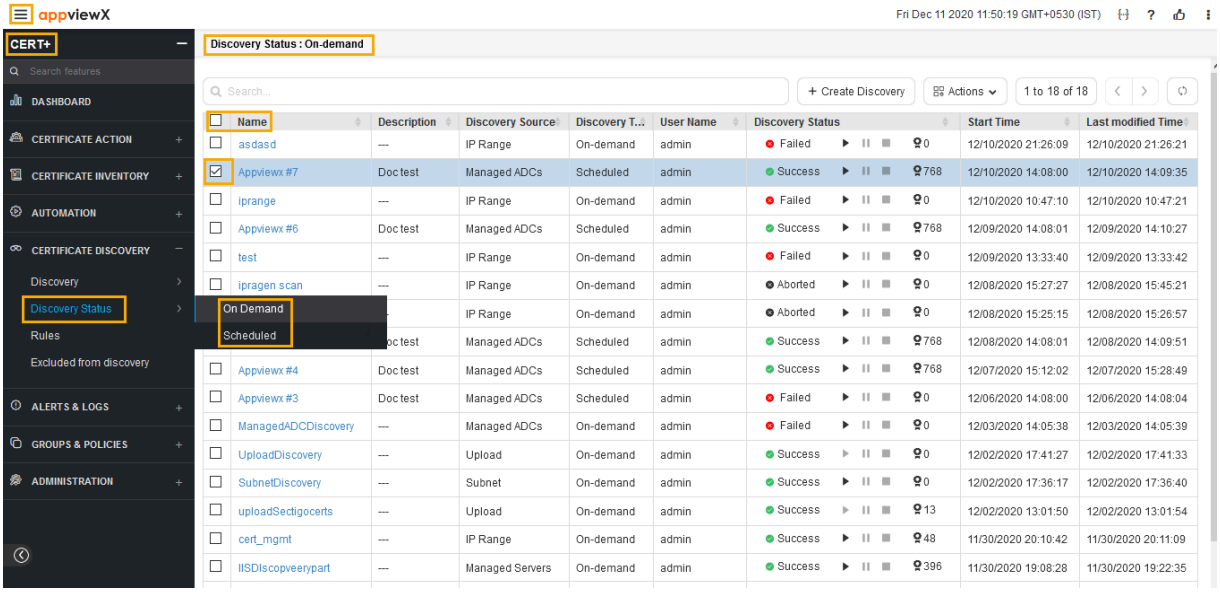
To exclude the unmanaged certificates,

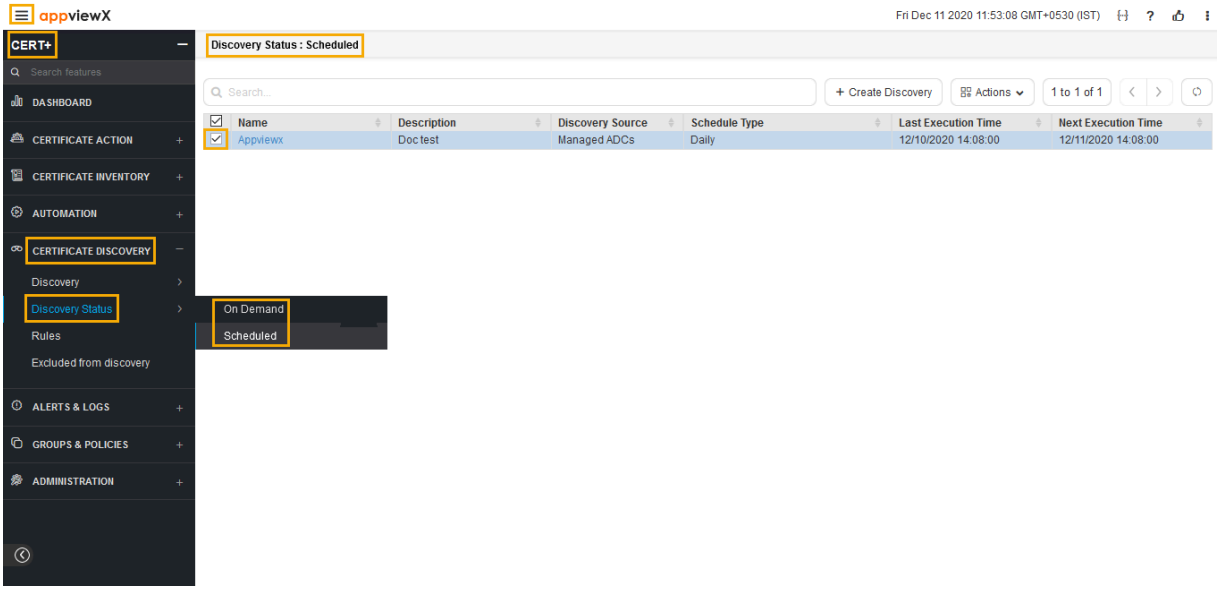
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

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

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE DISCOVERY**.
5. Click **Discovery** Status, and then select **On-Demand**.

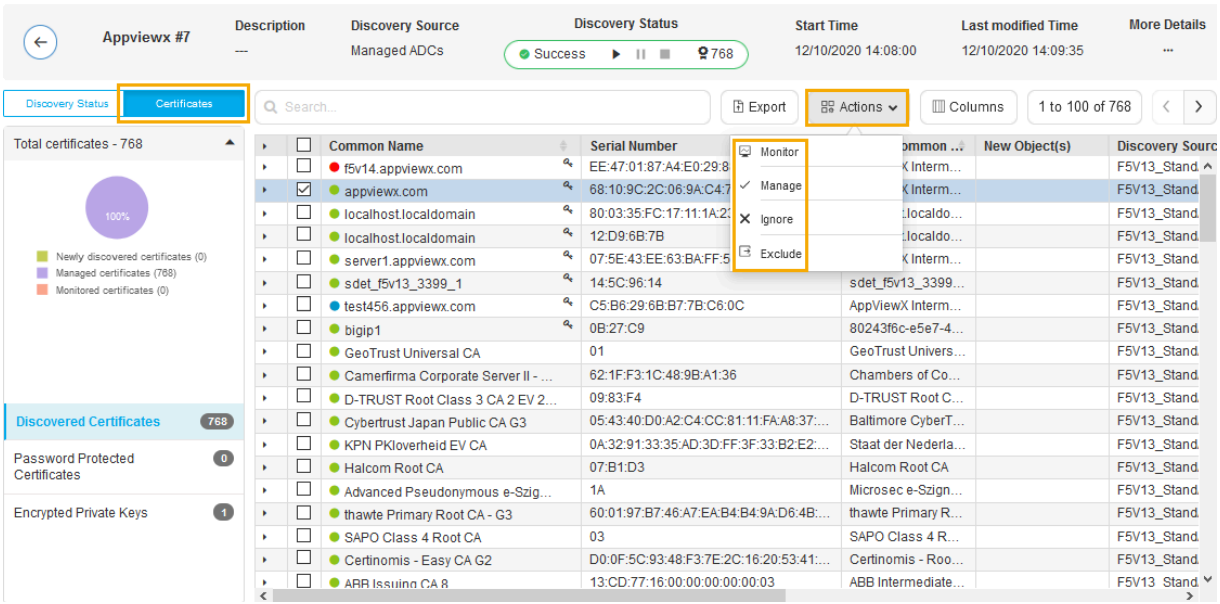
   The **On-Demand** page appears.





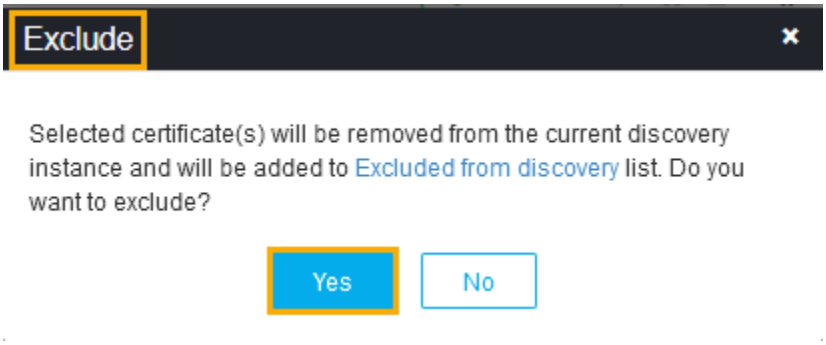
6. In the certificate list view, click on the name of the certificate.
7. Click Certificates on left of the pane.

The Certificates list page appears.



8. In the certificate common name list, select the certificate that you want to exclude.
9. Click **Actions**, and then select **Exclude**.

   The Exclude pop up window appears.



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

    Click **Yes**.

    The pop-up message appears as **Selected certificate(s) are removed from the current discovery instance and added to "Excluded from Discovery"** list.

Filtering Discovered Certificates

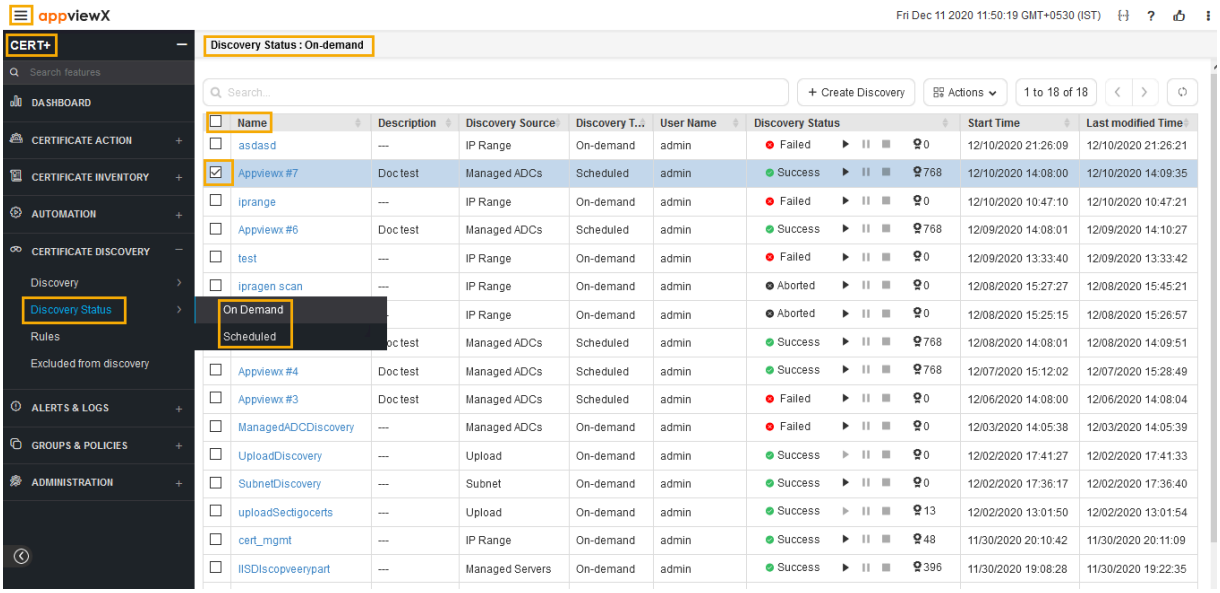
AppViewX provides smart discovery features options such as Monitor, Manage, Ignore, and Exclude. Discovery results can also be exported as <.csv> and <.xls> files. Certificate Discovery can also be aborted once started.

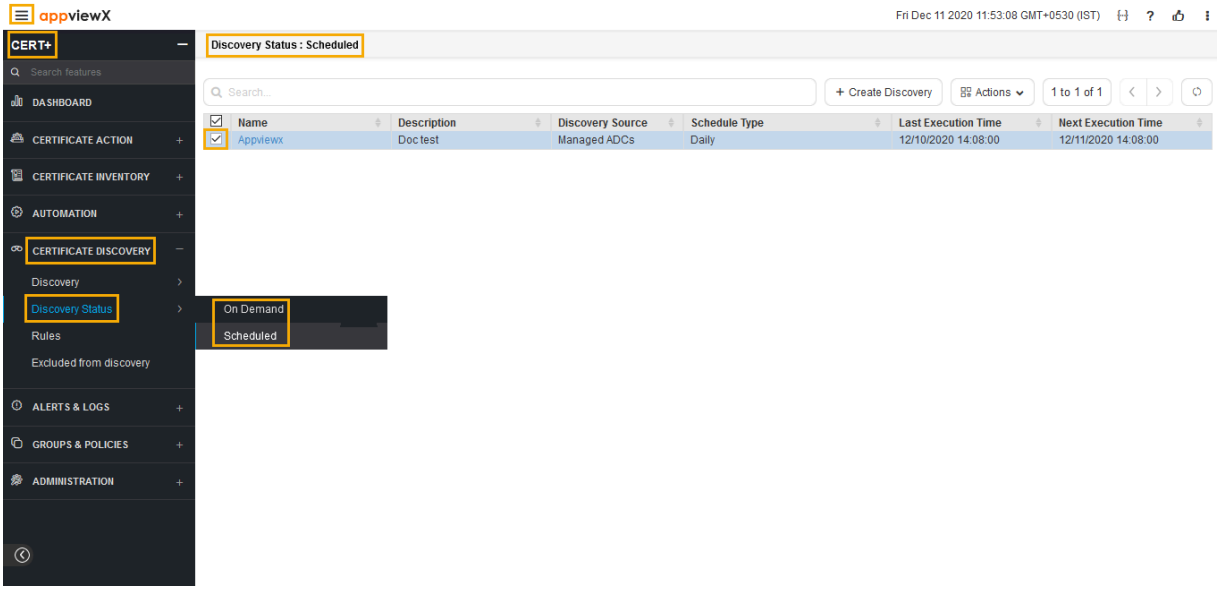
Certificates discovered can be set to one of these states:

- **Monitor** - Discovered certificate status will be updated as Monitored.
- **Manage** - Discovered certificate will be moved to inventory with status as Managed.
- **Ignore** - Discovered certificate will be removed only from the current discovery instance and can be rediscovered.
- **Exclude** - Discovered certificate will be excluded from discovery and will be added to Exclude from Discovery Inventory.

To set the discovered certificate to Monitor/Manage/Ignore/Exclude,

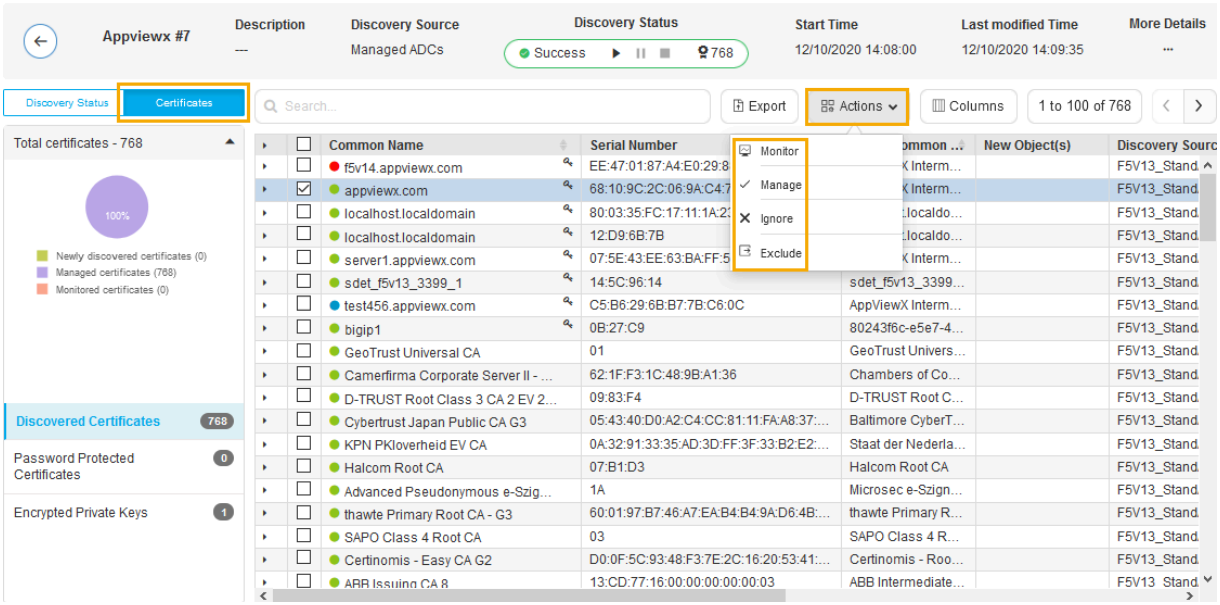
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE DISCOVERY**.
5. **Click On-Demand**, and then select **Discovery Status**.
   The **On-demand** page appears.





6. Click the discovery name from the list.
7. Click Certificates on the left of the pane.

   The Certificates list page appears.



8. A pie chart is drawn/displayed when the below tabs are clicked and each is segregated based on the color codes:

   • Discovered Certificates

   • Password Protected Certificates

   • Encrypted Private Keys

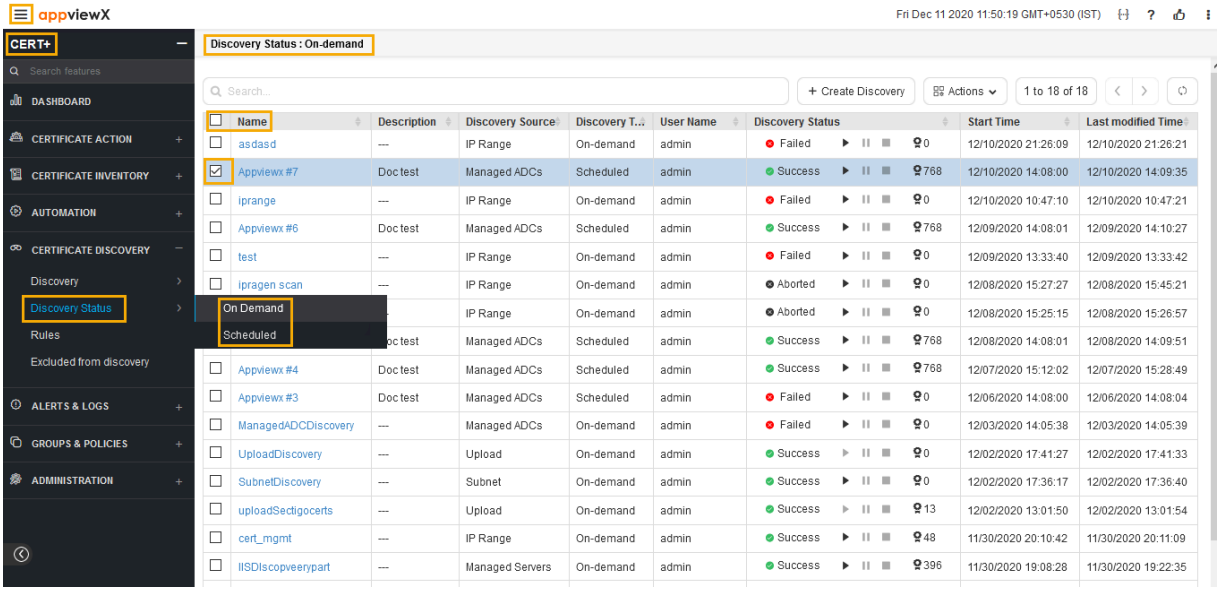
9. In the certificate common name column, select the certificate that you want to filter.
10. Click **Actions**, and then select Monitor or Manage or Ignore or Exclude.
    The pop-up window appears.
11. Click **Yes**.

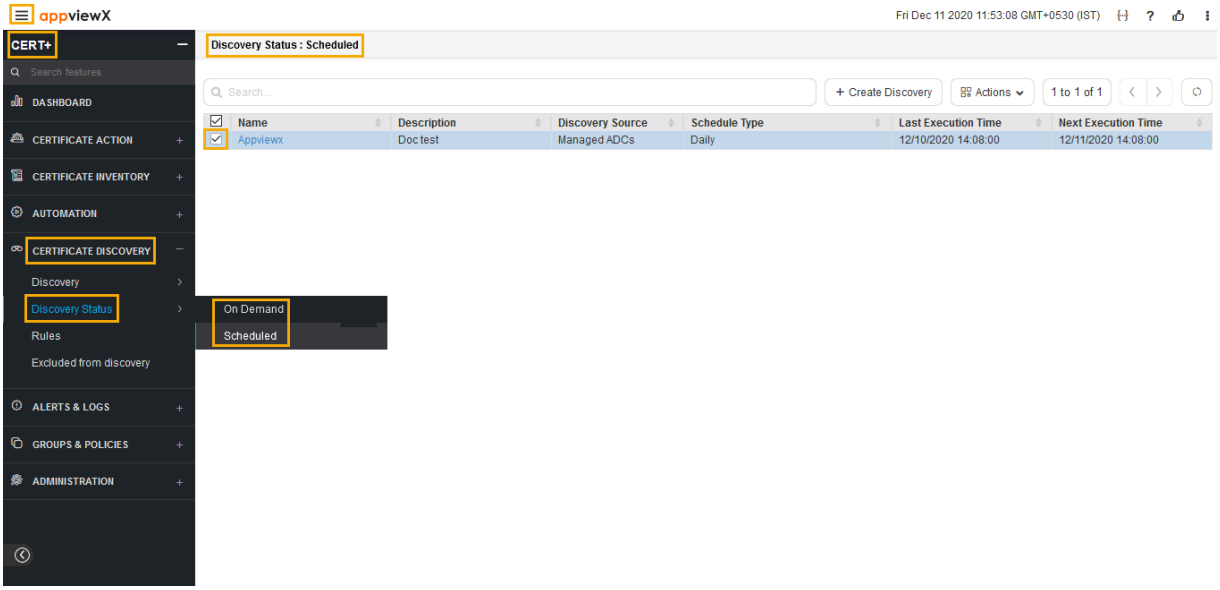
Exporting Discovered Certificates

To export discovered certificates,

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 DISCOVERY**.
5. Click **Discovery Status**, and then select **On-Demand**.

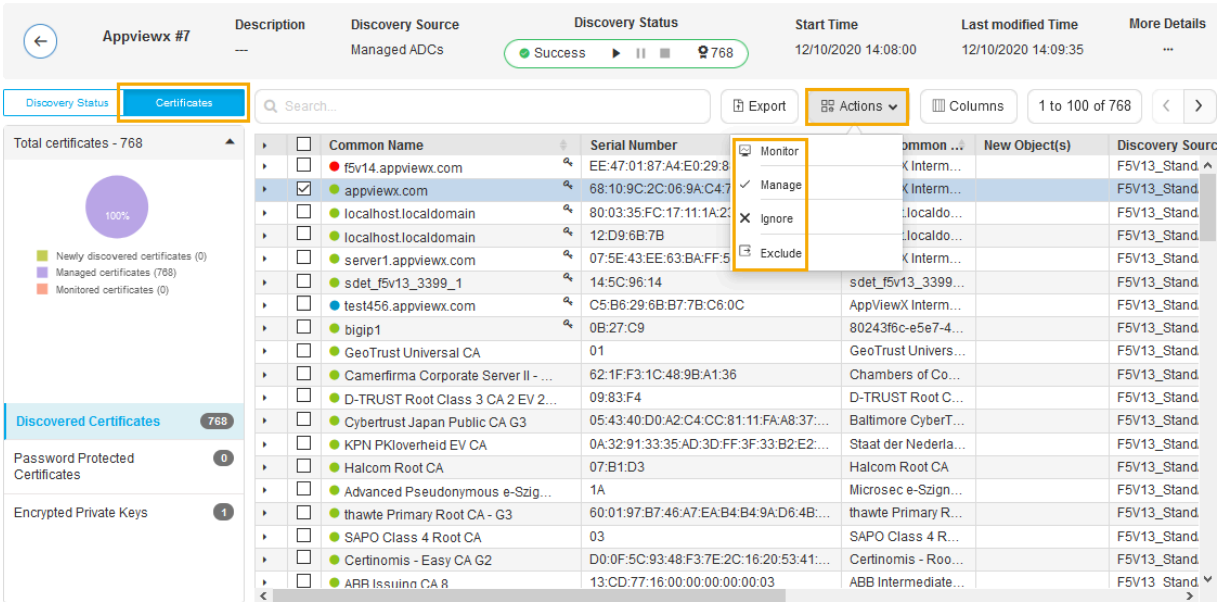
The **On-demand** page appears.





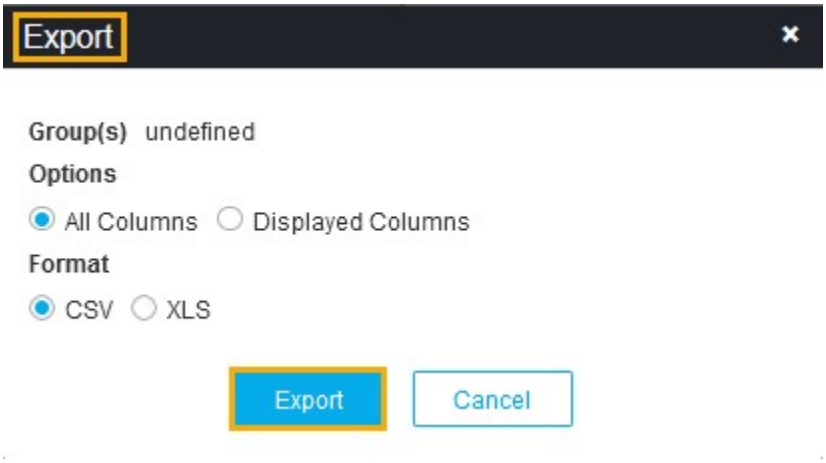
6. In the certificate list view, click on the name of the certificate.
7. Click Certificates on left of the pane.

   The Certificates list page appears.



8. In the certificate common name list, select the certificate that you want to Export.
9. Click **Export**.

   The Export popup window appears.



10. Select the desired **Options** and **Format** in the Export popup window.
11. Click **Export**.

    The selected certificates are exported to your local machine.

Aborting Certificate Discovery

Steps to abort discovered certificates,

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

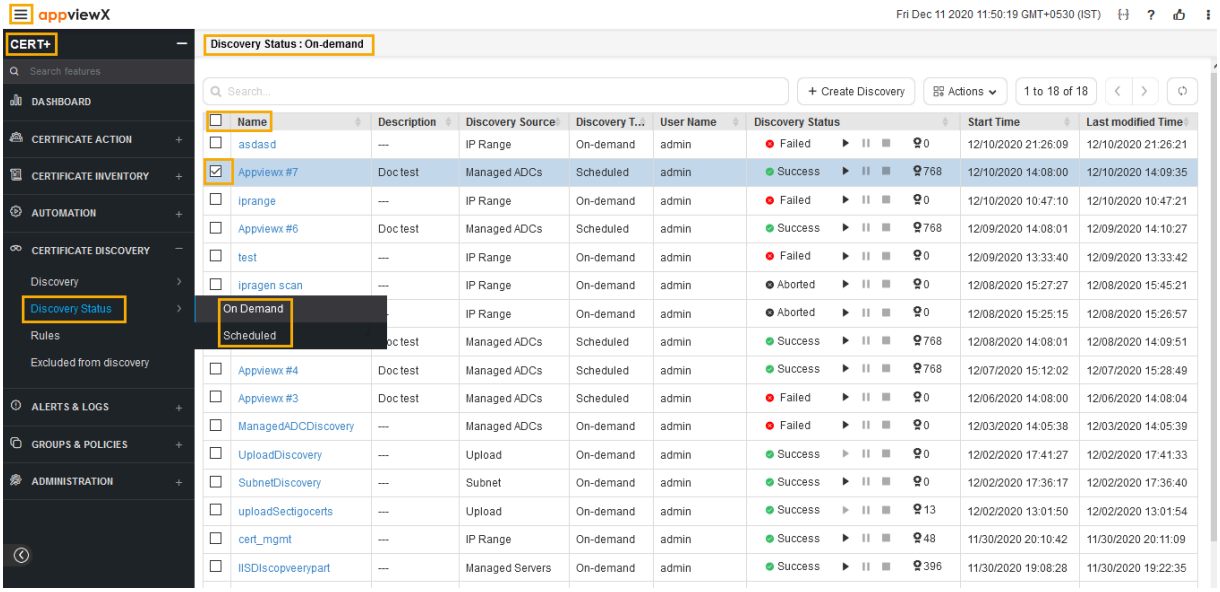
   The left navigation pane appears.

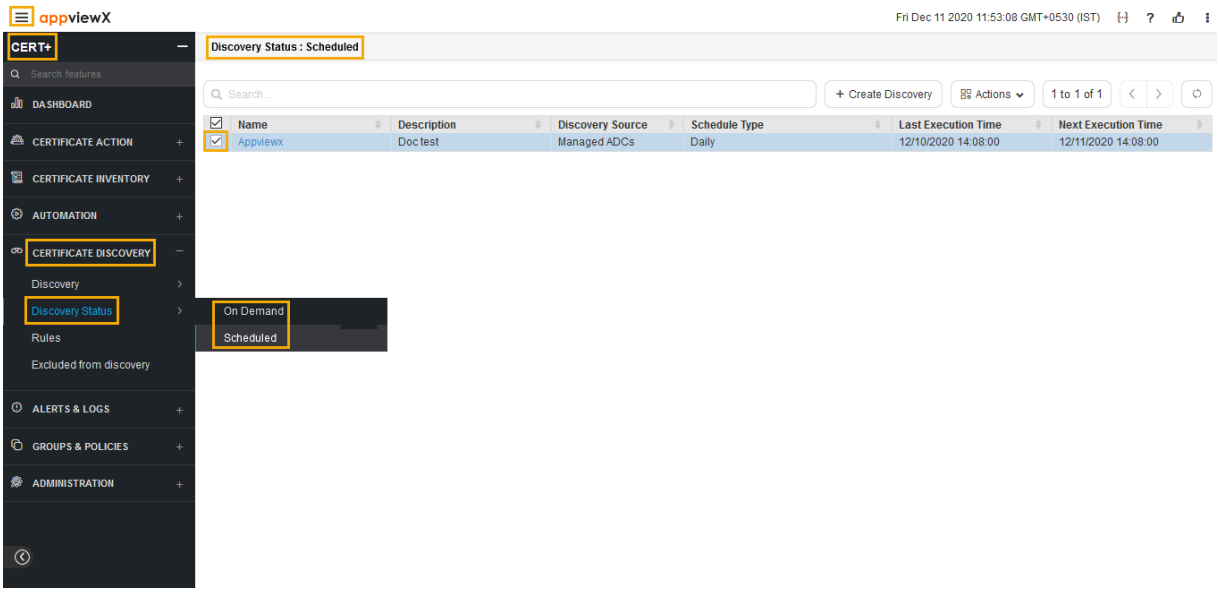
3. Click **CERT+**.

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

4. Expand **CERTIFICATE DISCOVERY**.
5. Click **Discovery Status,** and then select **On-Demand**.

   The **On-Demand** page appears.



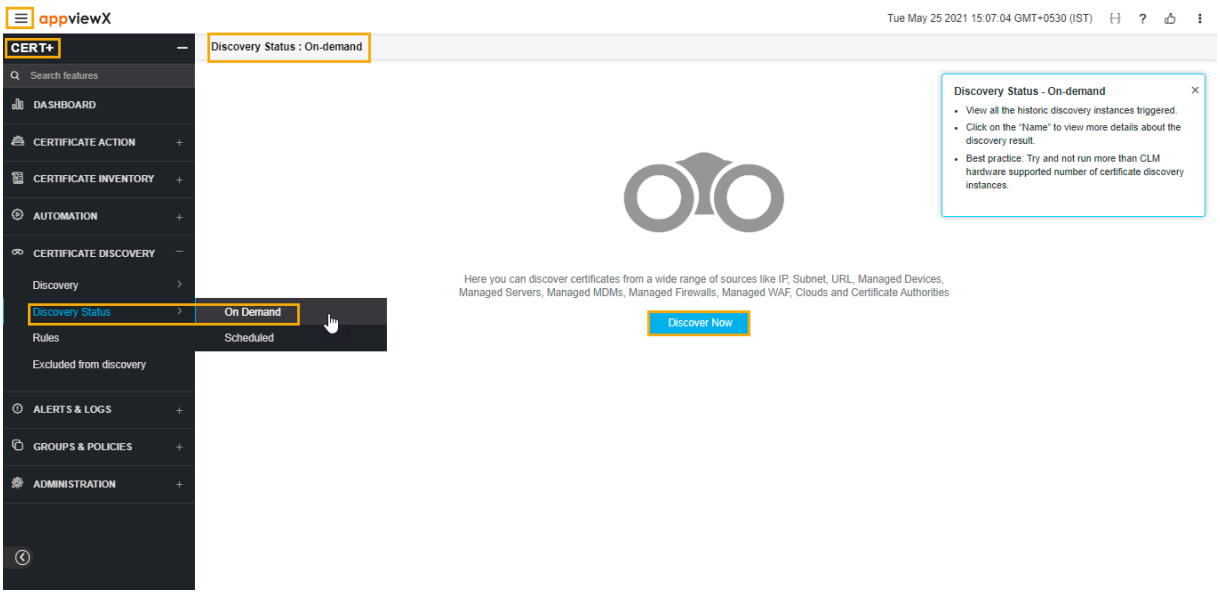


6. In the certificate list view, click on the discovery instance name of the certificate.
7. Click **Actions**, and then select **Abort**.

On-Demand Discovery Process

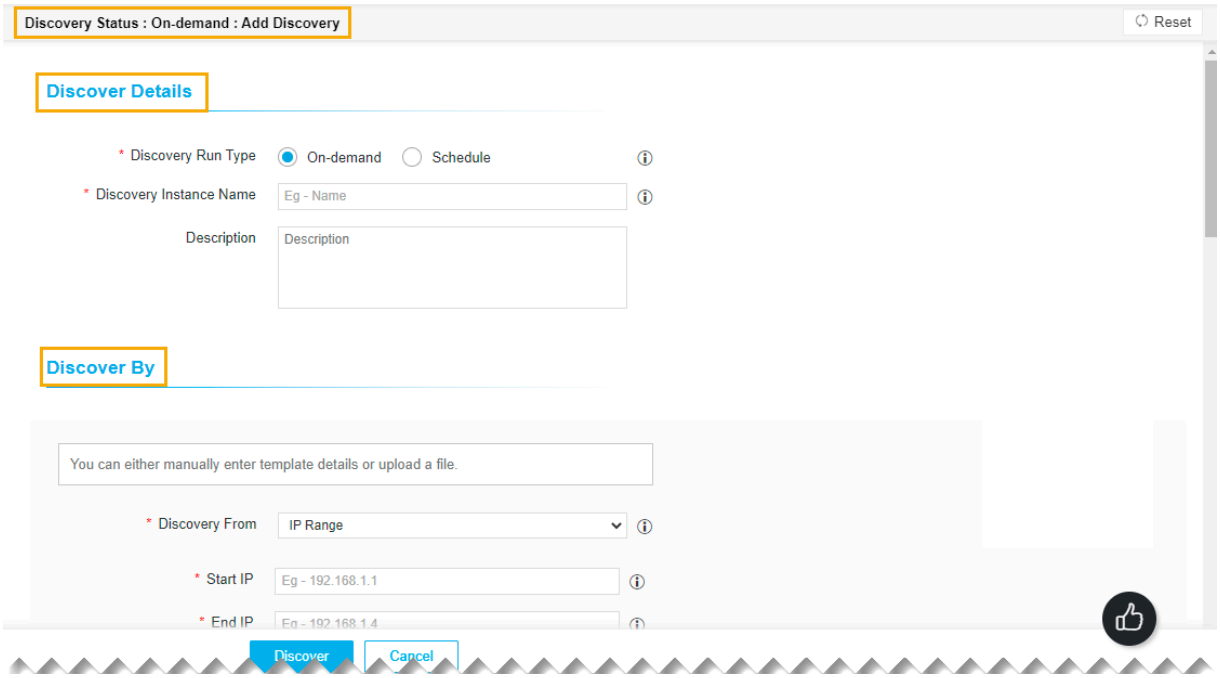
Steps to schedule on-demand discovery process,

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 DISCOVERY**.
5. Click **Discovery Status**, and then select **On-Demand**.



6. Click **Discover Now**.

   The **Add Discovery** page appears.



7. Select Discovery Run Type as On-demand in the **Add Discovery** page.
8. Enter the Discovery Instance Name and Description in the respective fields.
9. In the **Discover By** section, you can either manually enter the details or upload a file.
10. Click **Add**.
11. Make sure that the detail is listed in the record section.
12. Select the **Execute Batches Sequentially** check-box if required.

13. Increase the **Scanning Intensity** as required.
14. Select the **Skip Full Scan** if required.
15. In the **Device discovery** option, select the required discovery from the drop-down list.
16. In the **Discovery Rules** section, select the Associate Rule from the drop-down list.
17. In the **After Discover** section, enter/select the details as required.
18. Click **Password Vault** if you want to discover any encrypted certificate.
19. Click **Discover**.

Scheduled Discovery Process

Overview

If Discovery Run Type is selected as Scheduled, the discovery can be run multiple times at the scheduled time automatically.

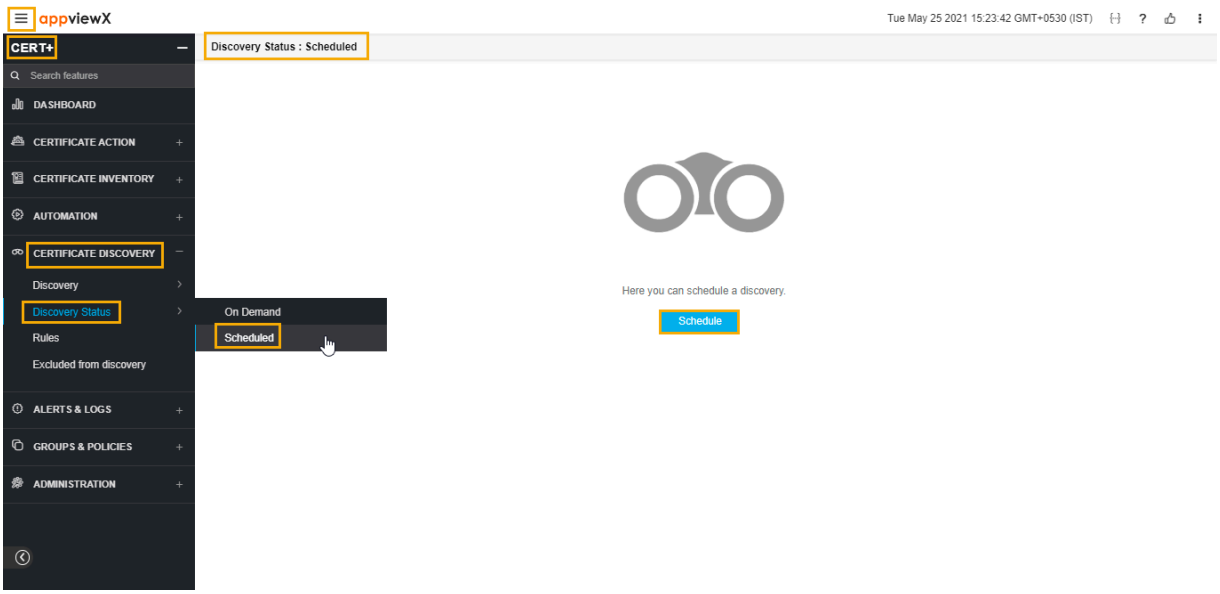
Scheduled Discovery Process

While creating discovery, it can run On-Demand or at a Scheduled time. On-Demand can be selected if needed to run the certificate discovery process only once. Discovery can be scheduled if needed to run the certificate discovery process one or more times in the scheduled duration.

Scheduled Discovery Process

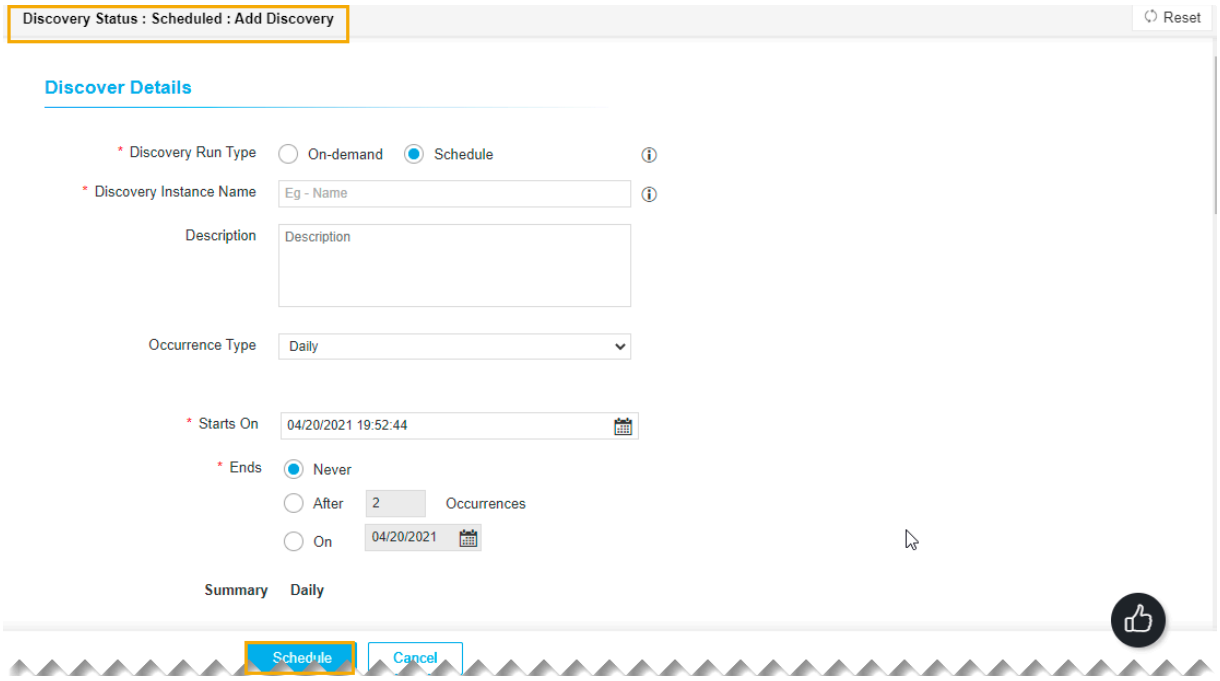
Steps to schedule the scheduled discovery process,

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 DISCOVERY**.
5. Click **Discovery Status**, and then select Scheduled.
   The Scheduled discovery page appears.



6. Click **Schedule**.

   The **Add Discovery** page appears.



7. Select Discovery Run Type as Schedule on the Add Discovery page.
8. Enter the Discovery Instance Name and Description in the respective fields.
9. Occurrence Type: You can select the frequency of the discovery process in this section. You can choose between Daily, Weekly, Monthly, and Yearly.
10. Starts On: You can select the start date and time for the discovery process in this field.
11. Ends: In this section, you can choose between the following:

a. Never: You can select this option if you never want the discovery process to end.
b. After a specific number of occurrences: You can enter the number of occurrences after which you want the discovery process to stop in this field.
c. On: You can enter the date by when you want to end the discovery process.

12. In the **Discover By** section, you can either manually enter the details or upload a file.
13. Click **Add**.
14. Make sure that the detail is listed in the record section.
15. Select the **Execute Batches Sequentially** check-box if required.
16. Increase the **Scanning Intensity** as required.
17. Select the **Skip Full Scan** if required.
18. In the **Device discovery** option, select the required discovery from the drop-down list.
19. In the **Discovery Rules** section, select the Associate Rule from the drop-down list.
20. In the **After Discover** section, enter/select the details as required.
21. Click **Password Vault** if you want to discover any encrypted certificate.
22. Click **Schedule**.

Discovering Rules

Overview

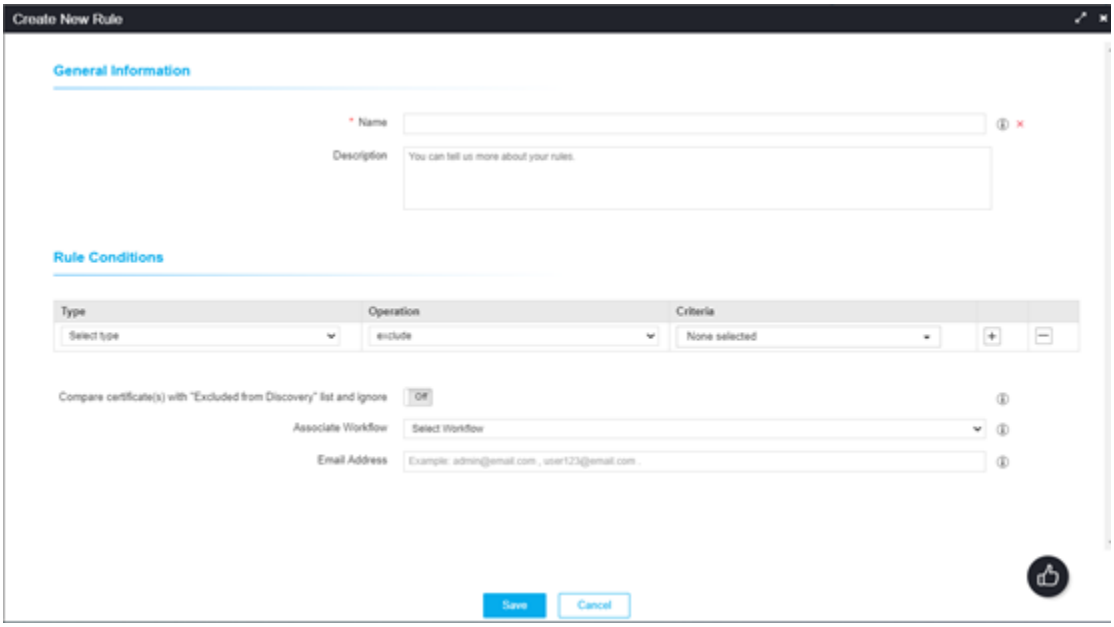
Discovering certificates are one-time activity and not required to continue for each discovery. You can optimize the discovered data by criteria, which helps to filter the necessary certificates. To enable an optimization filter, CERT+ provides a rule engine. You can set a rule to include or exclude any criteria on the discovery. For example, you can exclude certificates from the test CA present in the infrastructure that are not required to be managed by the production CLM server.

As an advanced use case, you can map a custom logic as a visual workflow template over the filtered certificates. You can provide the custom logic to be applied to certificates and the AppViewX will assist you with templates.

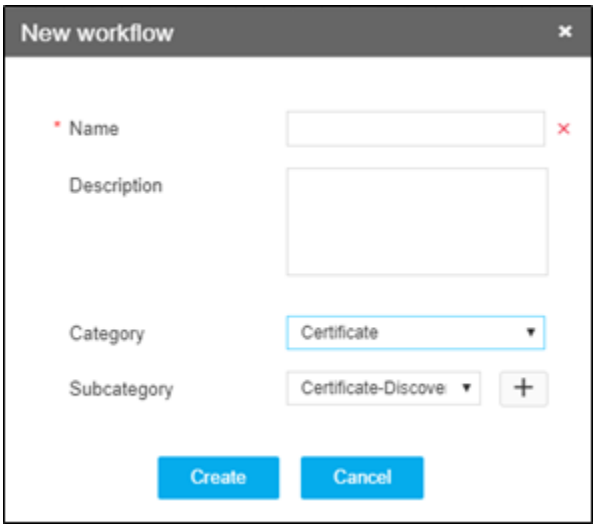
Creating New Rule

To create a new Rule,

1. Log in to **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 DISCOVERY**.
5. Click **Rules**, and then click **Create New Rule**.
   The **Create New Rule** page appears.



6. On the **Create New Rule** popup window, enter a unique **name** for the rule. You can also enter a **description** for the rule.
7. In the **Rule Conditions** section, you can specify the **type**, **operation**, and **criteria** of the rule.
8. If you want to compare certificate(s) from the **Exclude from discovery** list and ignore it, you can enable that option. Based on this discovery, the discovered certificates that were already excluded and stored in the **Excluded from discovery** inventory, will automatically be excluded.
9. To associate a workflow with your rule, you can select your workflow from the **Associate Workflow** drop-down list.
   Only workflows that were already created appear in this list. To create a workflow, go to **Menu >> Studio >> Workflow** and click **Design**. Ensure that you map the workflow to the Certificates. Only then it will appear in the **Rules** section.

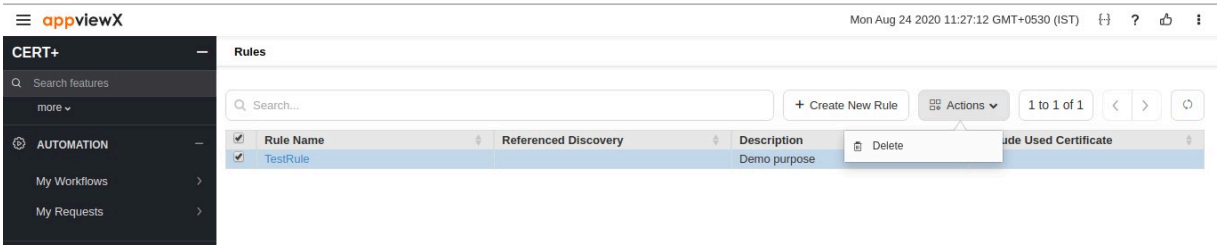


10. If you want to email the rule details to the **email address(es)**, you can enter the email addresses separated by a comma in the **Email Address** section.
11. Click **Save**.

Deleting Rule

To delete a rule,

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 DISCOVERY**.
5. Click **Rules**.
6. From the **Rule Name** list, select the rule that you want to delete.
7. Click **Actions**, and then select **Delete**.



Excluded from Discovery

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

To exclude certificates,

1. 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 DISCOVERY**.
5. Click **DiscoveryStatus**, and then select the type of discovery that was run to view all the historic discovery instances triggered.
6. Click on the name of the discovery to view details about the discovery result.
7. Click Certificates from the left pane to view a list of discovered certificates.
8. Select the certificates that you want to be excluded from the discovery list.
9. Click **Actions**, and select **Exclude.**
   The **Exclude** popup window appears.
10.  **Note:** Excluded certificates will be removed from the current discovery instance and will be added to the Excluded from discovery inventory.

    Click **Yes**.

Staying in Sync with Network Devices or Servers

Overview

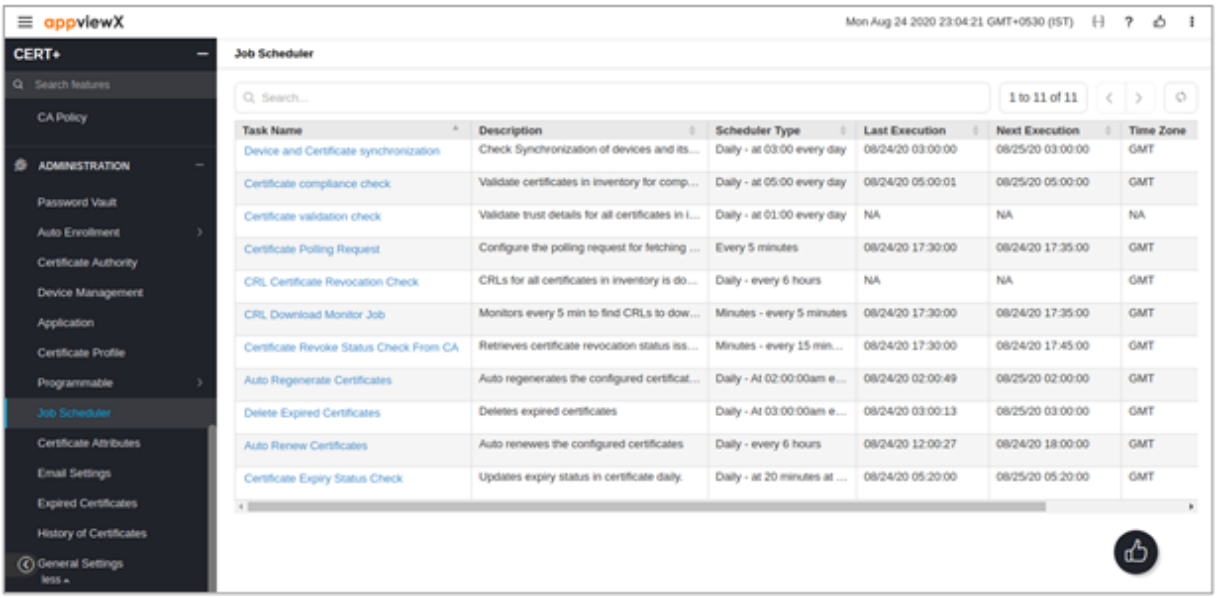
Important to ensure certificates are in sync with network devices. This is achieved via a cronjob which regularly fetches the config and updates the data.

Certificate Sync with Device

AppViewX has this cronjob named Device and Certificate Synchronization which syncs the configuration file for the eligible devices and thus refreshes the list of certificates available in the inventory from that device. The respective device must be managed in AppViewX. By default, this cronjob runs every day at 3 A.M. This job can be customized to run at a specific time using the Job Scheduler section. Users can customize the frequency of the trigger via cronjob.

To view this job,

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 select **Job Scheduler**.
5. Check the **TaskName** field and locate the **Device and Certificate Synchronization** job under that.
   This is the job being used for certificate sync with devices.

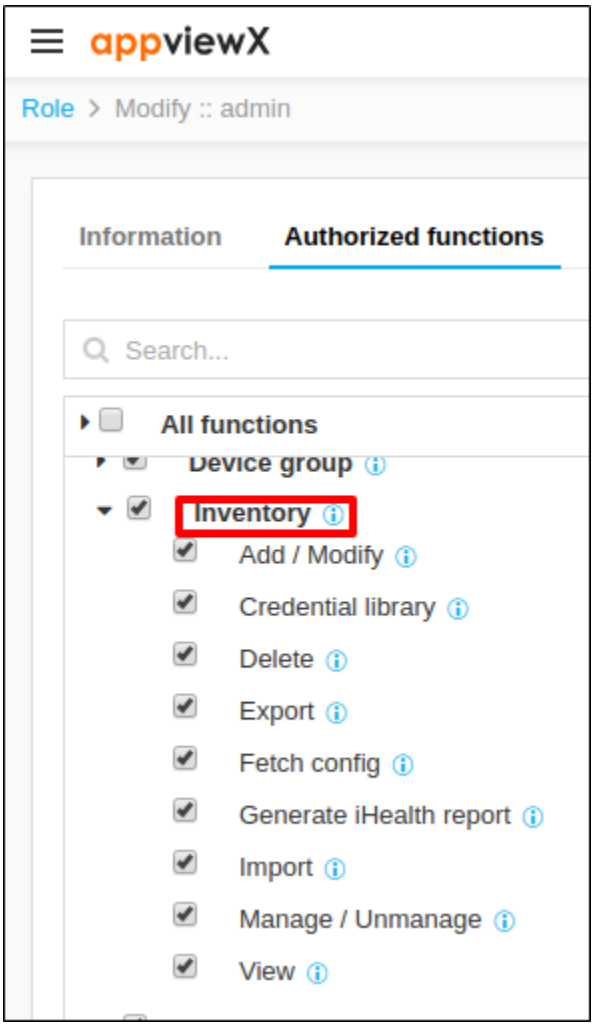


Chapter 3: Manage Devices

Inventory Actions

Inventory Actions

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



Manually Fetch the Configuration for a Device

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

To manually get the configuration for a device,

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. If the device is not listed on the screen, run a search to locate it.
4. Click the checkbox beside the device name. If you want to fetch configurations for multiple devices of the same type, select their checkboxes, too.

5. Click the  **Fetch Config** button in the Command bar.
6. A notification appears at the top of the screen stating, "**Fetch config has been triggered for the device.**

Delete Device

To delete the device from the inventory,

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. Select the desired device to delete.
4. Click the **Delete** button in the Command bar.
   The **Delete** confirmation modal appears.
5. Click **Yes** to delete the selected device.

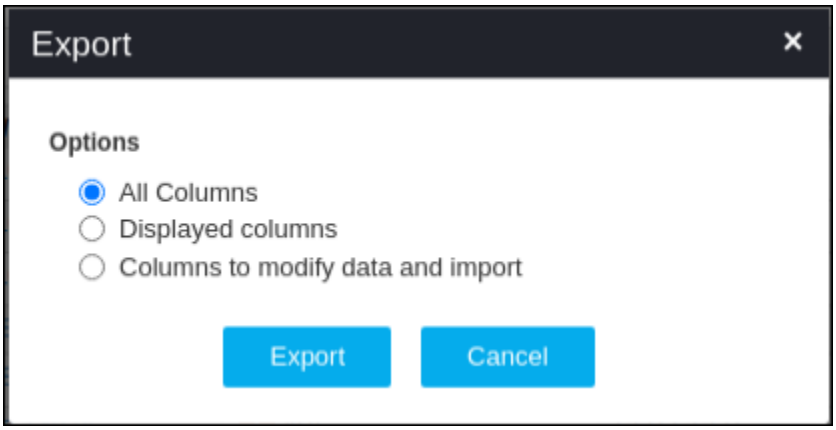
> **Note:** To discard the deletion, click **No**. The device details and configurations will be permanently deleted from AppViewX. If the deleted device is onboarded again, it will be considered as onboarding a new device.

Export Device Details

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

To export the details of one or more devices,

1. Log in to AppViewX application with valid credentials.
2. Click the  **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. If the device you want to export is not listed on the screen, run a search to locate it.
4. Click the checkbox beside the device name. If you are exporting details of multiple devices of the same kind, select the checkboxes for each one.
5. Click the  **Export** icon in the Command bar at the upper right of the screen.
6. On the **Export** pop-up screen that appears, select the type of information you want to export.



- **All Columns** - Select this option if you want to export all information about the device.
- **Displayed columns** - Select this option if you want to export only the information that is visible on the Device screen. This is useful if you need to compare values or settings for different devices and do not have any need to see the less important data.
- **Columns to modify data and import** - Select this option if you are exporting device details to make modifications and then re-import the data into the Device Inventory.

7. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
8. The details are then downloaded as an Excel `<.xls>` file.

Import Devices

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

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

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. Click the **Import** icon in the Command bar.
4. On the Import screen that appears, navigate to the location of the import file, then select it.

5. Click **Import** to add the devices and their details to the Inventory.

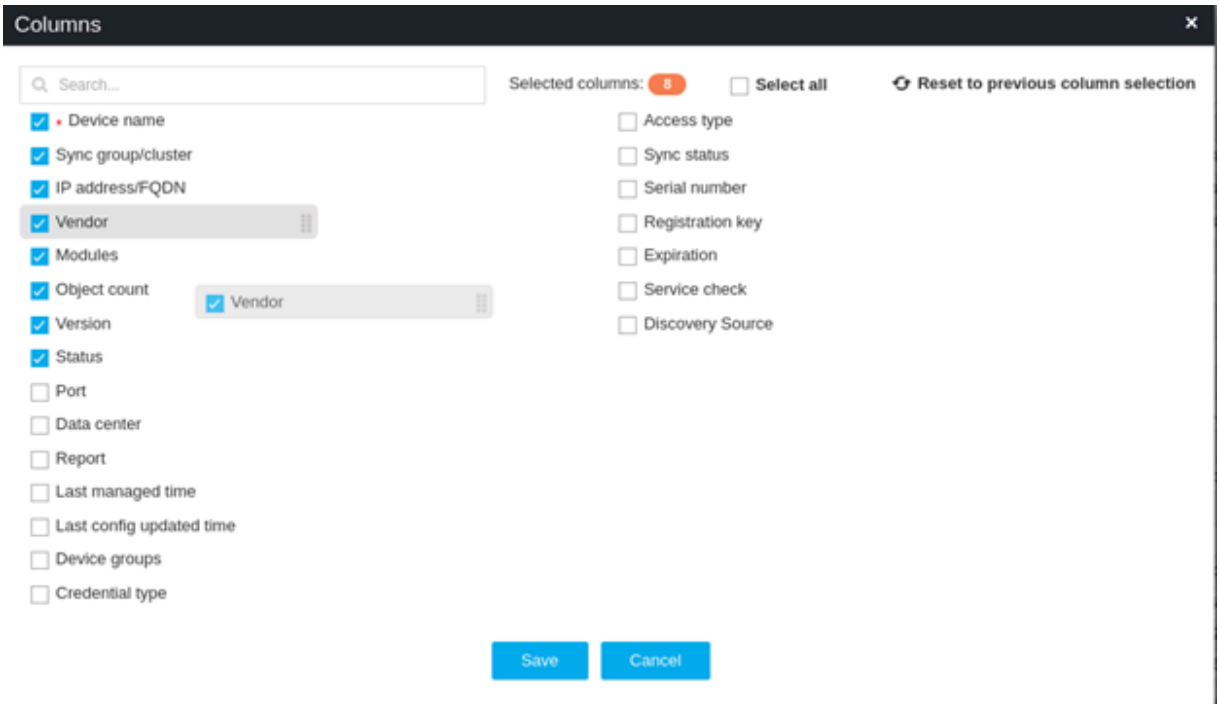
> **Note:** When the file is uploaded with improper structure or incorrect data, the import process will terminate with the errors highlighted.

Customizing Columns

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

To customize columns,

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. Click the **Columns** icon in the Command bar.
   The **Columns** pop-up opens.



4. In the Columns pop-up, you can modify the columns by doing any of the following or in combination:
   a. Select or deselect the desired columns to be displayed.
   b. Alter the order of the column by dragging the column name to the desired order.

c. Select all the available columns by clicking the **Select all** checkbox.

d. Reset to the previous column selection by clicking the "**Reset to previous column selection**".

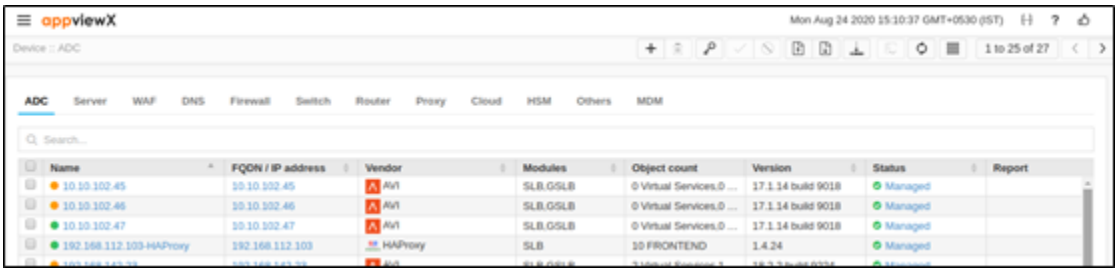
5. Click the **Save** button.

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

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

Validating the Column selection

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



Manage Device

To manage devices,

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

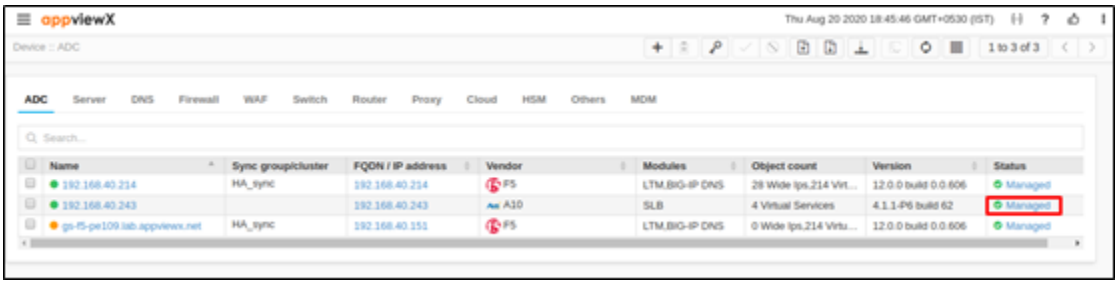
   By default, the **ADC** tab opens.

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

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

Validating the Manage Action

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

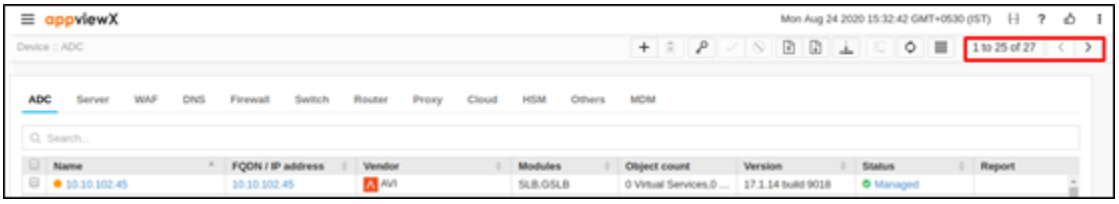


Pagination

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

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

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



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

Unmanage Device

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

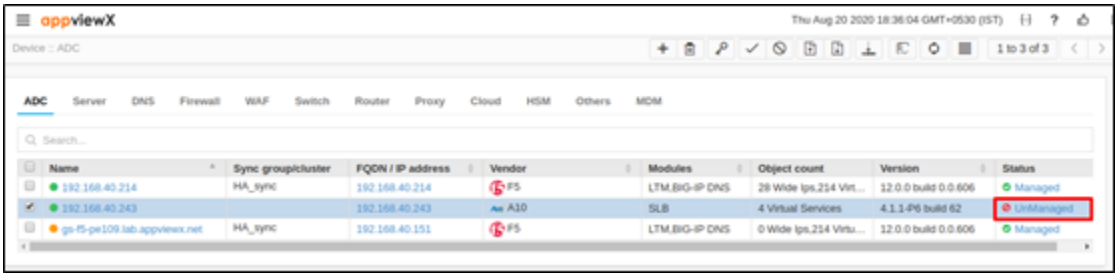
1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. **Note:** If you try to manage a device that is already in managed state or unmanaged a device that is already in an unmanaged state, an error message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

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

4. Click the checkbox beside the device name.
5. To start managing the device, click the Unmanage button in the Command bar at the top of the screen.

Validating the Unmanaged Action

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



Device Pre-requisite

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

ADC Pre-requisite

Supported Vendors	A10	AVI	Akamai	Amazon ELB	BigIQ	Cisco
IP Address/ FQDN	IP Address/ FQDN	IP Address/ FQDN Note: Device must not be	Not Applicable	Not Applicable	IP Address	IP Address

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

Supported Vendors	A10	AVI	Akamai	Amazon ELB	BigIQ	Cisco
Location from which the certificates are discovered if Certificate Managed	No specific location	No specific location(use API's to get certificate details)	Not Applicable	Not Applicable (Certificates that are assigned to the listeners will be discovered by AppViewX)	CERT+ Discovery is not supported	CERT+ Discovery is not supported

Supported Vendors	Citrix	F5	HAProxy	NginxPlux	Infoblox LBDN
IP Address/ FQDN	IP Address/ FQDN	IP Address/ FQDN	IP Address	IP Address/FQDN	IP Address/ FQDN
User Privilege	• Super-user access. • Username/ Password • Credential List • AppViewX/ CyberArk	• Admin access • TMSH access • Username / Password • Credential List AppViewx/ CyberArk	• Username / Password • Credential List AppViewx/ CyberArc	Access to Nginx Installed configuration locations and access to check the syntax of Nginx. conf and restart the Nginx service to apply changes.	• Super-user access or • Access to LBDN objects that need to be managed from AppViewX
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Yes	Yes	Yes	Not Applicable

Supported Vendors	Citrix	F5	HAProxy	NginxPlux	Infoblox LBDN
Services and Prot for AppViewX communication	• Outbound Access from AppViewX for SSH & HTTPS service (Default/ Custom Port Information is required) • Outbound access to port 5514 is required for Citrix Device to forward the Syslog to AppViewX	Port number: 22 and 443	Port number: 22 (SSH)	Port number: 22 and any custom port for stats	Port number: 443 or custom port to access API calls
Internet Access/Proxy if required	Required, if needs to be accessed with Public IP address.	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed	Certs are parsed only from /flash/ nsconfig/ssl/ directory	/config/ filestore/ files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/ pki/tls/certs/ V10	CERT+ Discovery is not supported	/etc/nginx/conf.d/ or any custom location	Not Applicable

Supported Vendors	Citrix	F5	HAProxy	NginxPlux	Infoblox LBDN
		/config/ssl/ ssl.crt/ /etc/ httpd/conf/ ssl.crt/ /etc/ pki/tls/certs/			

Firewall and Web Application Firewall (WAF) Pre-requisite

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

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
are discovered if Certificate Managed.	command to the device through SSH.		direct API call to the device.	direct API call to the device.	command to the device through SSH. Directory in the device are /web/conf/server.crt /web/conf/server.key
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Not Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
Services and Prot for AppViewX communication	Port number: 22 (SSH, till R77) and 443 (API, from R80)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH) and 443 (API)
Internet Access/Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are /web/conf/ server.crt /web/conf/ server.key	Certificates are fetched by issuing a direct command to device through SSH.	Not supported	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10 /config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10 /config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Server Pre-requisite

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

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

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

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

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

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

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

Cloud Service Management

Overview

AWS cloud instance has been integrated with AppViewX using SSM, which is an inbuilt agent supported by AWS. In this document, the pre-requisites required for integrating AWS EC2 instances with AppViewX and the basic functionality have been explained.

Supported Vendors

Server	
Linux (OS)	Web Service
Native	AWS
Apache	Y(19.4)
RapidSB	AWS
Generic Linux	Y(19.4)
JBoss	Y(20.1)
MQ Server	Y(20.1)
NGNIX	Y(20.1)
Rabbit MQ	Y(20.1)
My SQL	Y(20.1)
Windows (OS)	Web Service
RapidSB	AWS
Apache	Y(20.2)
Tomcat	Y(20.2)

Prerequisites

The following are the pre-requisites only for the EC2 services. For the other services, we do not have any pre-requisites.

- A dedicated/Shared S3 bucket with R/W and delete access is required.
- SSM should have command execution and document creation access.
- EC2 instances should have a working SSM agent with an EC2 Instance role associated with it for discovery.
- For adding a cloud account we need AWS API keys(Access key/Secret key).
- IAM policy configuration for EC2:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ssm:GetDocument",
        "ssm:CreateDocument"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::name_of_dedicated_bucket_created_for_appviewx"
      ]
    }
  ]
}
```

Note: For the other services, the IAM policy will be shared based on the ask.

Limitation

Only the processes on the Linux platform are supported.

Prerequisites

The following are the pre-requisites only for the EC2 services. For the other services, we do not have any pre-requisites.

- A dedicated/Shared S3 bucket with R/W and delete access is required.
- SSM should have command execution and document creation access.
- EC2 instances should have a working SSM agent with an EC2 Instance role associated with it for discovery.
- For adding a cloud account we need AWS API keys(Access key/Secret key).
- IAM policy configuration for EC2:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ssm:GetDocument",
        "ssm:CreateDocument"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
```

```
        "Resource": [
            "arn:aws:s3:::name_of_dedicated_bucket_created_for_appviewx"
        ]
    }
  ]
}
```

Note: For the other services, the IAM policy will be shared based on the ask.

Limitation

Only the processes on the Linux platform are supported.

Cloud Device Inventory

The cloud device outer inventory displays details (explained in the table below) for all cloud accounts added.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Account Description	Applicable only for a child account, this field displays the following details: • Account type (child) • Master account number • Discovery type: **ROLE_BASED** or **ORGANIZATION_BASED**
Vendor	Cloud device vendor name
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	This field takes the following values:
	• For the master account:
	  • **Managed**
	  • **Failed**

Field	Description

	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. **Note:** The resource discovery status of accounts in this outer cloud inventory list depends on the corresponding status of all its reporting entities listed in the account level inventory here. This field indicates the status of the resource discovery for the discovered accounts using the following values: • **Not started**: Resource discovery for the account is yet to begin **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:**

Field	Description
	• Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for ACM and ELB resources • for all existing devices and child accounts as part of data migration
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. **Note:** The certificate discovery status of accounts in this outer cloud inventory list depends on the corresponding status of all their reporting entities listed in the account level inventory here. Indicates the status of the certificate discovery for the discovered accounts using the following values: • **Not started**: Certificate discovery for the account is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete.

Field	Description
	Note: This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.

AWS

- Prerequisites for Migrating AWS Standalone Accounts from Older Versions
- Adding a New AWS Device
- Configuring Organization Based Discovery
- Configuring IAM Policy Based Discovery
- Configuring Trigger Based Sync
- Configuring Schedule Based Sync
- AWS Standalone Account Onboarding

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important: AWS standalone device migration is supported only from the following versions of CERT+ SaaS: **20.1**, **20.2**, **20.3** - **20.3 FP7**. The following prerequisites are also applicable to only these versions.

Important: AWS device migration **is not** supported from the following versions of CERT+ SaaS: **12.x**, **19.x**, and **21.x**. For these versions, it is recommended that you delete all AWS devices

(both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Note: For customers migrating from versions **20.1.x**, **20.2.x**, and **20.3.6**, we recommend that they delete the following before migration:

- All of their Amazon CA settings
- Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).

Note: For customers migrating from version **20.3.10** (mandatory):

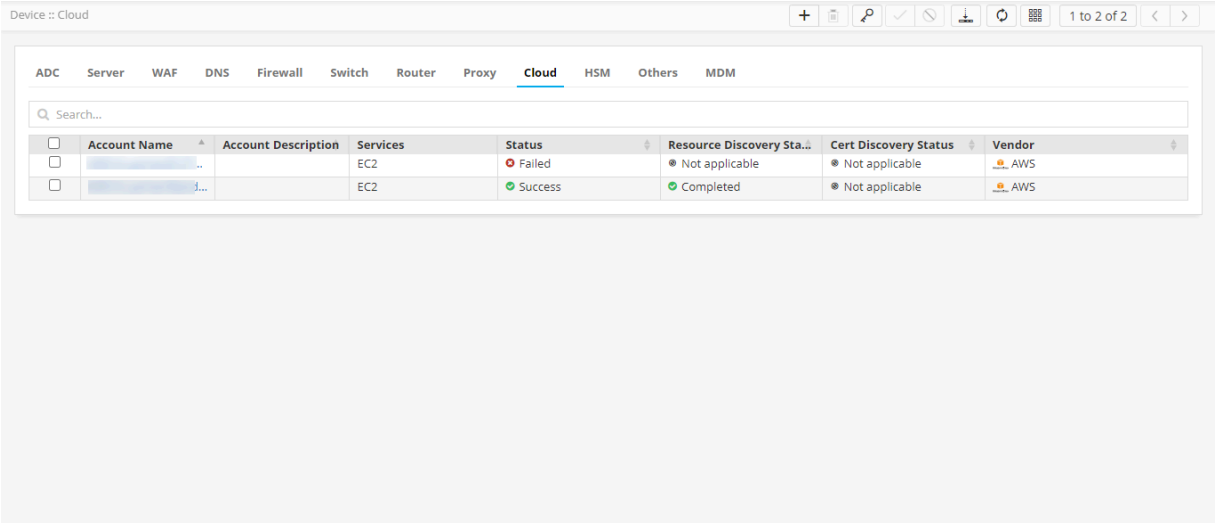
- Delete all of their Amazon CA settings before migration.
- Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the **standalone AWS cloud accounts** migrated from the above listed versions to version **22.1 FP1**:

- For standalone accounts where one of the associated services is not EC2
- For standalone accounts where one of the associated services is EC2

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < 20.3 FP8 to 22.1 FP1, from the top left corner of the AppViewX user interface, click .
2. From the menu displayed, select **Inventory > Device**.
   The **Device :: ADC** page is displayed.
3. From the **Device :: ADC** page, select **Cloud**.
   The **Device :: Cloud** page is displayed.



4. From the device accounts listed under **Account Name**, select the migrated standalone accounts (as required).

> **Troubleshooting:** If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.

5. From the top-right corner of the **Device :: Coud** page, click the 

icon.
This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in 22.1 FP1.

For standalone accounts where one of the associated services is EC2

In versions 20.1/20.2/20.3-20.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In 22.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

> **Note:** For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

Before Migration

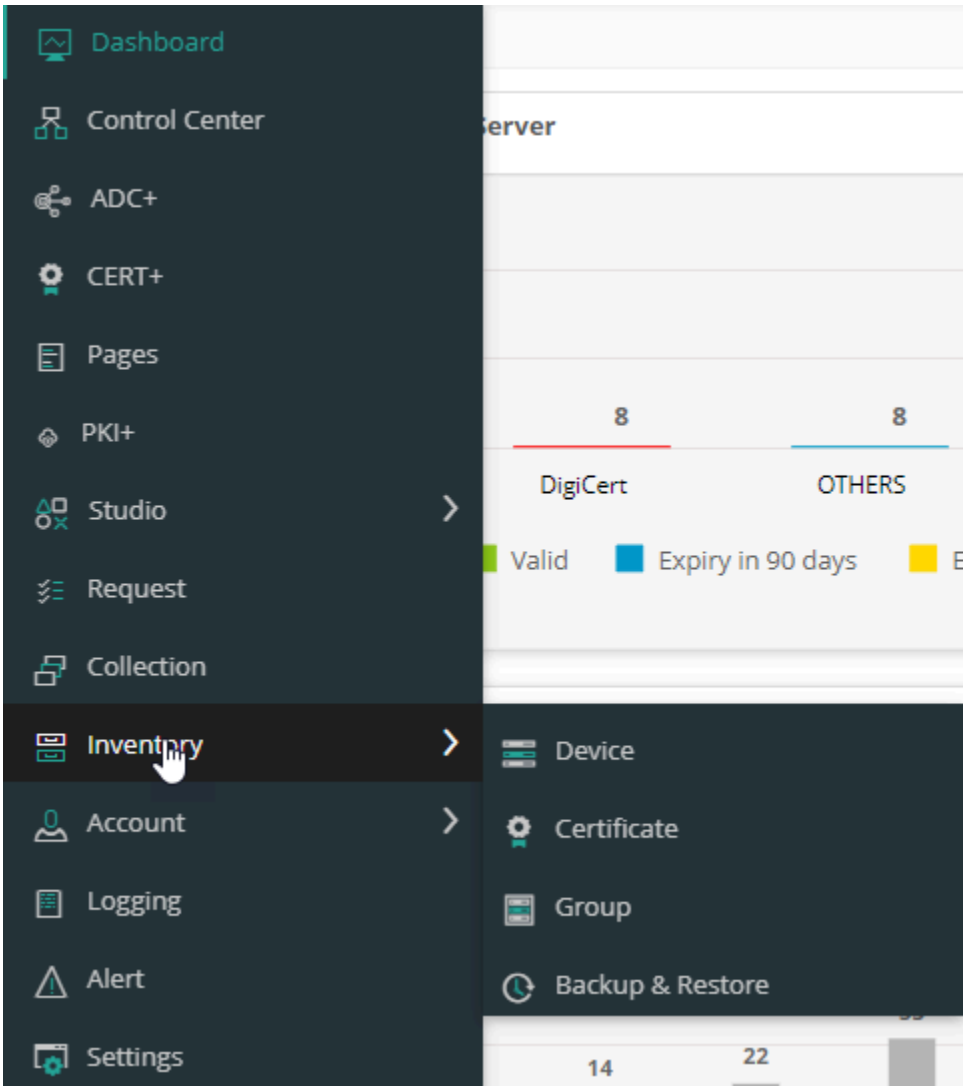
Merge permissions from all individual buckets into any one S3 bucket.

After Migration

1. Select a migrated standalone account from the **Device :: Cloud** page.
   The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
4. Click **Add**.
5. Click **Save**.
   Fetch Config is automatically triggered and the account details are upgraded according to the latest version

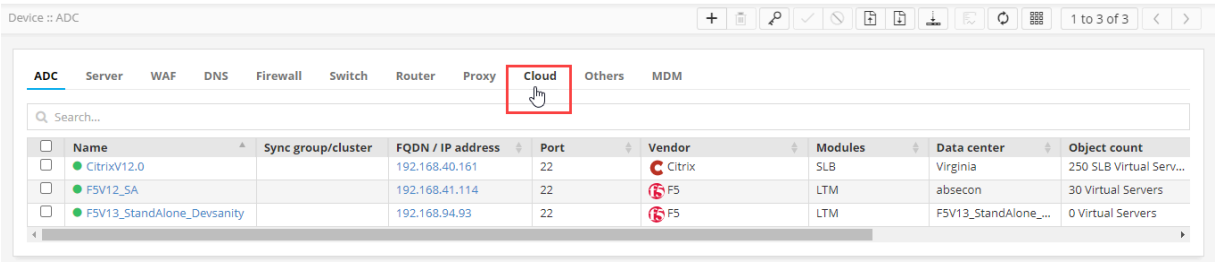
Adding a New AWS Device

1. Login to AppViewX.
2. From the top left corner of the screen, click ☰.
3. From the menu displayed, select **Inventory** > **Devices**.

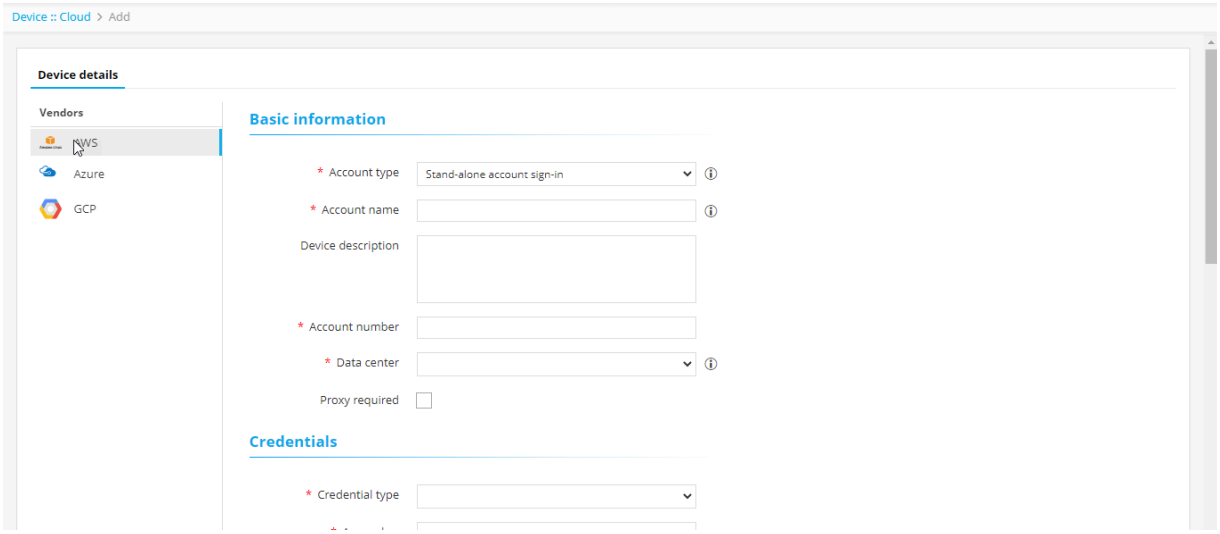


The **Device :: ADC** page is displayed.

4. To navigate to the cloud device inventory, click **Cloud**.



5. On the **Device :: Cloud** > **Add** page, from the list of Vendors, select **AWS**.



6. Enter/Select the following **Basic information**:

Field	Description
Account type*	From the dropdown list, from the following options, select the customer's AWS account type: • **Stand-alone account sign-in**: The user account and the resources are available in the same account. • **Cross account sign-in**: Resources are available across multiple accounts and users are given role-based access.
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Account number*	Enter the customer's AWS account number.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox.

7. Enter/Select the following **Credentials**-related information:

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account)
Access key*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.

8. Enter/Select the following details for the **Amazon Cloud Service Settings**:

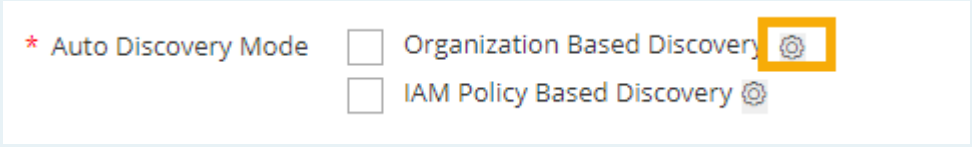
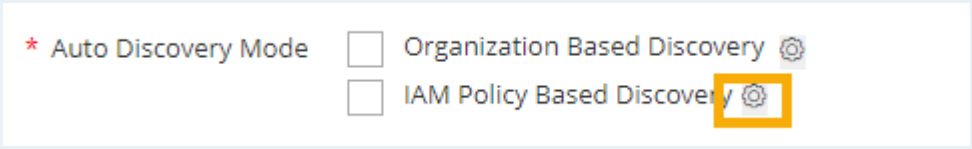
Field	Description
Services*	According to the type of the new cloud device being added, select the corresponding Amazon Cloud Service for the device.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.

Field	Description
Service region*	Service regions are regions that are supported by the selected service. From the dropdown list, select the service regions that should be scanned for certificates. **Note:** To be able to fetch and select from the available regions, ensure that the credentials have been provided in the **Credentials** section.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.

9. In the **Discover Resources** section, enter/select the following details:

Note: This section is displayed instead of the **Amazon Cloud Service Settings** section if the **Account Type** is C**ross or Federated**.

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	Select the auto discovery mode from the following options:

Field	Description
	• **Organization Based Discovery**: On selecting this option, the **Organization based discovery** popup window is displayed. For instructions on configuring organization based discovery, click here. **Tip:** An alternate way to access the **Organization based discovery** popup window is by clicking ⚙, located as shown in the image below:  • **IAM Policy**: On selecting this option, the **IAM Policy based discovery** popup window is displayed. For instructions on configuring IAM policy based discovery, click here. **Tip:** An alternate way to access the **IAM Policy based discovery** popup window is by clicking ⚙, located as shown in the image below:  **Note:** You can select one or both auto-discovery modes.
Service*	From the **Select the Service(s)** dropdown list, select the services required for the CLM operations. **Tip:** To select all services, select the **Select all** check box displayed at the beginning of the list of services. **Note:**

Field	Description
	• When **ACM (Certificate Authority)** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Certificate Authority Service**to configure the ACM services. These fields are explained in the table in Step 10. • When **Amazon Private CA** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Private CA**. These fields are explained in the table in Step 11. • When the **EC2(EC2 Instance)** service is selected, an additional set of fields is displayed to configure the EC2 services. These fields are explained in the **EC2 Services** table in Step 7.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)

10. In the **ACM Certificate Authority Service** section, enter/select the following details:

Note: This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected. From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.

11. In the **ACM Private CA** section, enter/select the following details:

Option	Description
Field	**Description**
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • ACM Private CA • AWS Certificate Manager (ACM)
S3 Bucket*	**NOTE**: This field is displayed only when the **ACM Private CA** operation mode is selected. a. Enter the S3 bucket name. b. Click .

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
The ARN Advanced Settings action pane is displayed.

c. In the ARN Advanced Settings action pane, enter the following details:

s

Table 1.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:</td></tr>
</table>
</td></tr>
</table>

Option	Description

Field	Description
	• **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.
The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
</table>

12. In the **EC2 Services** section, enter/select the following details:

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.
S3 Deployment Type*	From the dropdown list, select the deployment type for the S3 bucket.
S3 Bucket Name*	a. Click  . The **ARN Advanced Settings** action pane is displayed. b. In the **ARN Advanced Settings** action pane, enter the following details:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming.</td></tr>
<tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:
a. In the Enter Key field, enter a key for the key-value pair.
b. In the Enter Value field, enter a value for the key-value pair.
c. Click Add.

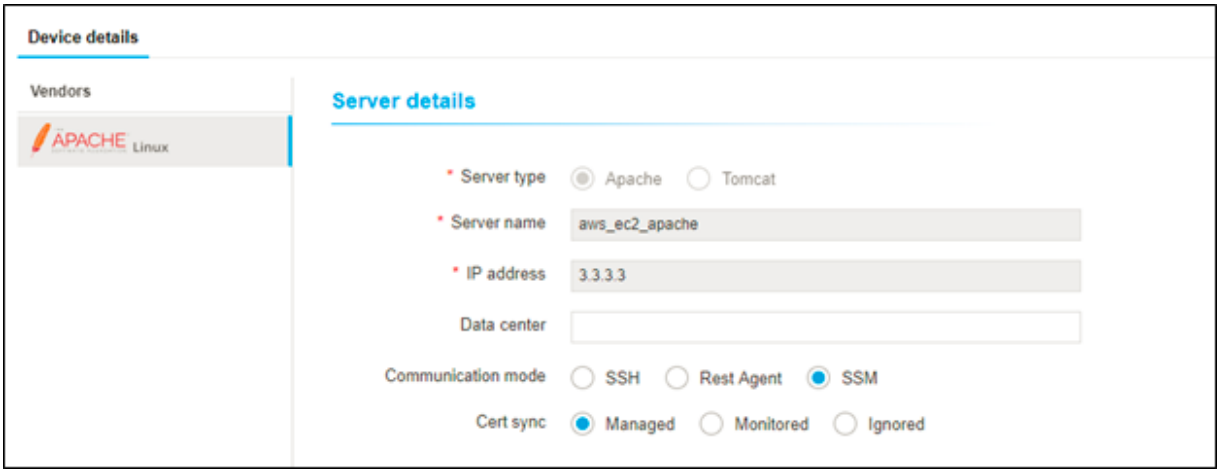
The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
</table>

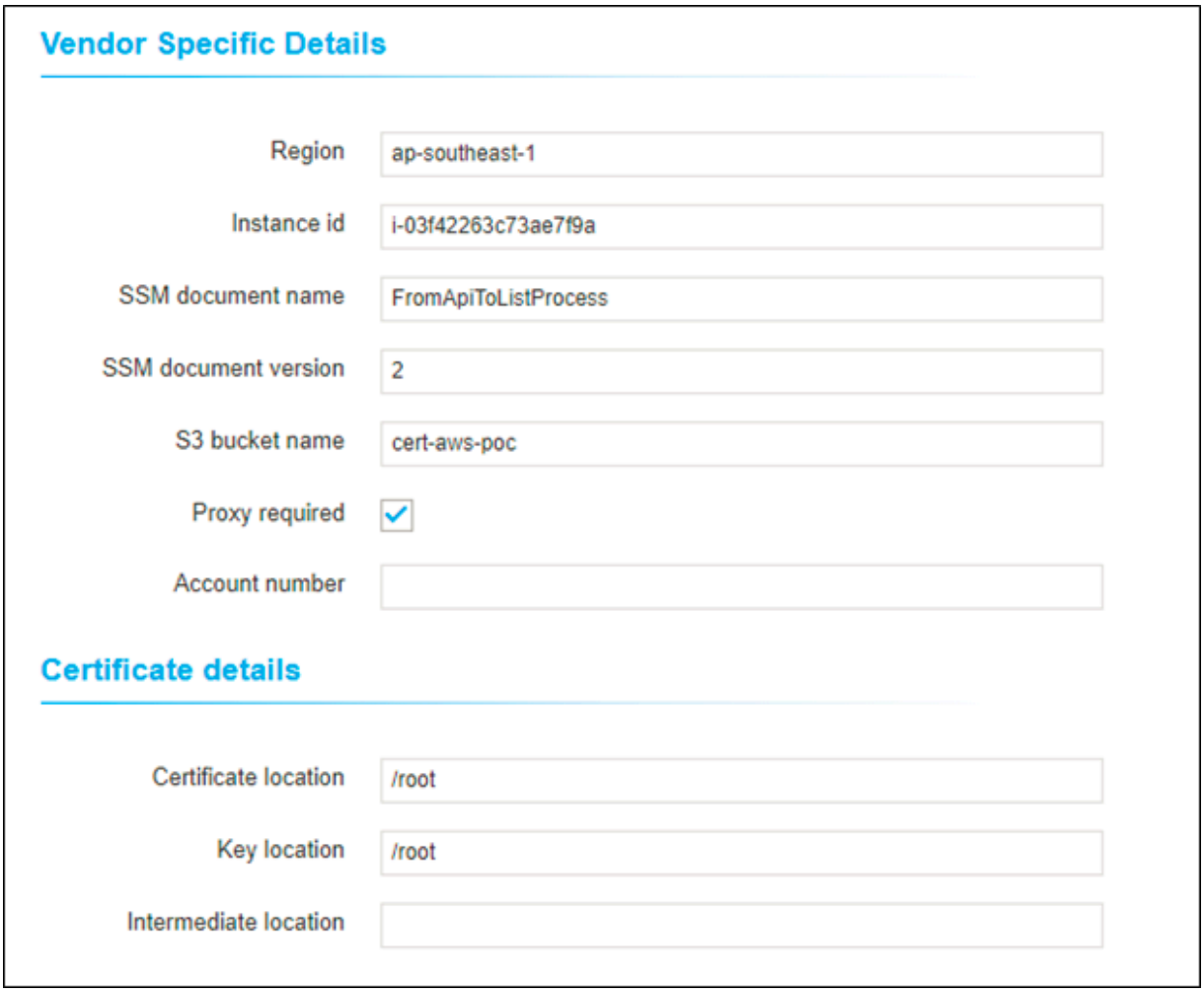
13. To add the new device to the cloud device inventory, click **Add**.

> **Tip:** To select multiple services for a device, after you click **Add**, go back to the **Services** dropdown list and select the next service you want to enable for the device. Enter/select the rest of the details and click **Add**. Repeat this process for as many services you want to enable for the new device. The table is populated with a separate entry for each service.

Details of the added cloud device are displayed in the inner inventory table at the bottom of the page. The details captured in the inner inventory are explained here.

14. After enabling all the services for the new device, click **Save**.
    - On saving the device, through SSM, AppViewX will communicate with EC2 instances through SSM.
    - AppViewX will discover the processes from these instances and manage them in the Server device inventory.





Once all the details are entered, you can add them to the Apache Linux server.

Note: Apart from the Apache and Tomcat processes vendor, the rest of the processes will be managed in the server inventory only as "Generic Linux".

• Account Level/Inner Inventory

Account Level/Inner Inventory

Field	Description
Account Name	Name of the account to which the cloud device belongs

Field	Description
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

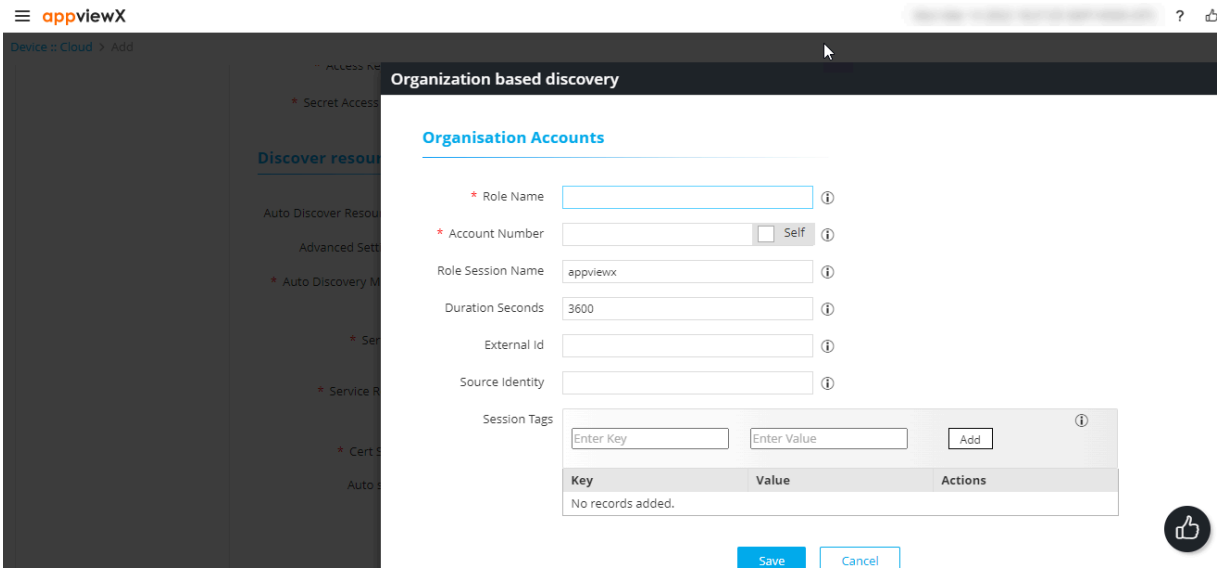
Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**.

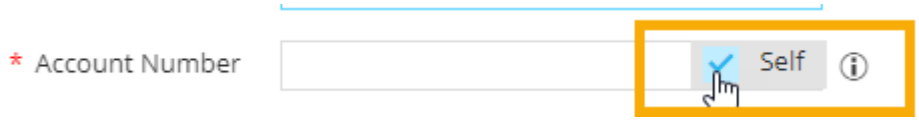
Field	Description
	Note: This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for ACM and ELB resources • for all existing devices and child accounts as part of data migration
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**.

Field	Description
	• **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the following details:



Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.

Field	Description
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. In the **Child Accounts** section, enter/select the following details:

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions:

Field	Description
	• **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

3. Click **Save**.

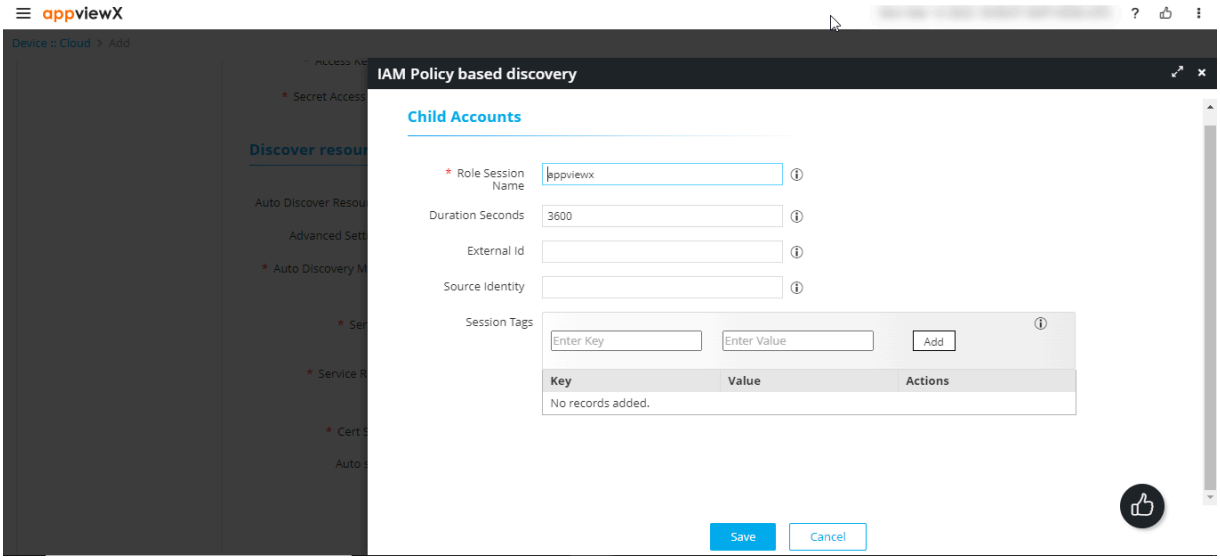
   The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window, under **Child Accounts**, enter/select the following details:



Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

Field	Description
	To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

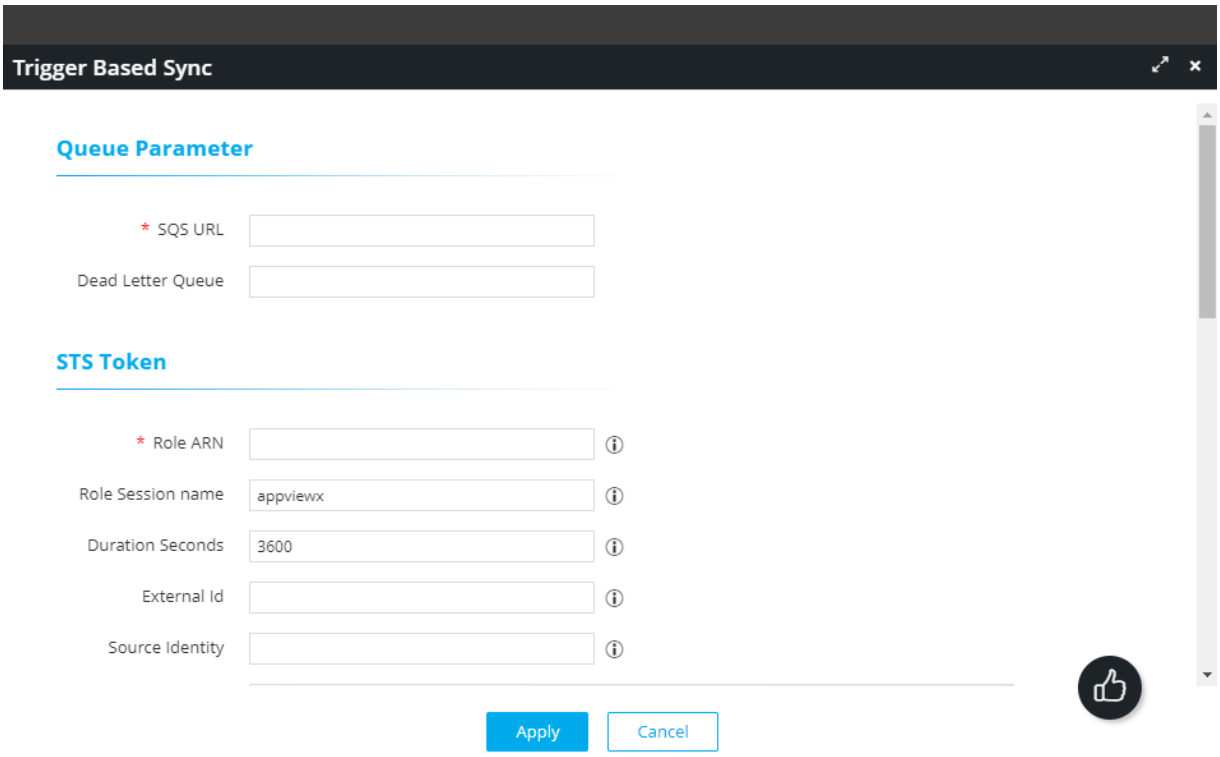
   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.

   The **Trigger Based Sync** popup window is displayed.



2. In the **Queue Parameter** section, enter the following details:

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.

3. In the **STS Token** section, enter/select the following details:

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.

Field	Description
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

4. In the **SQS Attributes** section, enter/select the following details:

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.

Field	Description
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.

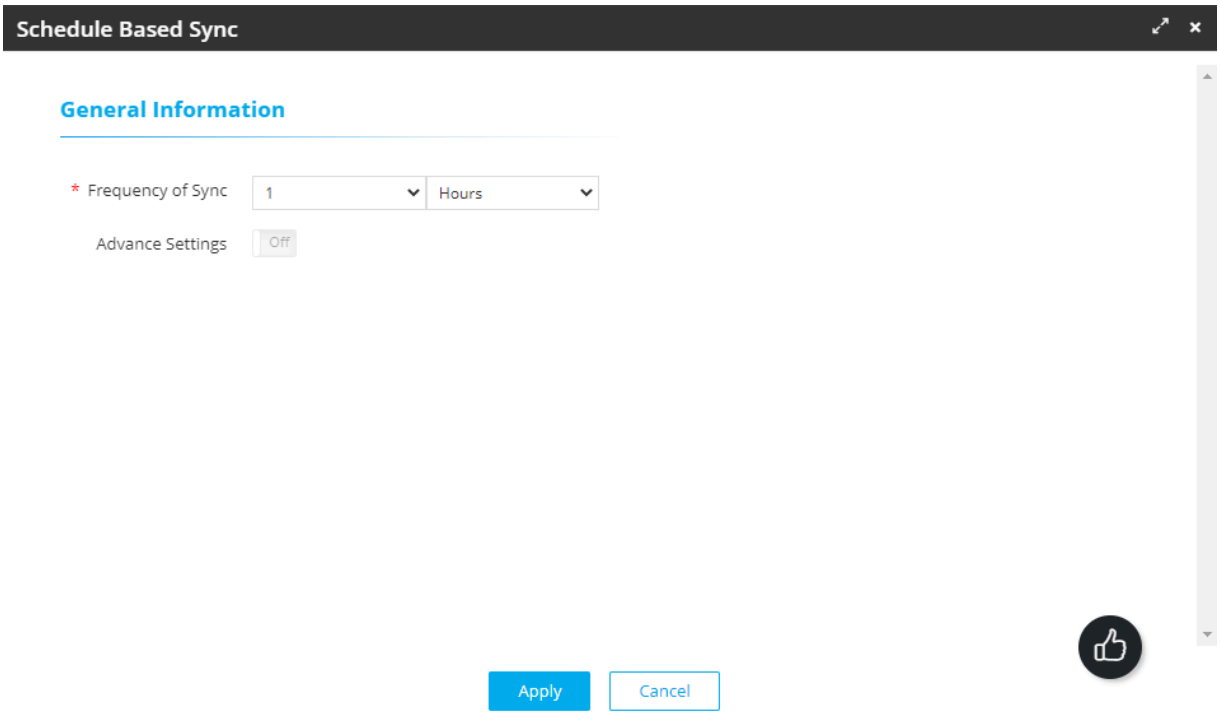
5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.



2. In the **General Information** section, select the following details:

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**. 
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.

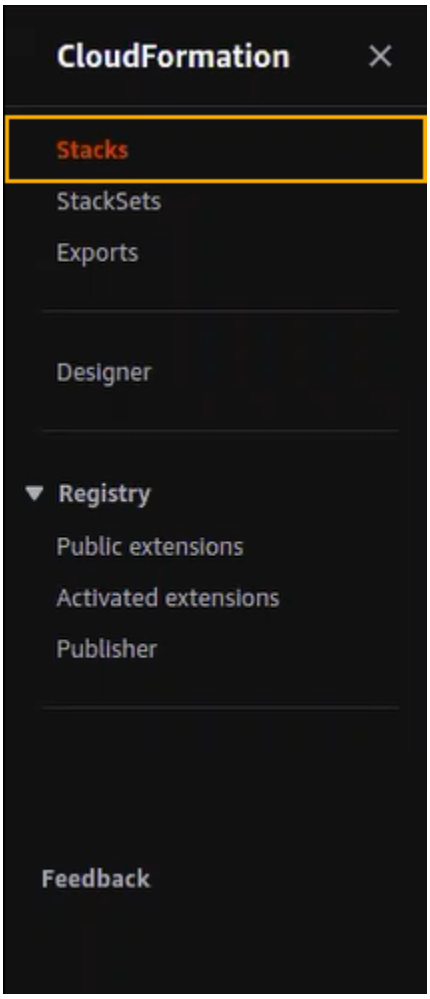
3. Click **Apply**.

AWS Standalone Account Onboarding

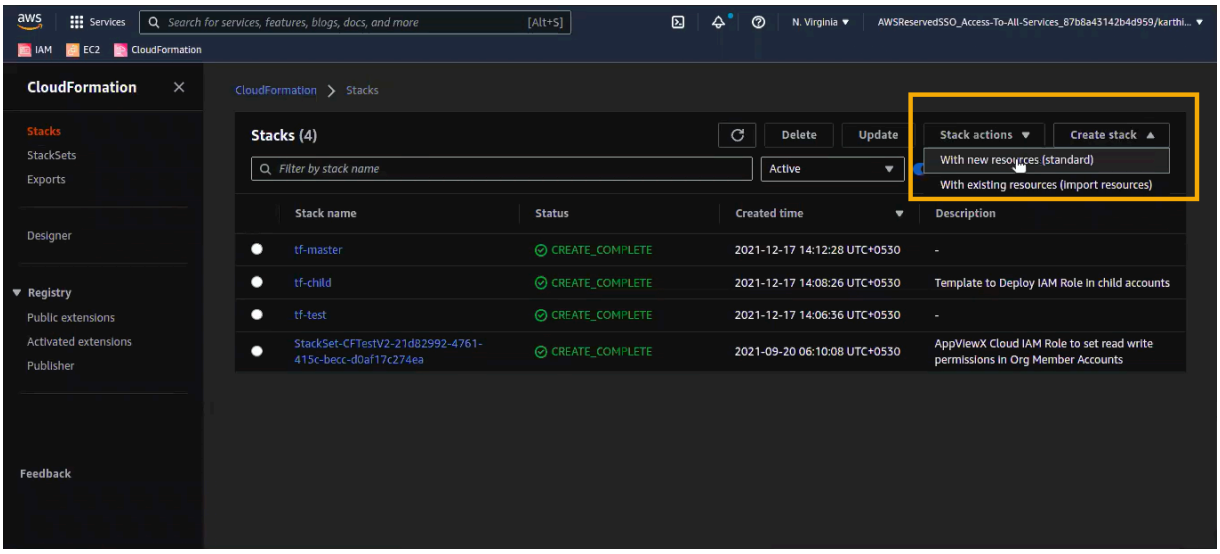
The process of onboarding a standalone account through a cross or federated account access involves the following steps:

Step 1: Creating an S3 bucket using the Cloudformation template

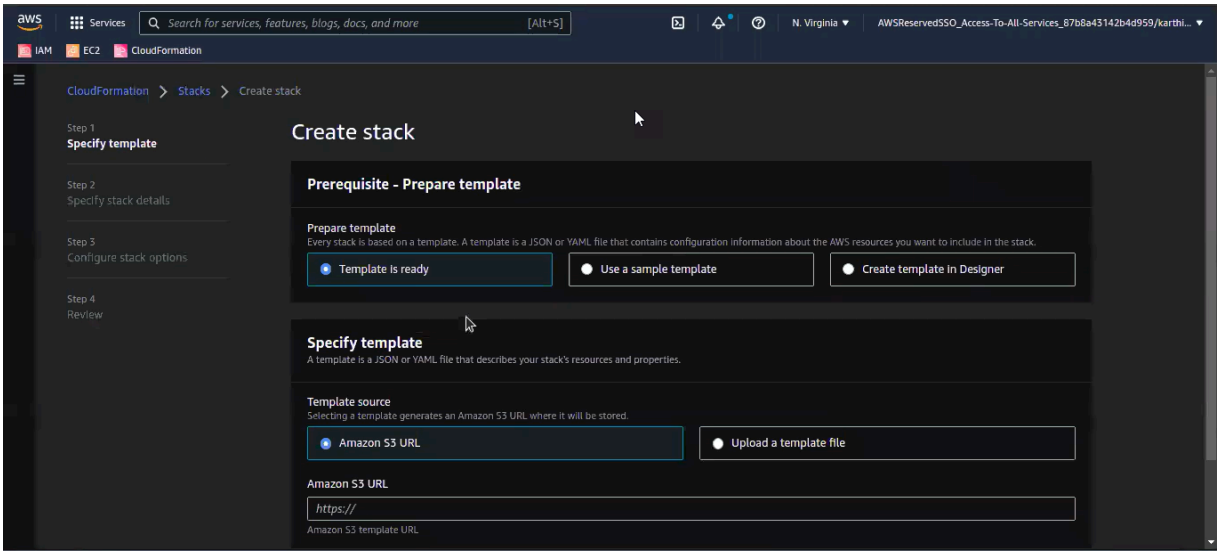
1. Login to the AWS account and navigate to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.



3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

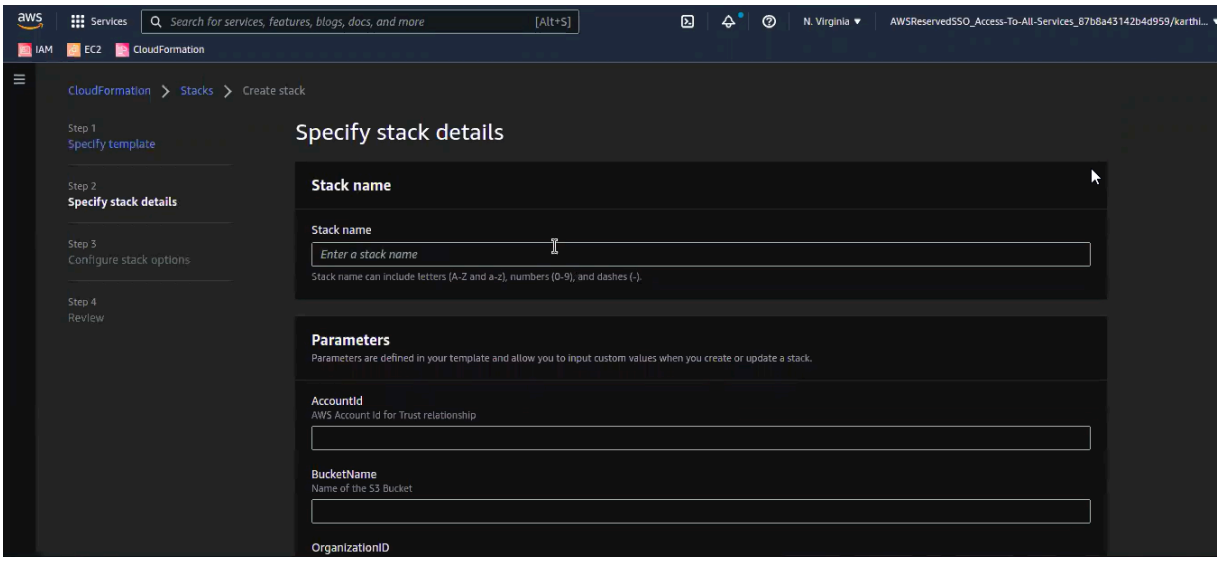


The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.



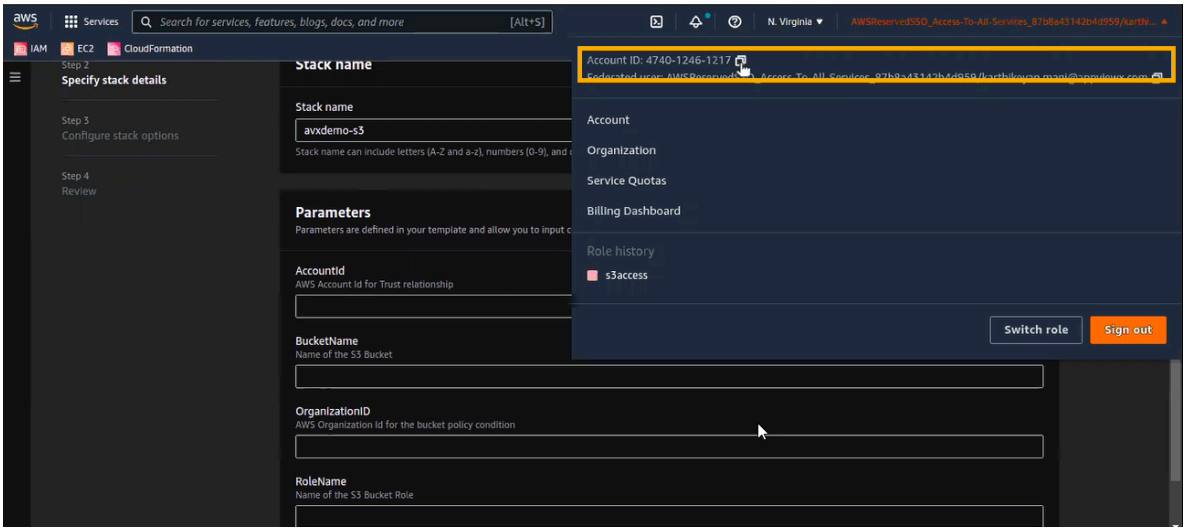
4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:
   a. For **Template source**, select **Upload a template file**.
   b. To **Upload a template file**, click **Choose file**.
   c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
   d. Select the **S3Bucket.yaml** file and click **Open**.
6. Click **Next**.

The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.



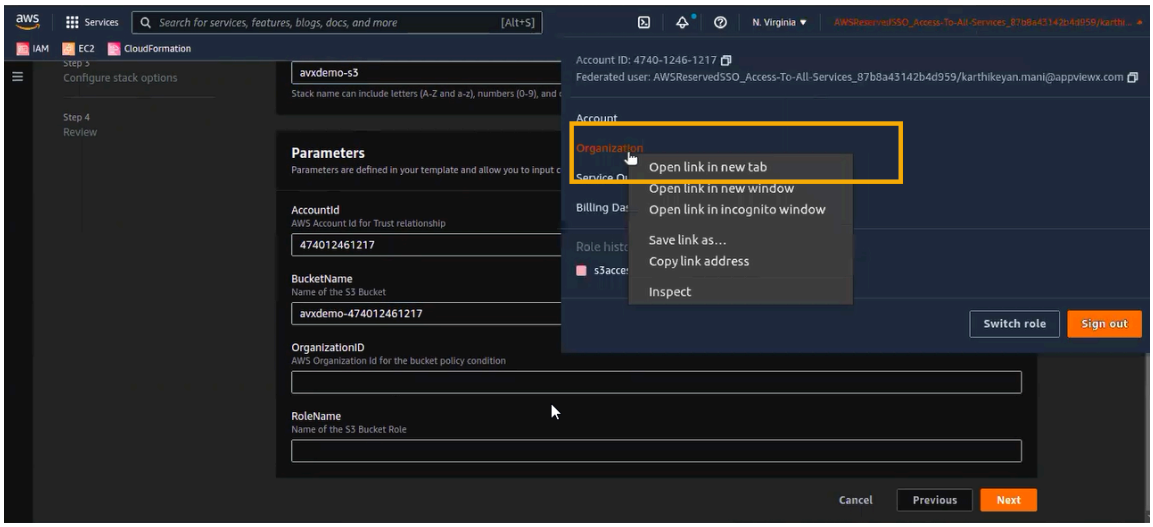
7. Enter a **Stack name**. For the purpose of this guide, we will name this stack **avxdemo-S3**.
8. In the **Parameters** section, enter the following details:

   a. **AccountId**: From the top-right corner of the screen, click your username and copy the account ID displayed.



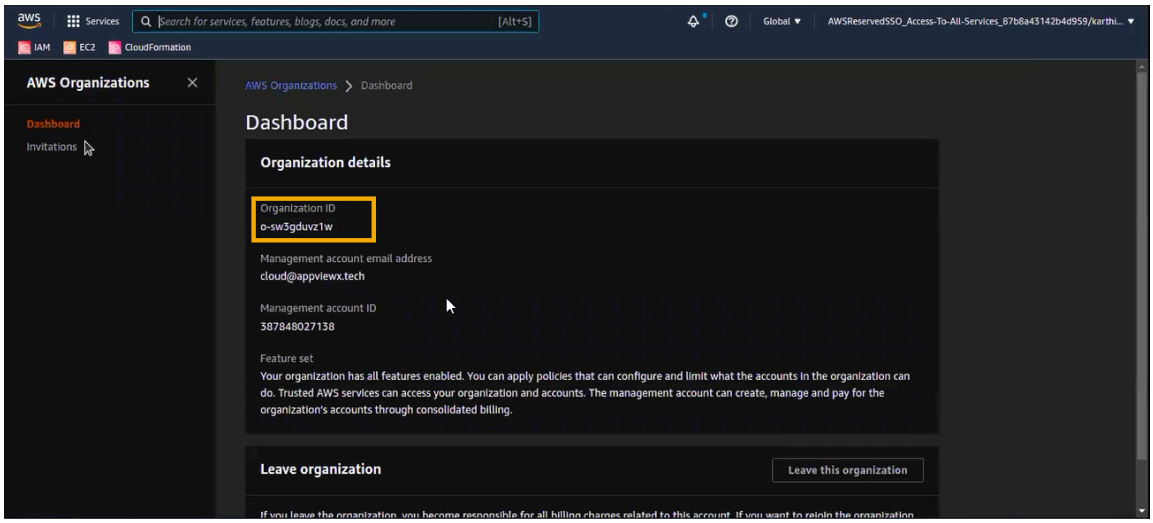
   b. **BucketName**: Enter a name for the S3 bucket that will be created in the backend. Recommended format to name the S3 bucket: **avxdemo-<account ID>**.

   c. **OrganizationID**:
      i. From the top-right corner of the screen, click your username.
      ii. From the menu displayed, right click **Organization** to open it in a new tab.



The **Dashboard** is displayed.

iii. From the **Dashboard**, copy the organization ID and paste it into the **OrganizationID** field.

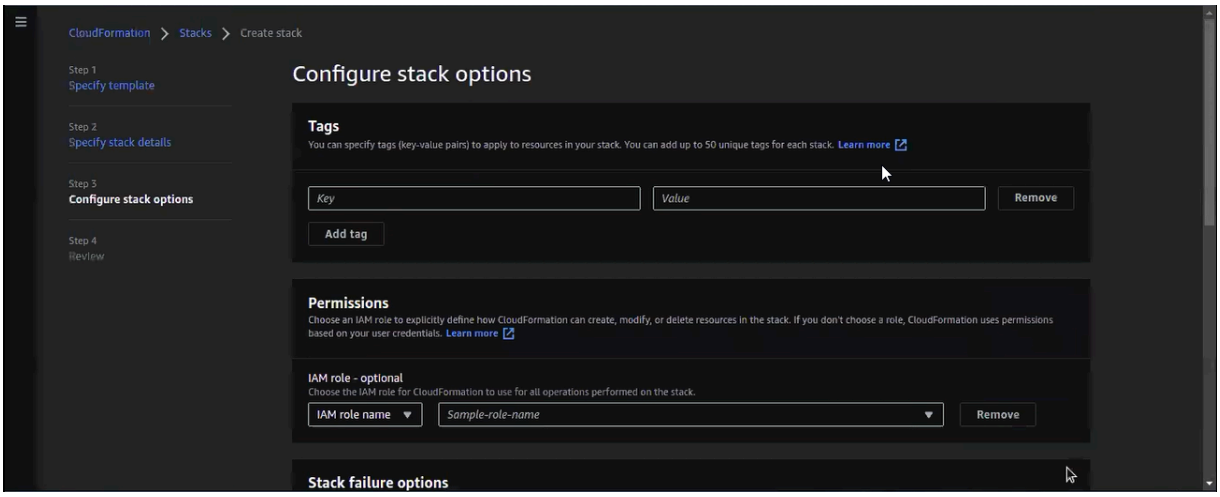


Note: The organization ID is a mandatory entry for the CloudFormation template.

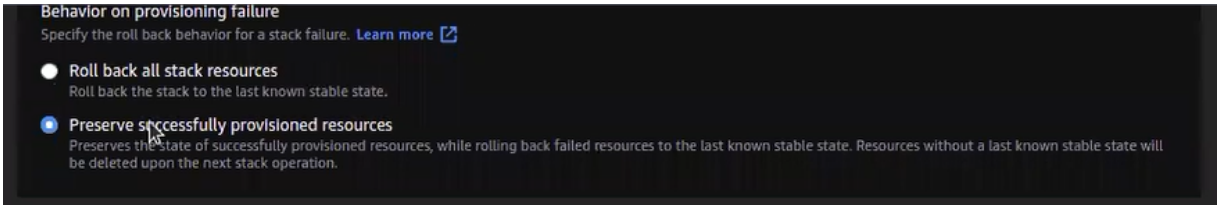
d. **RoleName**: Enter a name for the S3 bucket role. For the purpose of this guide, the S3 bucket role will be called **avxdemos3bucketrole**.

The details entered on the **Specify stack details** page will be used to create a bucket policy for the S3 bucket we created for the AWS account. This bucket policy can be customized later based on customer preferences for how they want to secure their infrastructure.

9. Click **Next**.
   The **Configure stack options** page (step 3 of the stack creation process) is displayed.

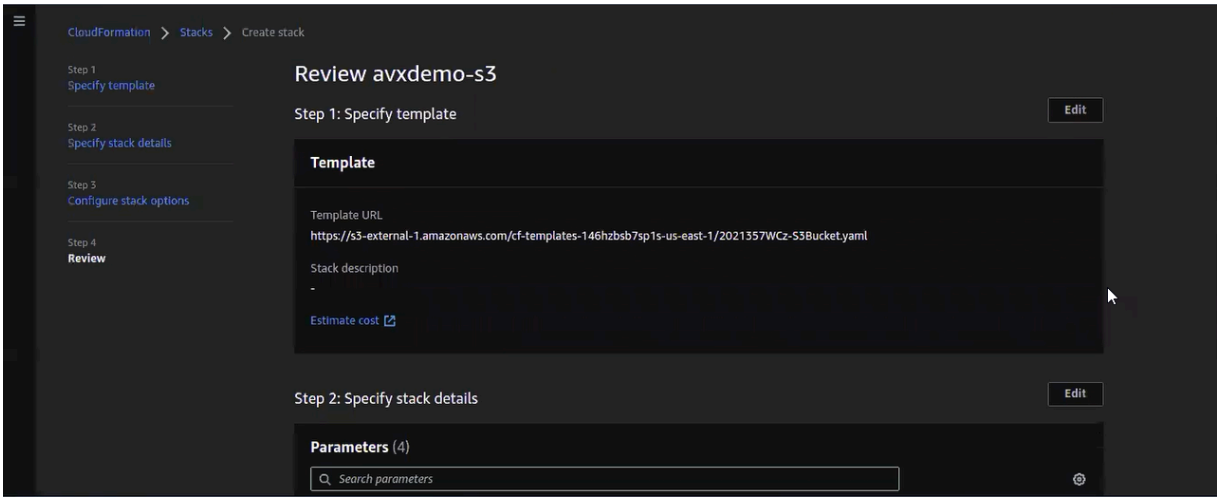


10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.

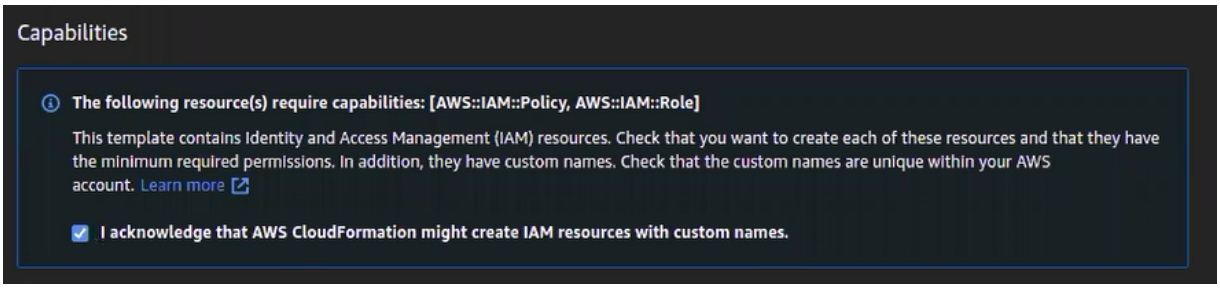


11. Click **Next**.

    The **Review <stack name>** page (step 4 of the stack creation process) is displayed



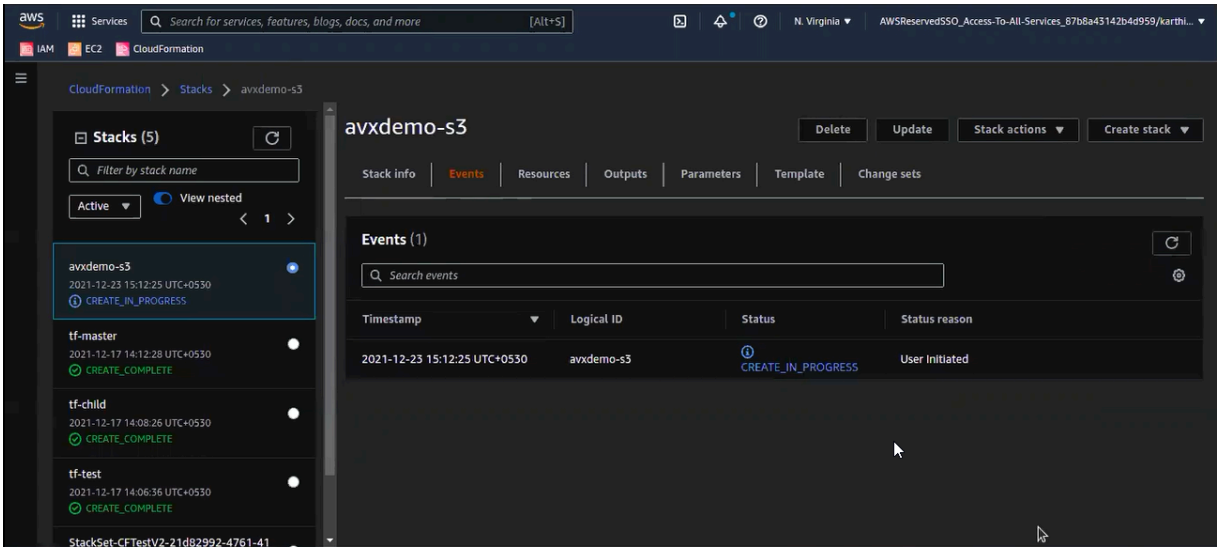
12. On the **Review <stack name>** page, scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.



13. Click **Create stack**.

    The **<stack name>** page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    a. **Stack info**
    b. **Events**
    c. **Resources**
    d. **Outputs**
    e. **Parameters**
    f. **Templates**
    g. **Change sets**

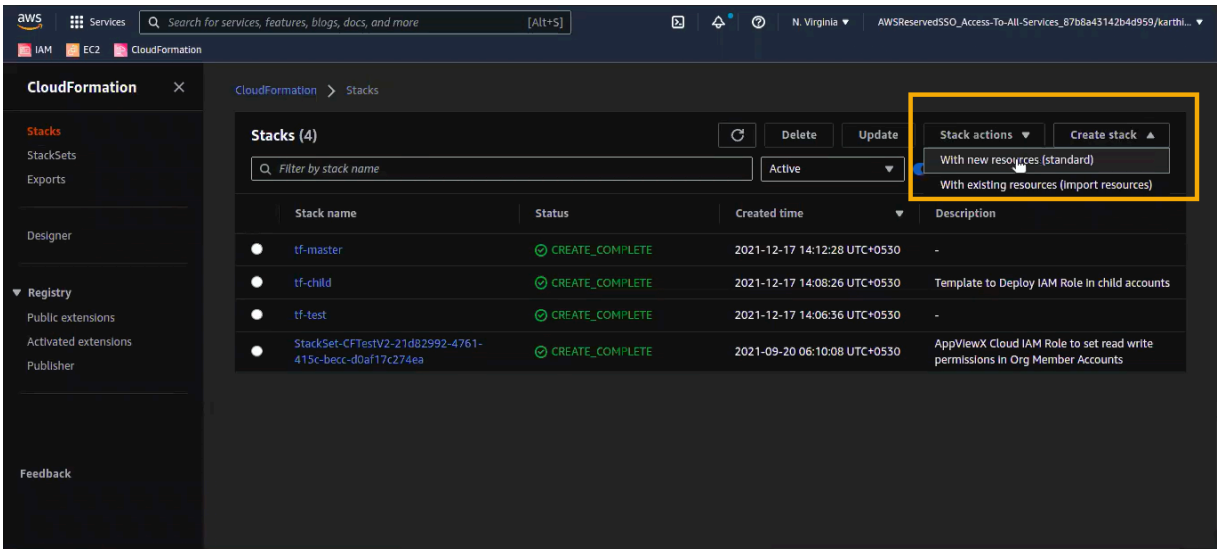


    When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**. This means that, in the backend, an S3 bucket as well as the roles required to provision the bucket have been created. The bucket policy for the S3 bucket has also been updated accordingly.

14. Navigate to the **Parameters** tab and note the bucket name to use it in the CloudFormation template for the master account.

Step 2: Creating a child account using the CloudFormation template

1. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.



   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.

2. From the navigation pane on the left, click **Step 2 Specify stack details**.
   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.
3. Enter a **Stack name**. For the purpose of this guide, we will name this stack **avxdemoc1**.
4. In the **Parameters** section, enter the following details:
   a. **MasterAccountNumber**: From the top-right corner of the screen, click your username and copy the account ID displayed. Paste it in the **MasterAccountNumber** field.
   b. **S3BucketName**: Enter the S3 bucket name copied from the **Parameters** tab of the **avxdemo-S3** stack.
5. Click **Next**.

   The **Configure stack options** page (step 3 of the stack creation process) is displayed.

6. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
7. Click **Next**.

   The **Review <stack name>** page (step 4 of the stack creation process) is displayed.

8. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.

9. Click **Create stack**.

   The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

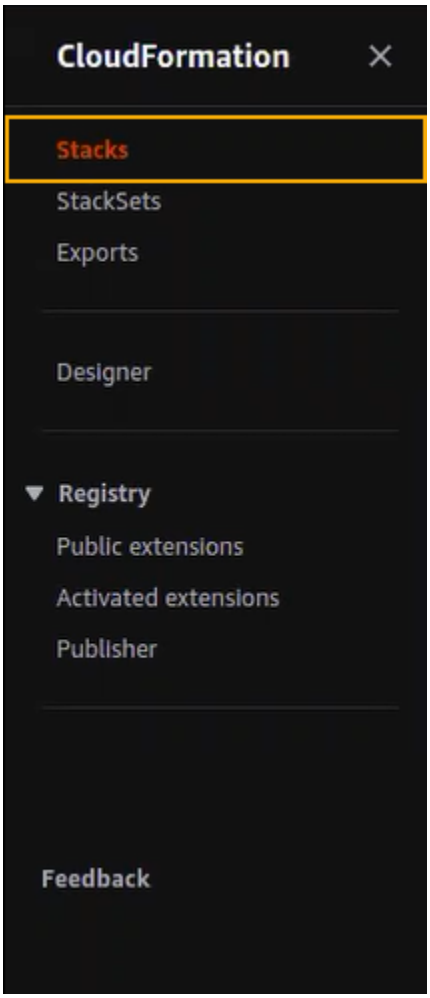
   a. **Stack info**
   b. **Events**
   c. **Resources**
   d. **Outputs**
   e. **Parameters**
   f. **Templates**
   g. **Change sets**

   When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**.

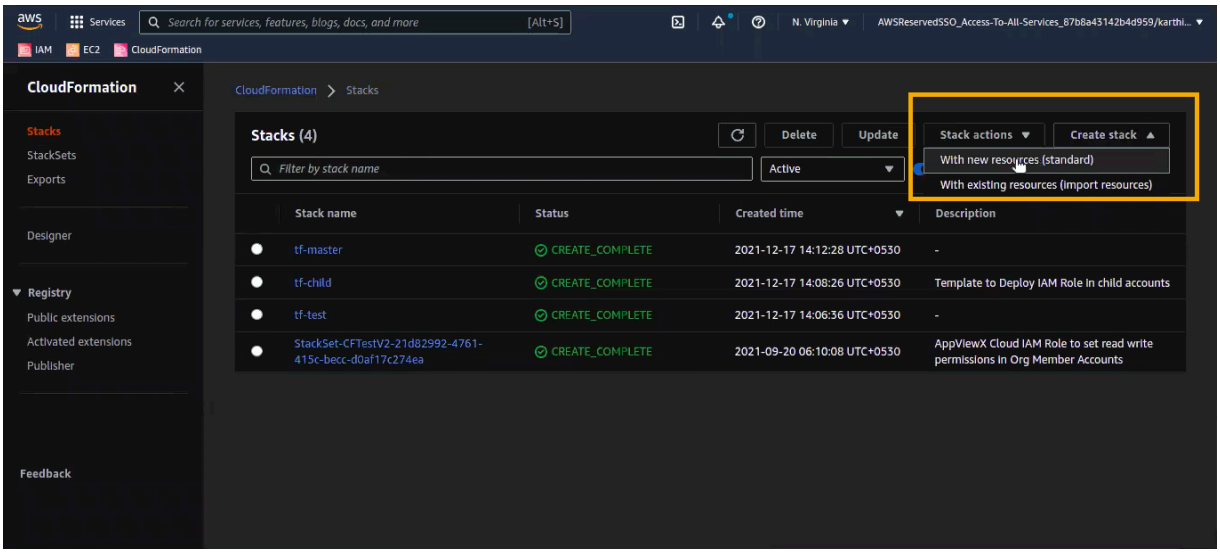
10. Navigate to the **Resources** tab for the **avxdemoc1** stack.
    You will see that a policy called **AppViewXCLM** has been created. This policy will have all the permissions and prerequisites required for AppViewX to discover all the ACM, ELB, and EC2 instances.
11. Navigate to the **Outputs** tab for the **avxdemoc1** stack.
    Note down the **ChildRoleARN** to use it in the CloudFormation template for the master account.

Step 3: Creating a master account using the CloudFormation template

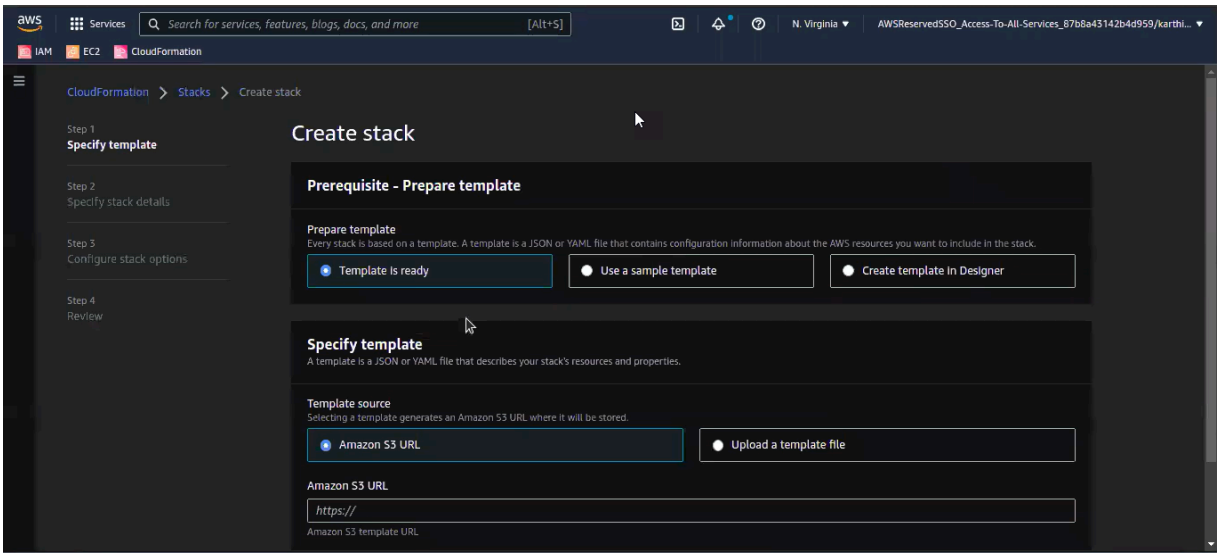
1. Navigate to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.



3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

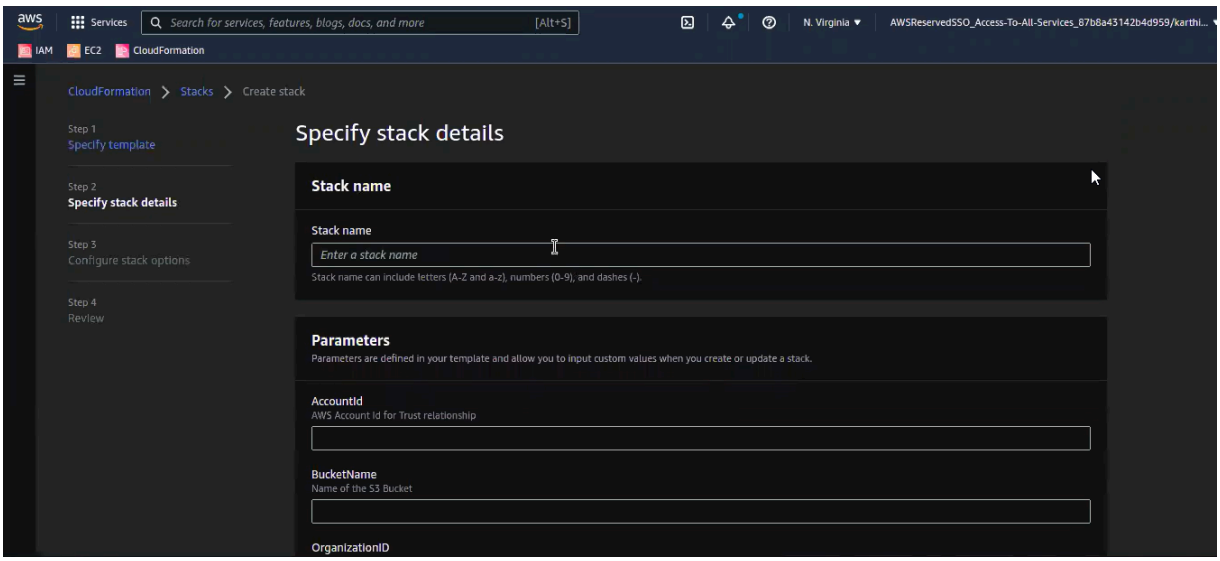


The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.



4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:
   a. For **Template source**, select **Upload a template file**.
   b. To **Upload a template file**, click **Choose file**.
   c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
   d. Select the **master_account.yaml** file and click **Open**.
6. Click **Next**.

The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.



7. Enter a **Stack name**. For the purpose of this guide, we will name this stack **avxdemom1**.
8. In the **Parameters** section, enter the following details:

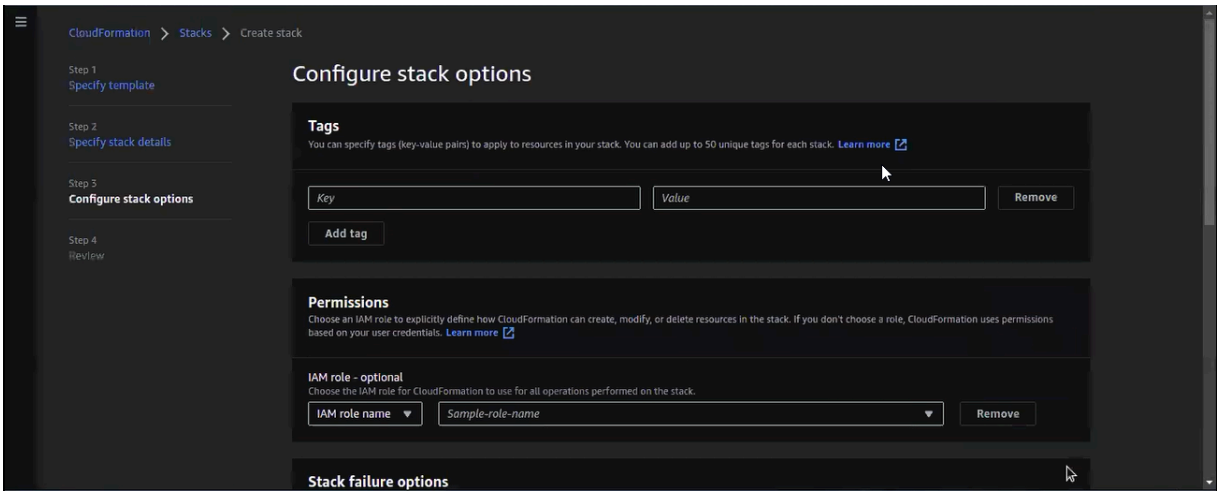
   a. For **ApplyAssumeRoleForAll**, from the dropdown list, select **False**.

   b. From the **Outputs** tab of the **avxdemoc1** CloudFormation template for the child account, copy the **ChildRoleARN** and paste it in the following fields:
   - **ChildRoleARN**
   - **OrganizationRoleARN**

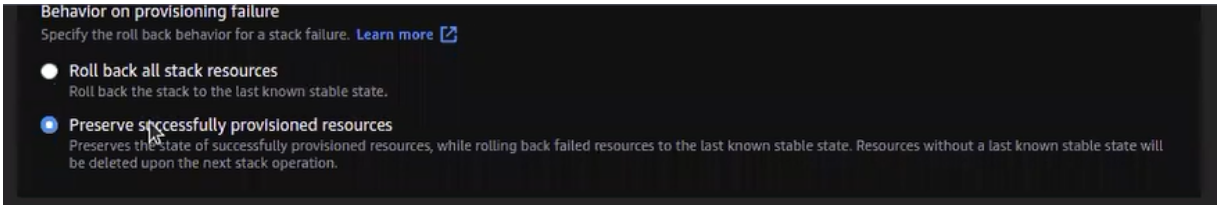
   c. From the **Outputs** tab of the **avxdemo-S3** CloudFormation template, copy the **S3BucketAssumeRole** and paste it in the following fields:
   - **S3BucketRoleARN**
   - **SQSRoleARN**

   d. In the **UserName** field, enter a username for the IAM account. For the purpose of this guide, the username will be set to **avxdemo-user**.

9. Click **Next**.
   The **Configure stack options** page (step 3 of the stack creation process) is displayed.

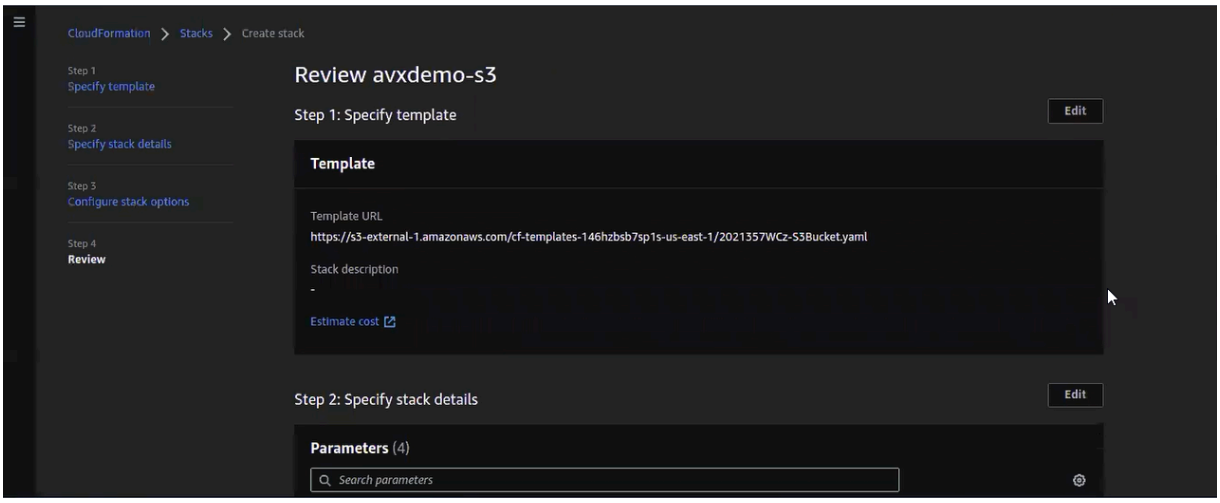


10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.

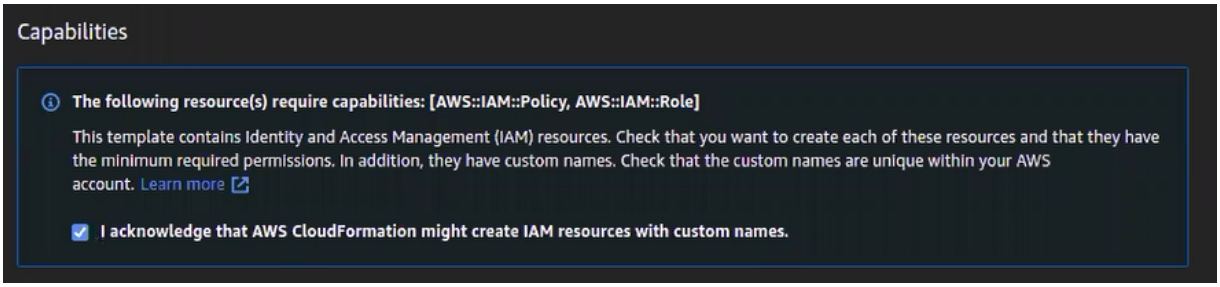


11. Click **Next**.

    The **Review <stack name>** page (step 4 of the stack creation process) is displayed



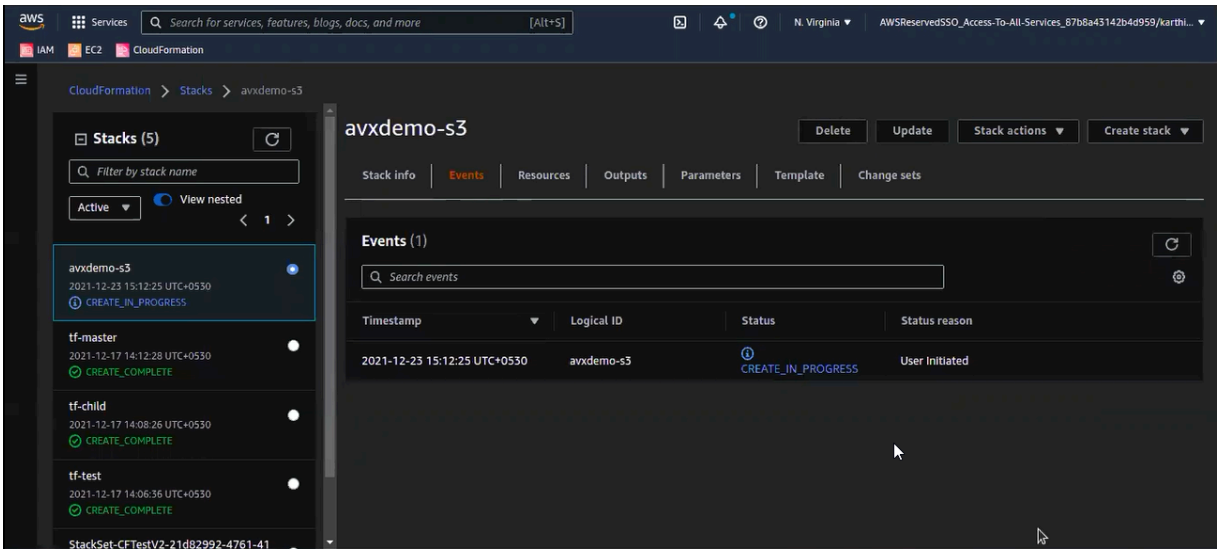
12. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.



13. Click **Create stack**.

    The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    a. **Stack info**
    b. **Events**
    c. **Resources**
    d. **Outputs**
    e. **Parameters**
    f. **Templates**
    g. **Change sets**



14. From the **Outputs** tab of the stack, note the access key and the secret key information to use in AppViewX.

Step 4: Mapping EC2 roles to a customer's EC2 instances

The EC2 role created using the CloudFormation template with the naming convention **<Stack_Name>-Ec2RoleForSSM** must be mapped to the EC2 instances. This mapping is required for enabling SSM communication between the instances and AppViewX and for enabling access to the S3 buckets to store the SSM run command response.

Step 5: Testing Onboarding in the AppViewX Environment

1. Login to AppViewX.
2. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **AWS**.
3. Enter the following **Basic information**:

Field	Description
Account type*	From the dropdown list, select **Cross or Federated**.
Account name*	Enter the account name, **avxdemo**.
Account number*	Enter the AWS account number.

Field	Description
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for the communication, select this checkbox.
Default Region*	From the dropdown list, select a default region for the API communication.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

4. Enter the following **Credentials** details:

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry** (to manually enter the access and secret key for the customer's AWS account) **Credential List - CyberArk** (to automatically retrieve the customer's AWS key details from CyberArk)
Access key*	Copy the **AccessKey** from the **Outputs** tab of the **avxdemom1** template.
Secret key*	Copy the **Secret Access Key** from the **Outputs** tab of the **avxdemom1** template.

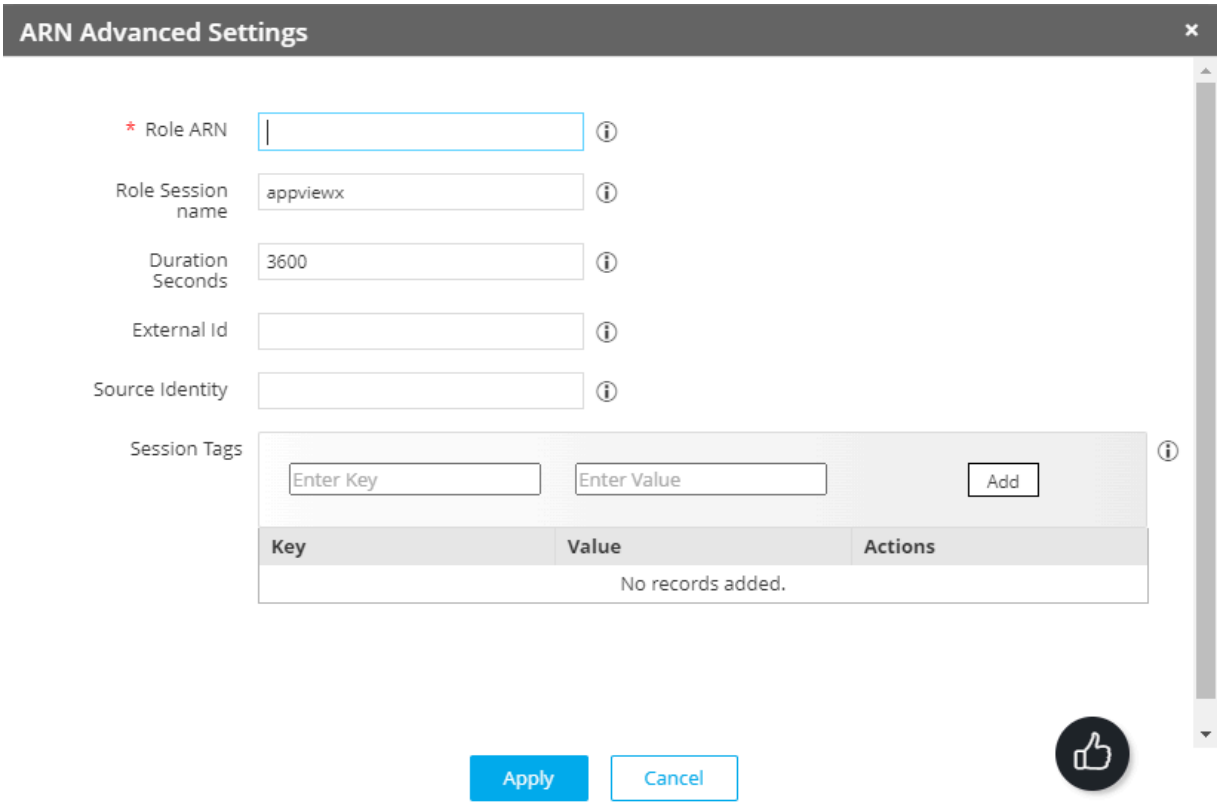
5. Enter the following details for the **Discover resources**:

Field	Description
Auto Discover Resources*	By default, the **Auto Discover Resources** toggle key is set to **ON** and is non-editable. Enabling this feature allows discovering all the cross or federated/child accounts for the provided master account details.
Advanced Settings*	By default, the **Advanced Settings** toggle key is set to **ON** and is non-editable. This feature allows customizing the auto discovery process.
AutoSync	To enable automatic synchronization, enable this toggle.

Field	Description
Auto Discovery Mode*	Select the **IAM Policy**.
Services*	Select the ACM, ELB, and EC2 services (and their subservices)
Service region*	For the purpose of this solution guide, click Fetch Region and select the regions US East (N. Virginia) and US West (N. California).
Route53 Zone Auto Approval*	To support DNS validation as an automatic process, turn on the **Route53 Zone Auto Approval** toggle.
Cert sync	Select one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • Minimum: 900 seconds (15 minutes) • Maximum: 129,600 seconds (36 hours) • Default: 3600 seconds (1 hour)
Role Session name*	**Role Session name** is an identifier for the assumed role session. Use the **Role Session name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons. By default, the **Role Session name** is set to **appviewx**.
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account. For the purpose of this guide, external ID is undefined.

Field	Description
Source Identity	The source identity is specified by the principle that is calling the **AssumeRole** operation. For the purpose of this guide, source identity is undefined.
Session Tags	Enter the key-value attribute pairs required when assuming an IAM role or federating a user in the AWS STS.

6. In the **EC2 Services** section, copy the **S3Bucket Name** from the **Resources** tab of the **avxdemo-S3** template.
7. In the **S3 Bucket Name** field, click .
   The **ARN Advanced Settings** pop-up window is displayed.



8. Copy the **Role ARN** from the **Outputs** tab of the **avxdemo-S3** template and paste it in the **Role ARN** field.
9. Click **Apply**.
10. Click **Save**.

The discovered account will be displayed in the grid on the **Device :: Cloud** page.

> **Note:** The discovered account will be added one more time as a child account since we are using federated access. This behaviour will be altered in the future releases to avoid dual listing of discovered AWS accounts.

Azure

- Azure-Overview
- Key Vault
- Application Gateway
- Virtual Machines

Azure-Overview

This documentation focuses on the benefits and implementation of integrating the following Azure services with AppViewX, for a holistic certificate lifecycle management for the Azure services:

- Azure Key Vault
- Azure Application Gateway
- Azure Virtual Machines

Key Vault

- Prerequisites for Implementing AppViewX's Azure Solution
- Adding a New Cloud Device to the Azure Key Vault
- Pushing a Certificate to the Azure Key Vault

Prerequisites for Implementing AppViewX's Azure Solution

- Internet and proxy connections
- The following key information from the cloud platform to be configured in AppViewX:
  - Subscription ID
  - Tenant ID

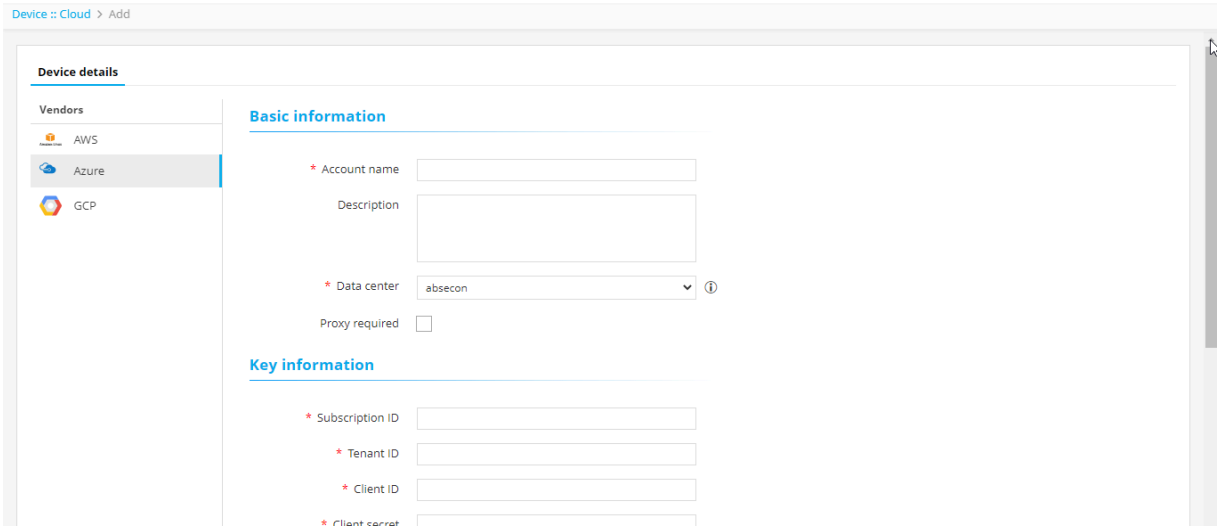
- Client ID
- Client Secret

• Permissions to manage the Azure Key Vault:

```
{ "properties":
  { "roleName": "AppViewX_KeyVault_Role",
    "description": "",
    "assignableScopes": [ "/subscriptions/f2689969-42f6-4fb5-b3be-e3a02e33751c" ],
    "permissions": [
     { "actions": [ "Microsoft.KeyVault/vaults/read" ],
       "notActions": [],
       "dataActions": [
         "Microsoft.KeyVault/vaults/certificates/import/action",
         "Microsoft.KeyVault/vaults/certificates/create/action",
         "Microsoft.KeyVault/vaults/certificates/update/action",
         "Microsoft.KeyVault/vaults/certificates/read" ],
       "notDataActions": [] } ] }}
```

Adding a New Cloud Device to the Azure Key Vault

1. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.



2. Enter/Select the following **Basic information**:

Field	Description
Account name*	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox.

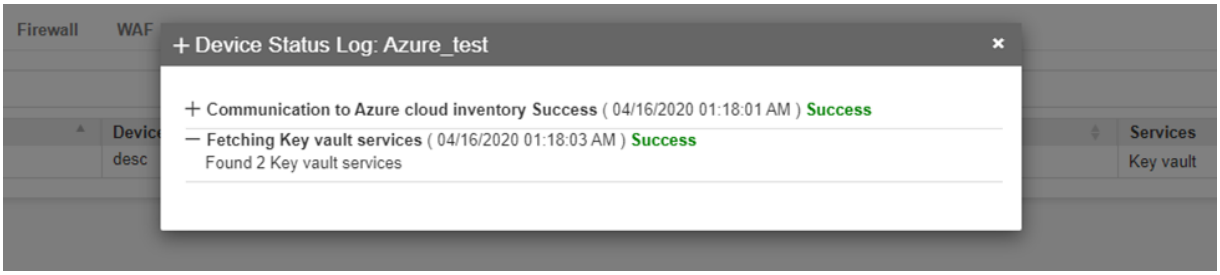
3. Enter/Select the following **Key information**:

Field	Description
Subscription ID*	Enter the customer's Azure subscription ID.
Tenant ID*	Enter the customer's Azure tenant ID.
Client ID*	Enter the customer's Azure client ID.
Client secret*	Enter the customer's Azure client secret key.
Services*	For the new device being added, from the dropdown list, select **Key Vault**.

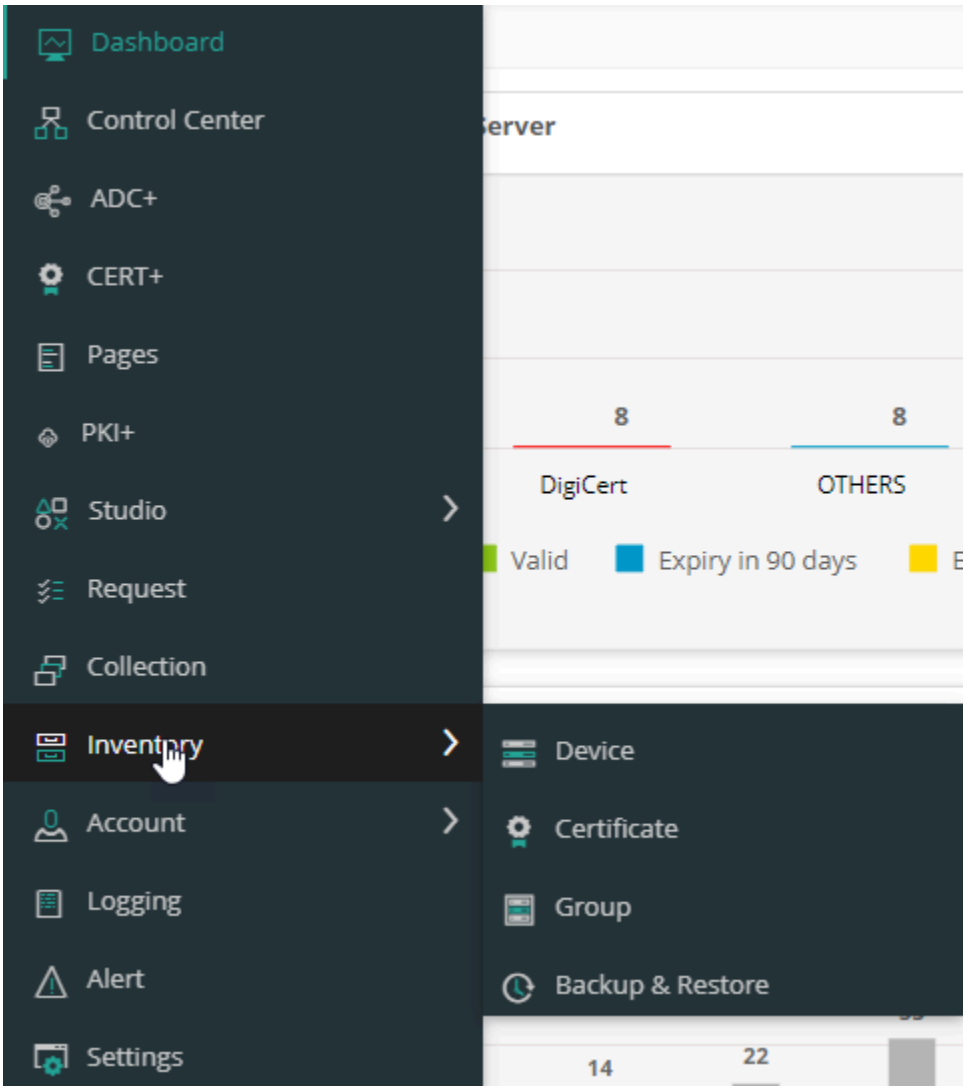
4. From **Additional attributes**, for the services selected, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
5. Click **Save**.
6. Return to the **Device :: Cloud** page.

7. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.

   The status of the added device is displayed.



8. To view the certificates, navigate to **Inventory** > **Certificate**.



   Certificates are automatically discovered and displayed here.

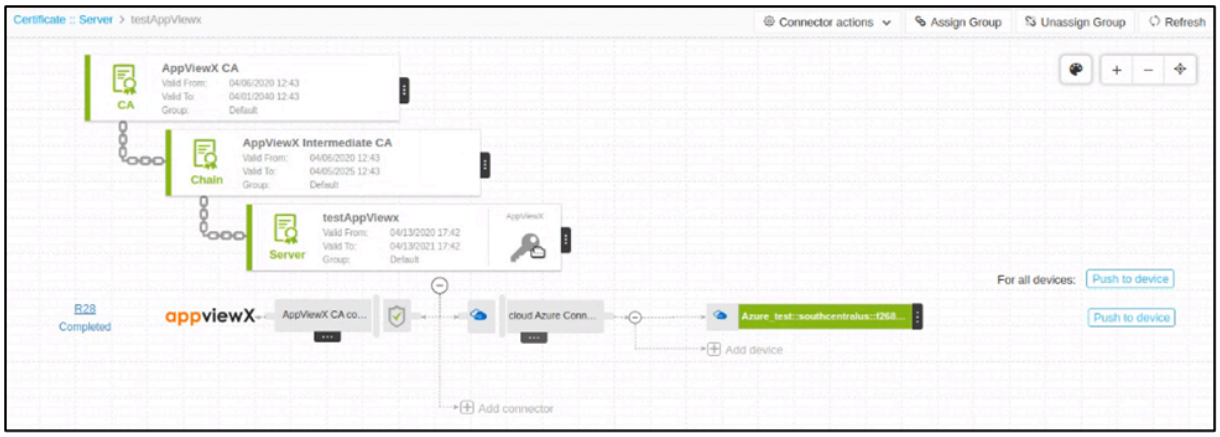
Pushing a Certificate to the Azure Key Vault

To import a certificate to the key vault, you will need to add a connector to the existing certificate.

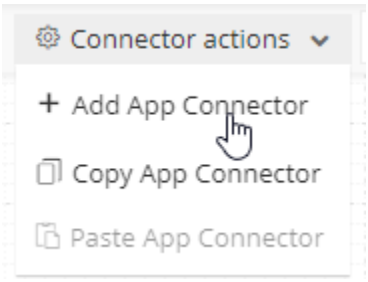
Note: If the certificate does not exist, you will be required to create a new certificate.

1. From the list of certificates displayed, click the **Common Name** of the certificate to which you want to add the connector.

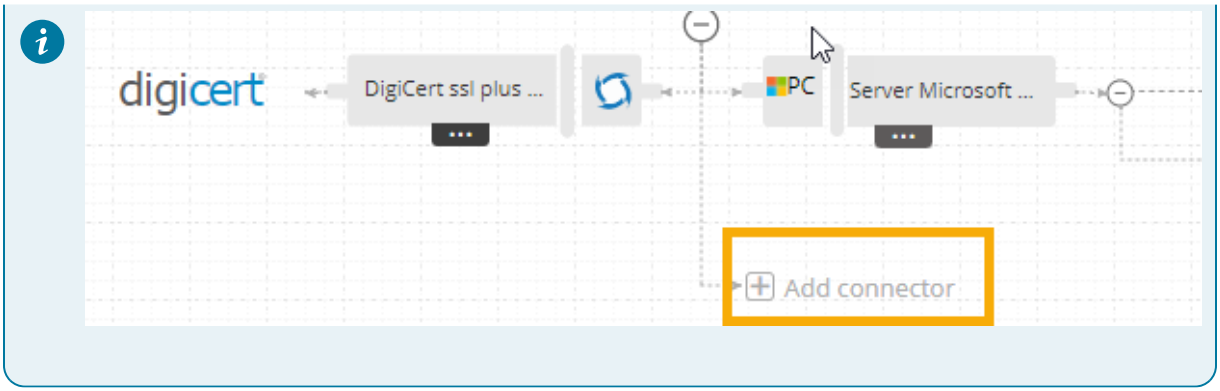
   The holistic certificate view is displayed.



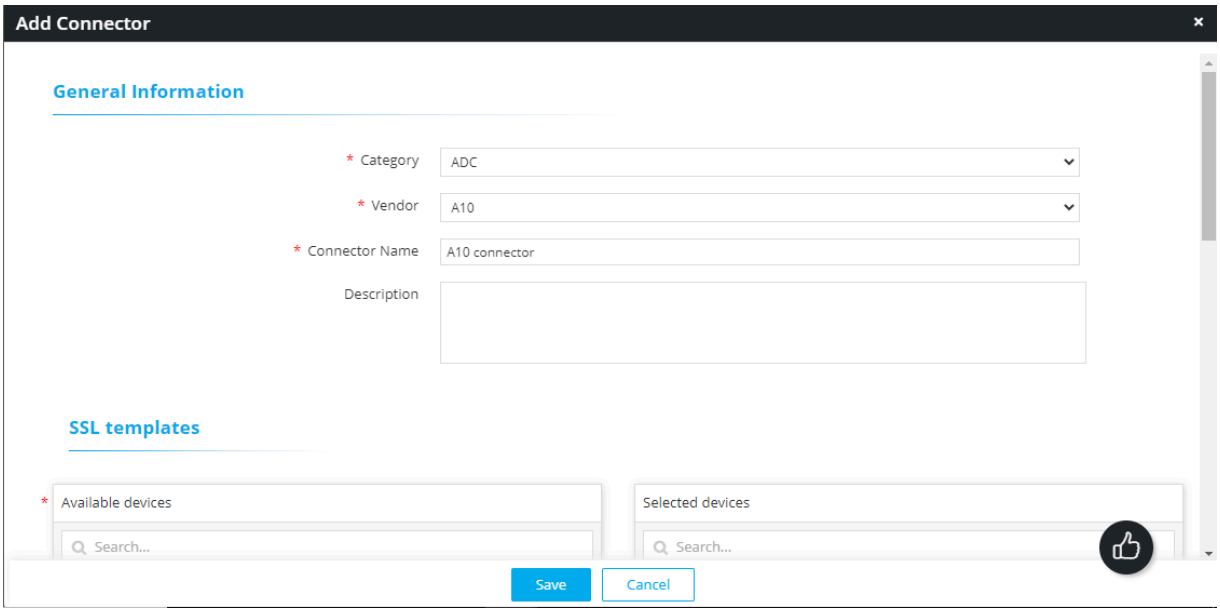
2. To add the connector, from the **Connector actions** menu, select **Add App Connector**.



Tip: You can also select the **Add Connector** option from the certificate holistic view.



The **Add Connector** action pane is displayed.



3. Enter/Select the **General Information** details:

Field	Description
Category*	Select the device type from the dropdown list. To add a connector for the device you just added, select **Cloud**.
Vendor*	From the dropdown list, select the device vendor. For this process, select **Azure**.
Service Type*	Select a service type to filter the available devices.

Field	Description
	For this process, select **Key Vault**.
Connector Name*	Enter a name for the connector. By default, the connector name is set to **Azure connector**.
Description	Enter a description for the connector.

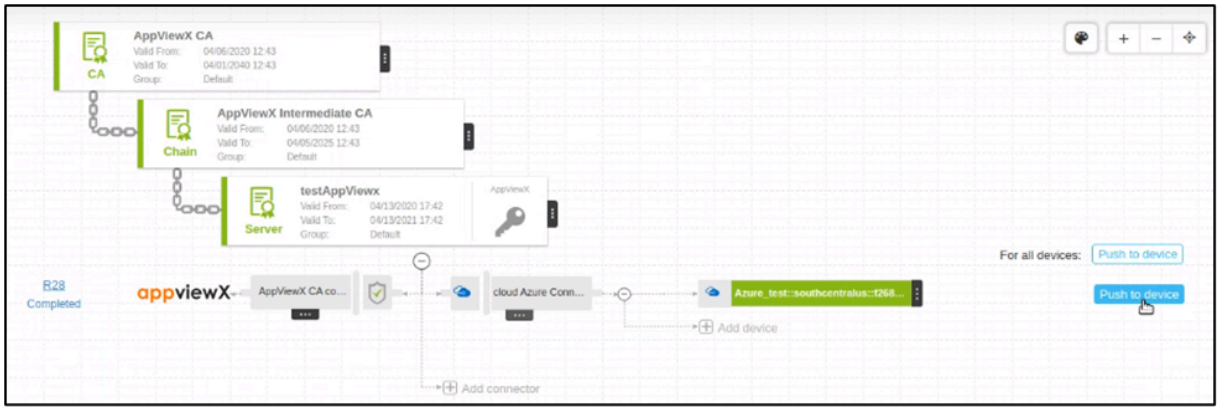
4. In the **Service Endpoint** section, under **Available devices**, search for and select the available device that was created for the Key Vault.
5. Enter/Select the following **Certificate Details**:

Field	Description
Certificate Type*	From the dropdown list, select the certificate type.
Certificate File Name*	Enter a name for the certificate file.
Password*	Enter the password to access the certificate file
Push Root and Intermediate Certificates	To push the root and intermediate certificates along with the selected certificate, select this checkbox.

Note: The **Push Details** section is optional for the Key Vault.

6. Click **Save**.

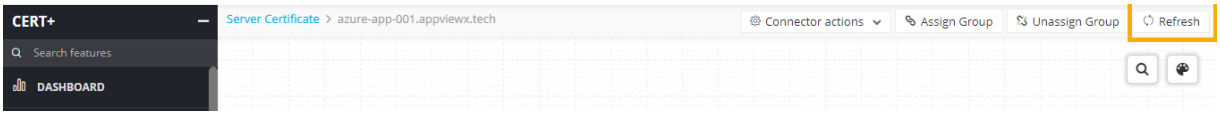
   The created connector will be displayed in the holistic view.



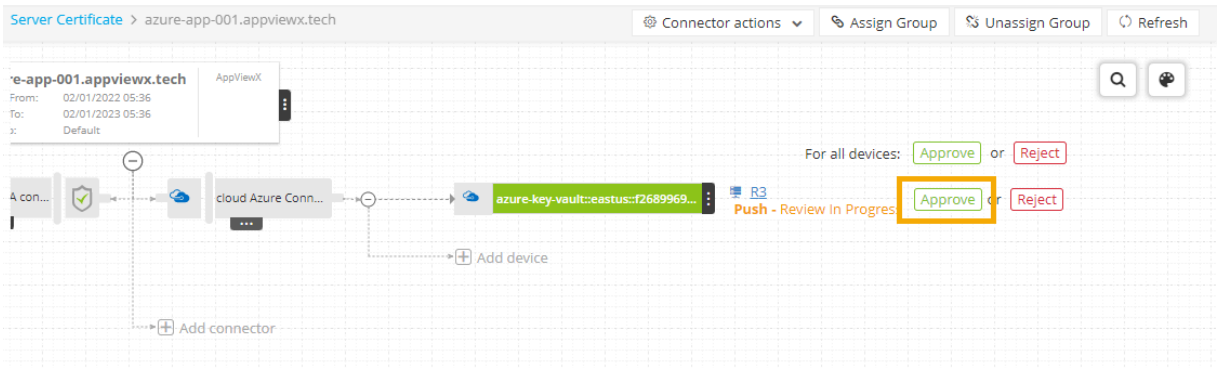
7. To push the certificate to a device, click **Push to Device**.
8. From the **Push to Device** dialog box, enter comments (optional) and click **OK**.

   The message **Push to device has been triggered successfully. Please refresh.** is displayed.

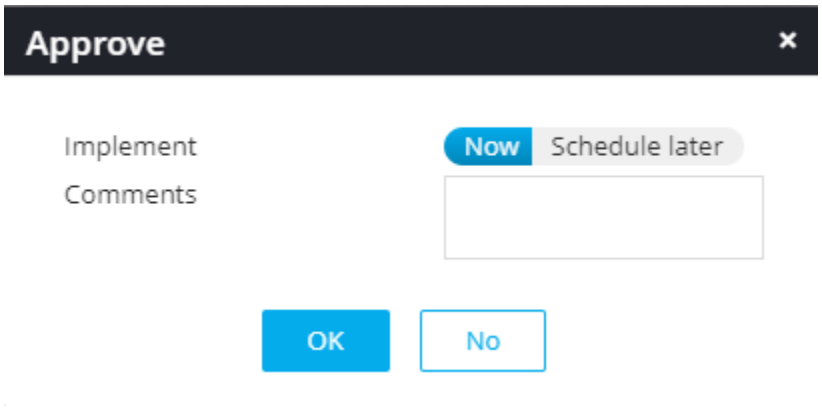
9. Click **Refresh**.



10. To approve the push operation, click **Approve**.



The **Approve** dialog box is displayed.

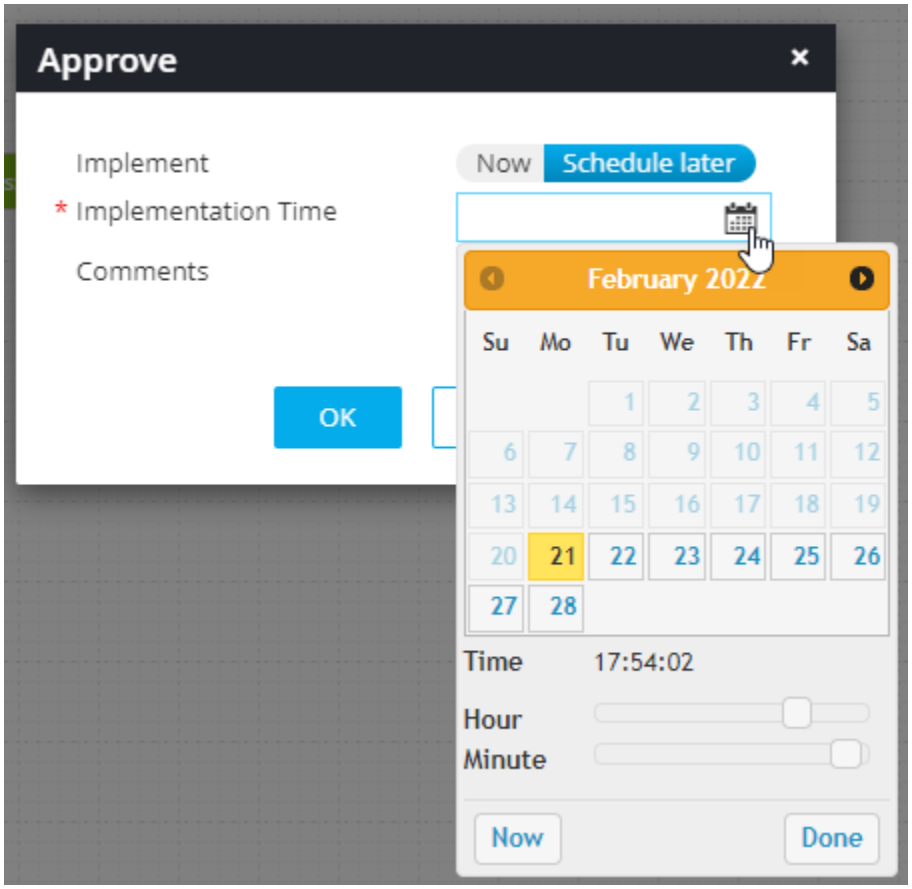


11. From the **Approve** dialog box:
    a. To implement the push operation immediately, select **Now**.

    OR

    a. To schedule the push operation for a later time, select **Schedule Later**.

    b. To set a date and time for the implementation, click  and select as required.

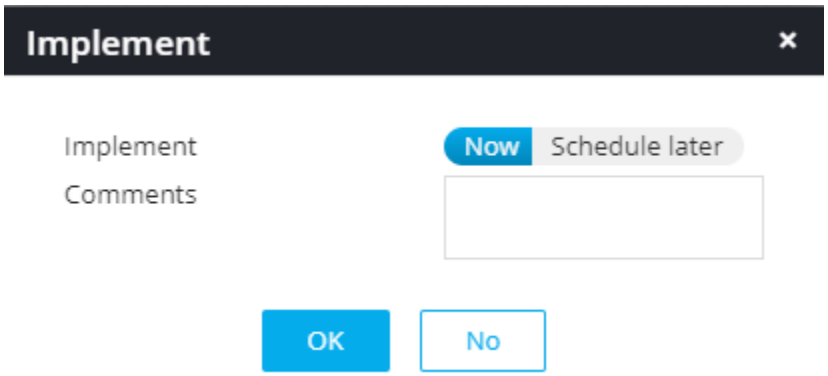


12. Click **OK**.

The message **Work order action has been triggered. Please refresh.** is displayed.

13. To implement the push operation, click **Implement**.

14. From the Implement dialog box, click **OK**.



Note: You can also schedule the implementation for later. The process is similar to scheduling the **Approve** operation for later.

When the push operation is successfully completed, the color of the connector changes to green and the following message is displayed:

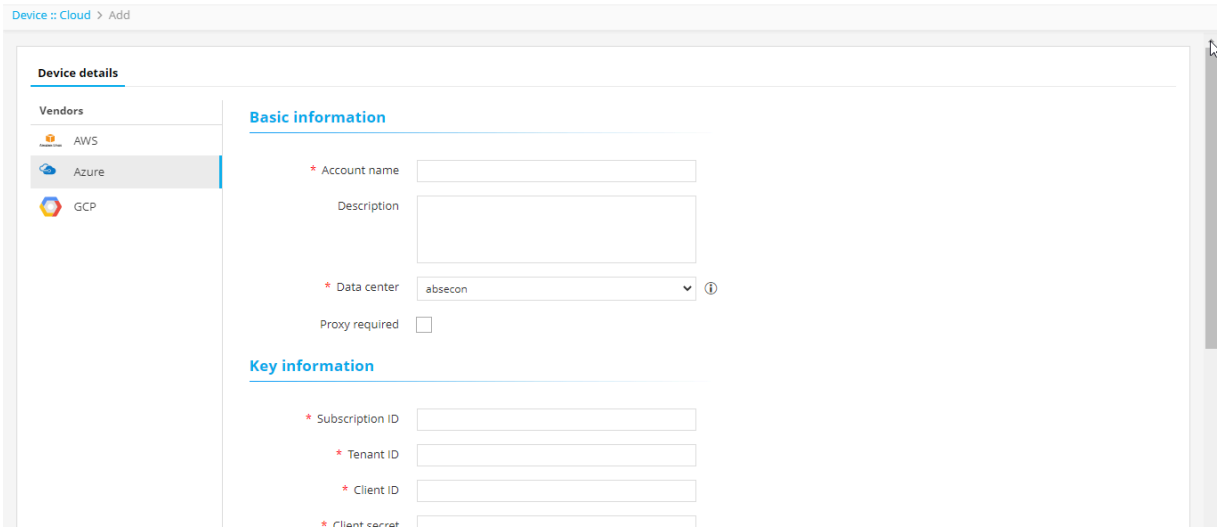
Note: To view the work order status, click the corresponding request ID.

Application Gateway

- Adding a New Cloud Device to the Azure Application Gateway
- Pushing a Certifcate to the Azure Application Gateway

Adding a New Cloud Device to the Azure Application Gateway

1. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.



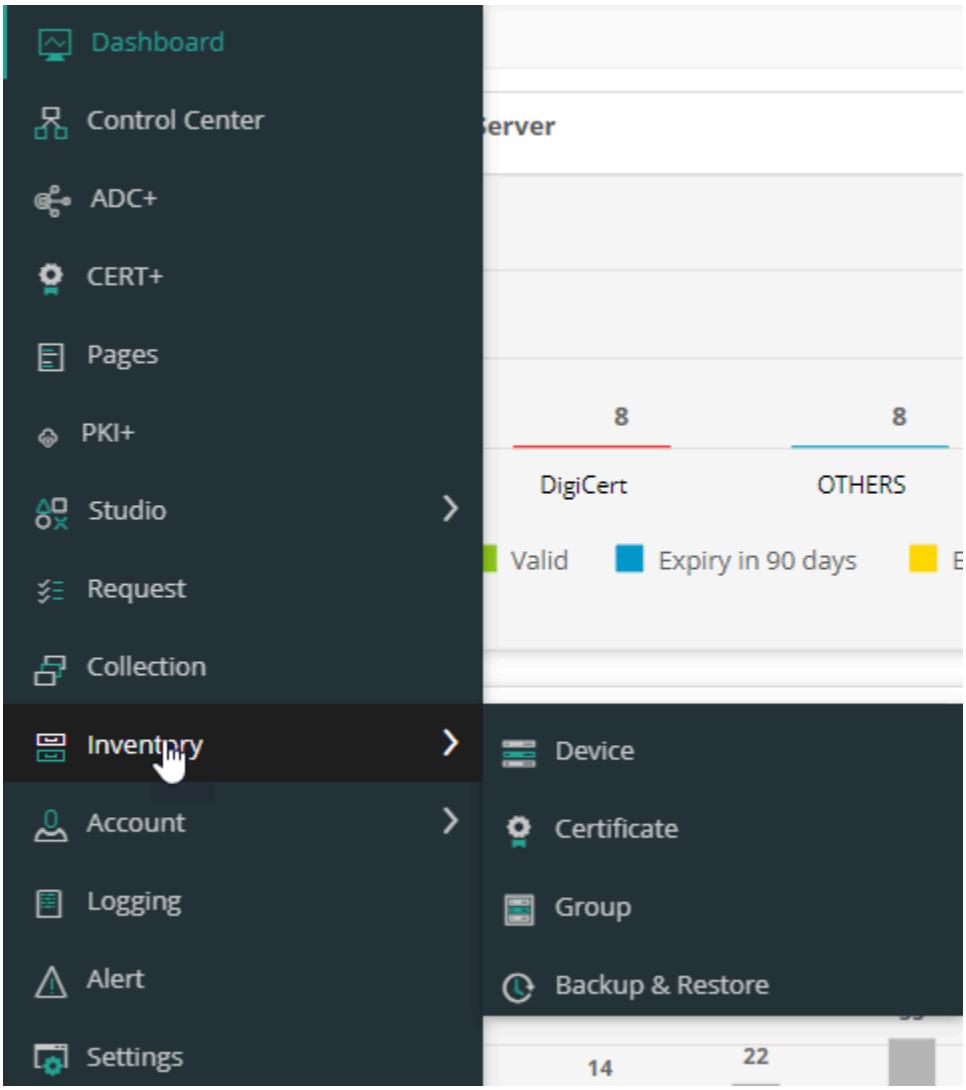
2. Enter/Select the following **Basic information**:

Field	Description
Account name*	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox.

3. Enter/Select the following **Key information**:

Field	Description
Subscription ID*	Enter the customer's Azure subscription ID.
Tenant ID*	Enter the customer's Azure tenant ID.
Client ID*	Enter the customer's Azure client ID.
Client secret*	Enter the customer's Azure client secret key.
Services*	For the new device being added, from the dropdown list, select **Application Gateway**.

4. From **Additional attributes**, for the services selected, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
5. Click **Save**.
6. Return to the **Device :: Cloud** page.
7. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
   The status of the added device is displayed.
8. To view the certificates, navigate to **Inventory** > **Certificate**.



Certificates are automatically discovered and displayed here.

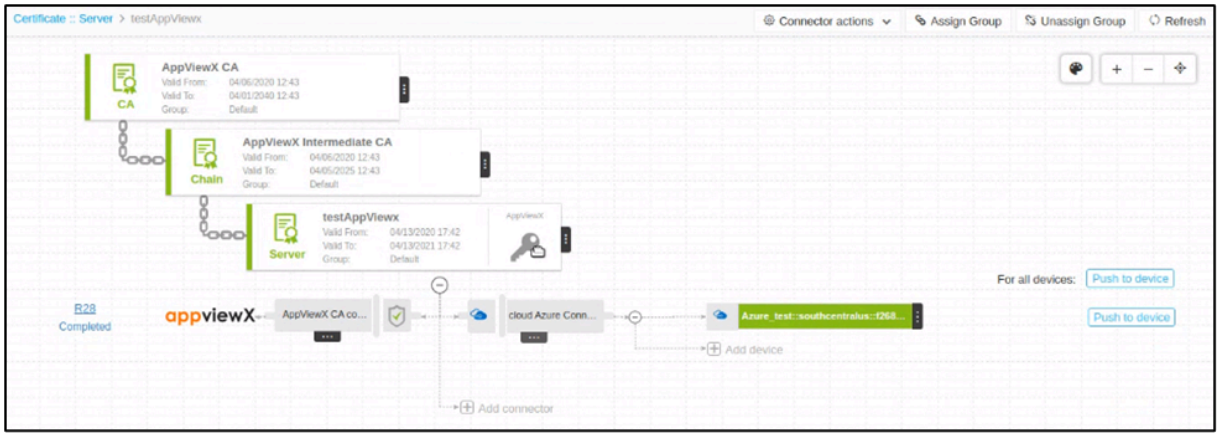
Pushing a Certifcate to the Azure Application Gateway

To import a certificate to the application gateway, you will need to add a connector to the existing certificate. The application gateway can perform the following services: push, bind, revoke, and auto-backup.

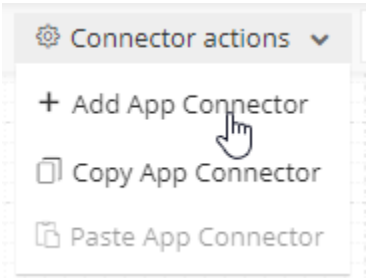
Note: If the certificate does not exist, you will be required to create a new certificate.

1. From the list of certificates displayed, click the **Common Name** of the certificate to which you want to add the connector.

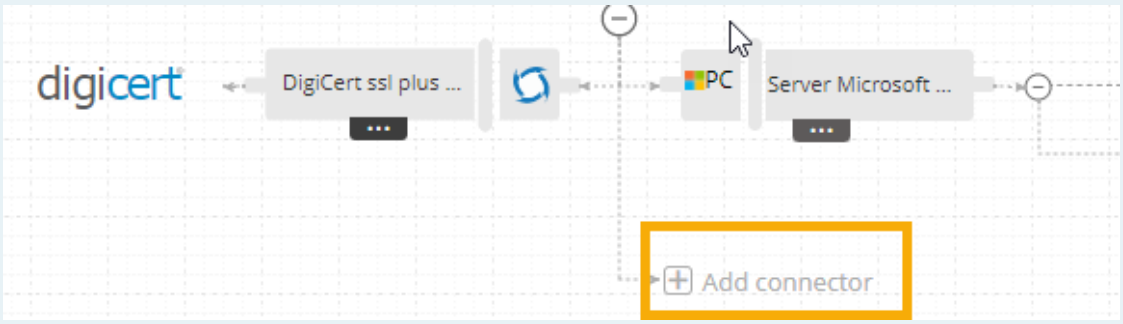
   The holistic certificate view is displayed.



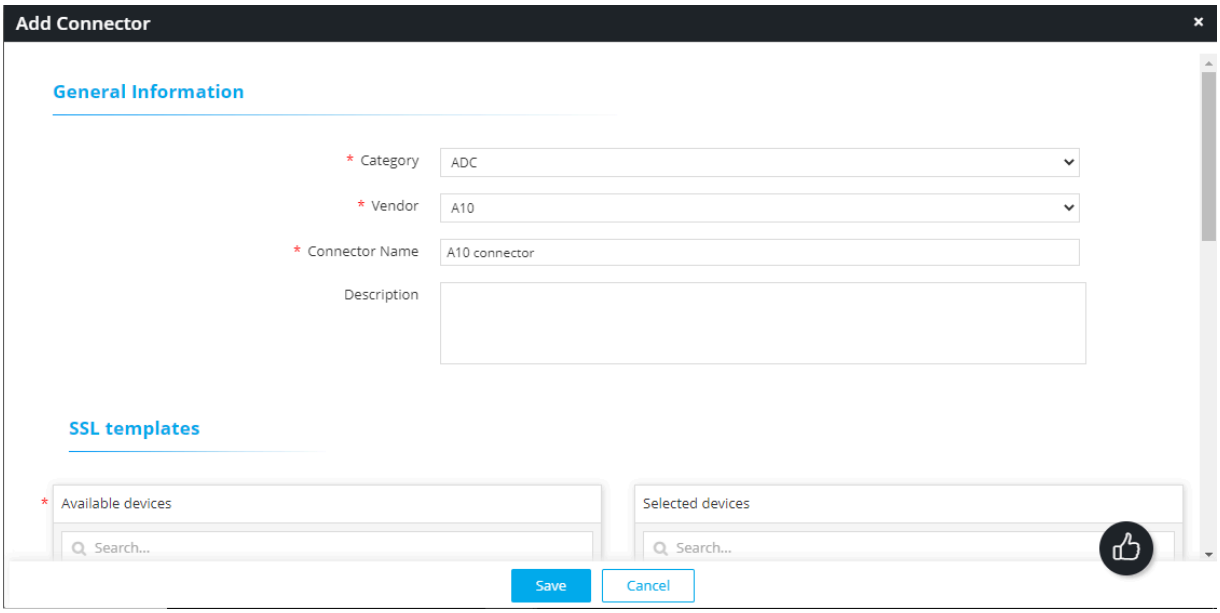
2. To add the connector, from the **Connector actions** menu, select **Add App Connector**.



Tip: You can also select the **Add Connector** option from the certificate holistic view.



   The **Add Connector** action pane is displayed.



3. Enter/Select the **General Information** details:

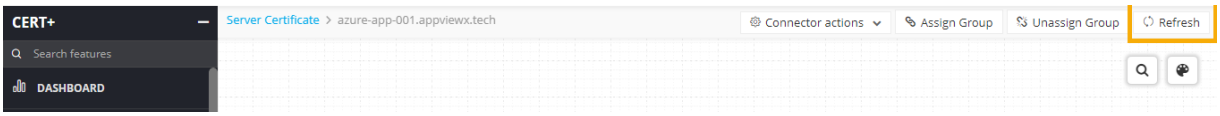
Field	Description
Category*	Select the device type from the dropdown list. To add a connector for the device you just added, select **Cloud**.
Vendor*	From the dropdown list, select the device vendor. For this process, select **Azure**.
Service Type*	Select a service type to filter the available devices. For this process, select **Key Vault**.
Connector Name*	Enter a name for the connector. By default, the connector name is set to **Azure connector**.
Description	Enter a description for the connector.

4. In the **Service Endpoint** section, under **Available devices**, search for and select the available device that was created for the Application Gateway.
5. Enter/Select the following **Certificate Details**:

Field	Description
Certificate Type*	From the dropdown list, select **PKCS#12 (*.pfx)**.
Certificate File Name*	Enter a name for the certificate file.
PFX Password*	Enter the password to access the certificate file
Push Root and Intermediate Certificates	To push the root and intermediate certificates along with the selected certificate, select this checkbox.

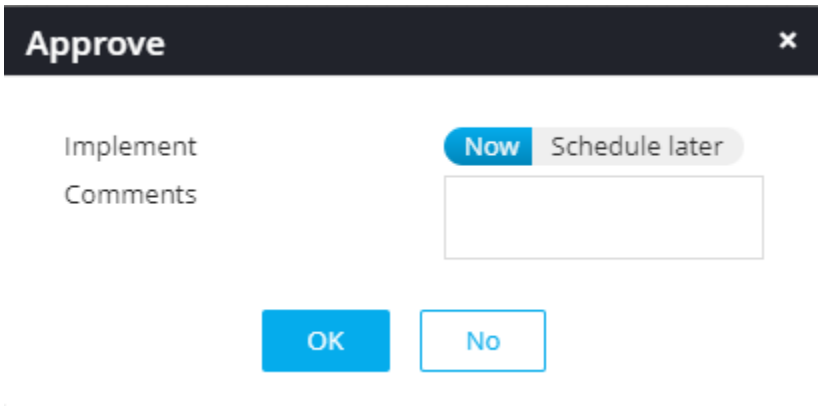
6. In the **Push Details** section, select the **Push automatically** checkbox.
   If the certificate attribute gets updated or renewed, this will automatically push the updated/renewed certificate to the device.
7. Click **Save**.
   The created connector will be displayed in the holistic view.
8. To push the certificate to a device, click **Push to Device**.
9. From the **Push to Device** dialog box, enter comments (optional) and click **OK**.

   The message **Push to device has been triggered successfully. Please refresh.** is displayed.
10. Click **Refresh**.



11. To approve the push operation, click **Approve**.

    The **Approve** dialog box is displayed.

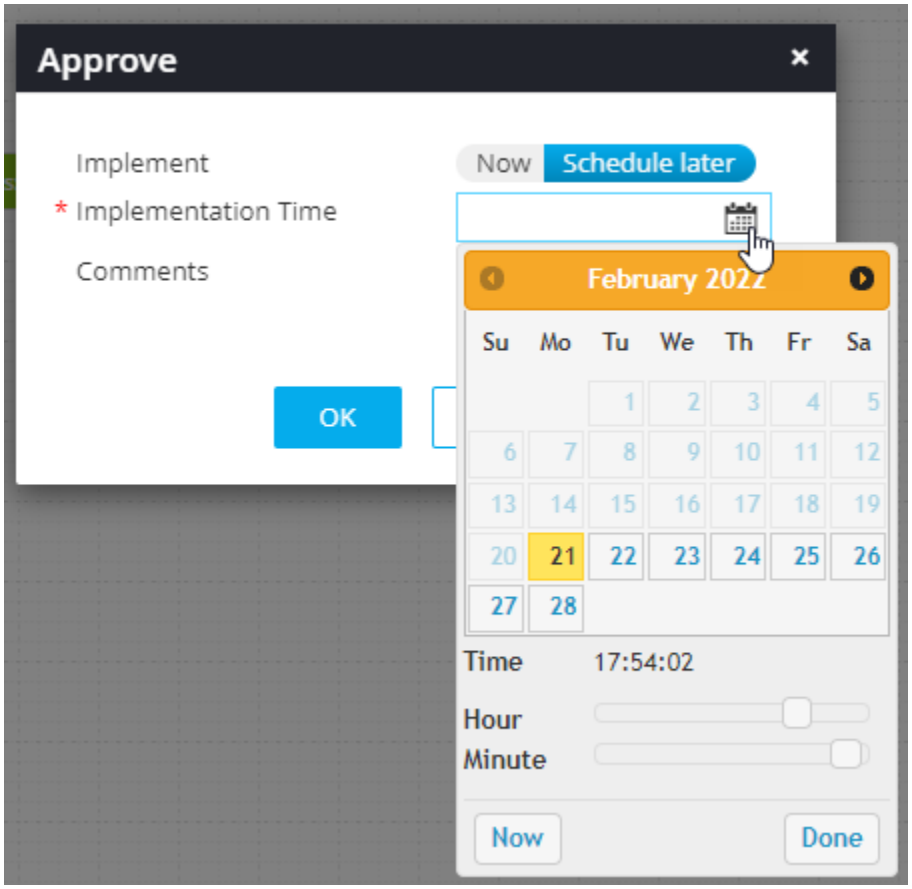


12. From the **Approve** dialog box:
    a. To approve the push operation immediately, select **Now**.

    OR

    a. To schedule the push operation for a later time, select **Schedule Later**.

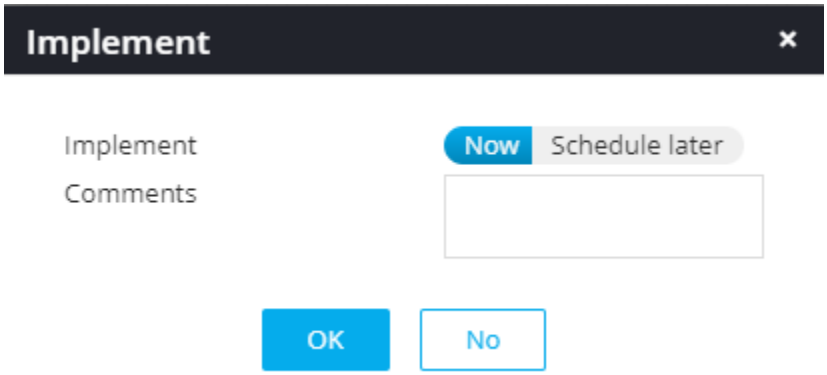
    b. To set a date and time for the implementation, click  and select as required.



13. Click **OK**.

The message **Work order action has been triggered. Please refresh.** is displayed.

14. To implement the push operation, click **Implement**.
15. From the Implement dialog box, click **OK**.



Note: You can also schedule the implementation for later. The process is similar to scheduling the **Approve** operation for later.

When the push operation is successfully completed, the color of the connector changes to green and the following message is displayed:

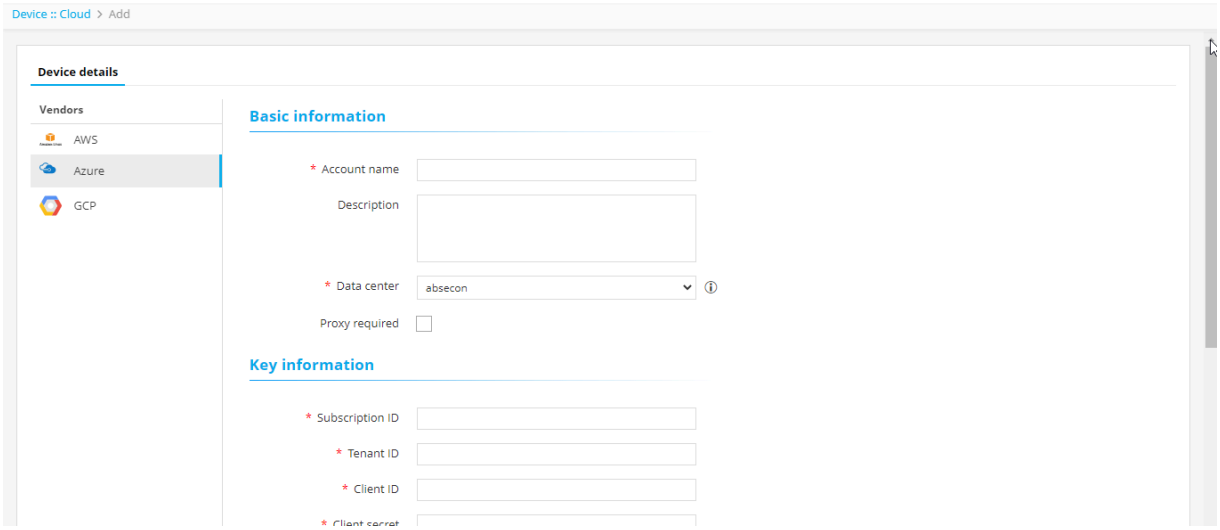
Note: To view the work order status, click the corresponding request ID.

Virtual Machines

- Adding a New Cloud Device to Azure Virtual Machines
- Pushing A Certificate to the Azure Virtual Machine

Adding a New Cloud Device to Azure Virtual Machines

1. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.



2. Enter/Select the following **Basic information**:

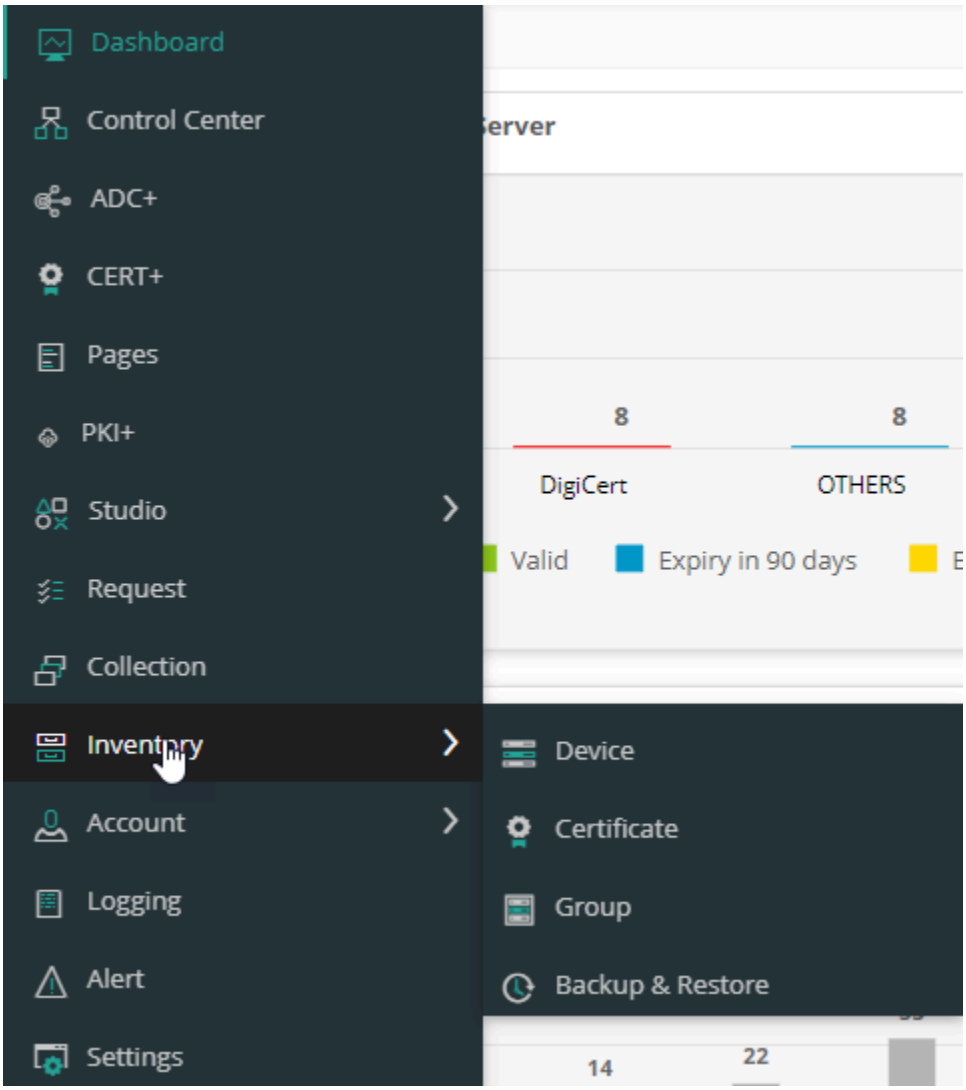
Field	Description
Account name*	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox.

3. Enter/Select the following **Key information**:

Field	Description
Subscription ID*	Enter the customer's Azure subscription ID.
Tenant ID*	Enter the customer's Azure tenant ID.

Field	Description
Client ID*	Enter the customer's Azure client ID.
Client secret*	Enter the customer's Azure client secret key.
Services*	For the new device being added, from the dropdown list, select **Virtual Machine**.

4. From **Additional attributes**, for the services selected, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
5. Click **Save**.
6. Return to the **Device :: Cloud** page.
7. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
   The status of the added device is displayed.
8. To view the certificates, navigate to **Inventory** > **Certificate**.



Certificates are automatically discovered and displayed here.

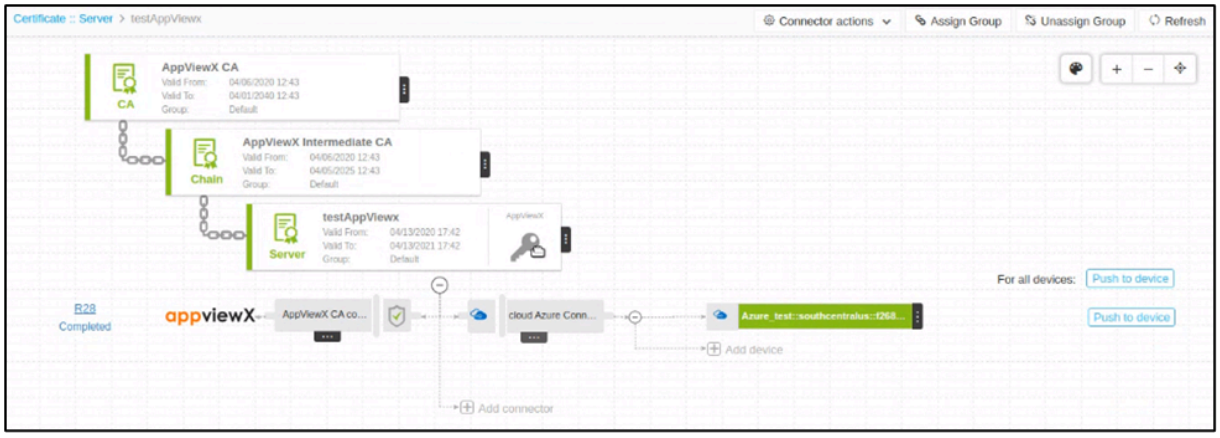
Pushing A Certificate to the Azure Virtual Machine

To import a certificate to the virtual machine, you will need to add a connector to the existing certificate.

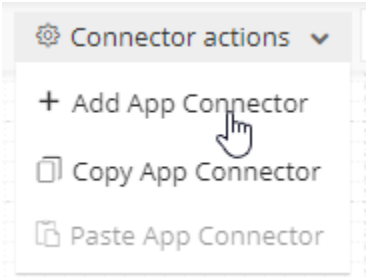
Note: If the certificate does not exist, you will be required to create a new certificate.

1. From the list of certificates displayed, click the **Common Name** of the certificate to which you want to add the connector.

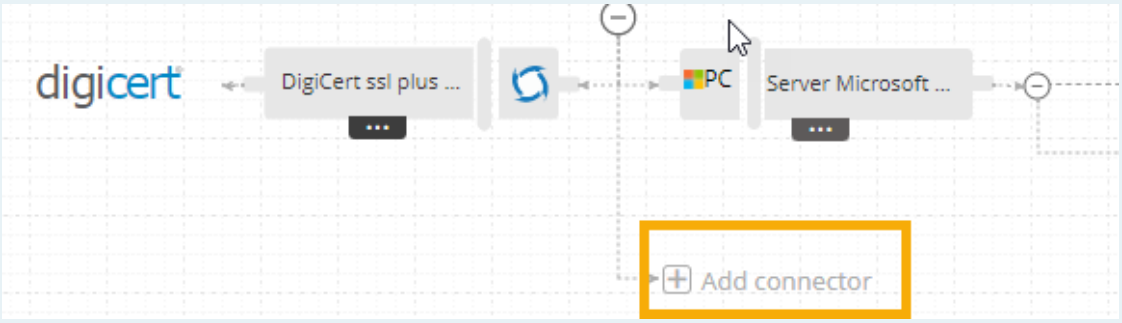
   The holistic certificate view is displayed.



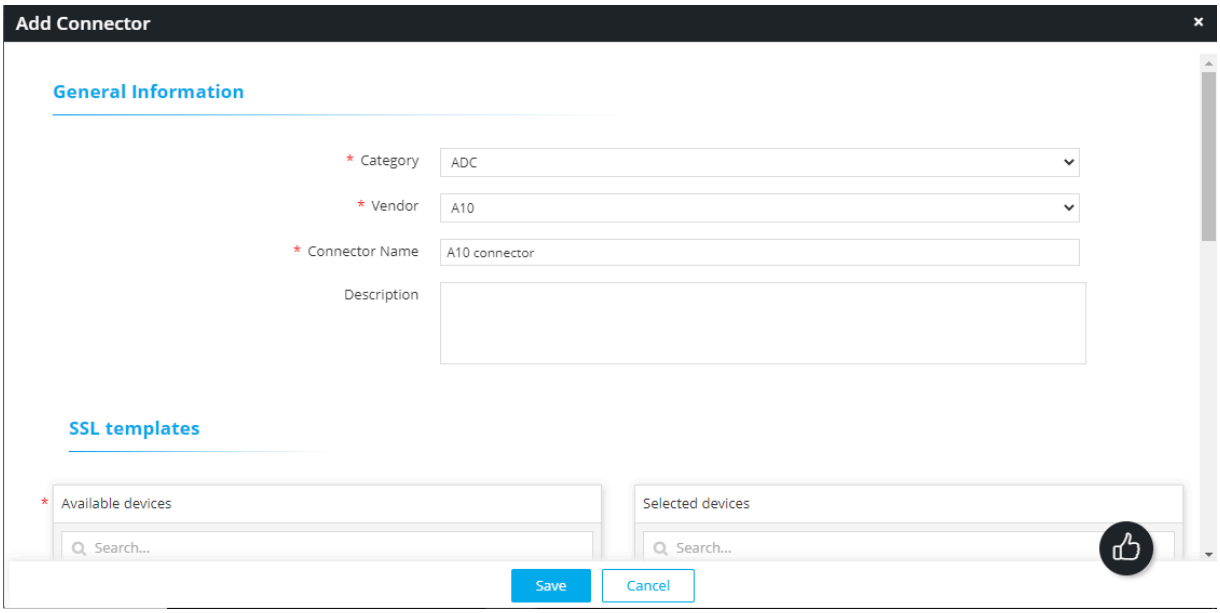
2. To add the connector, from the **Connector actions** menu, select **Add App Connector**.



Tip: You can also select the **Add Connector** option from the certificate holistic view.



The **Add Connector** action pane is displayed.



3. Enter/Select the **General Information** details:

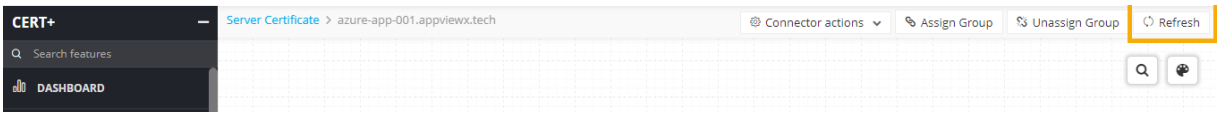
Field	Description
Category*	Select the device type from the dropdown list. To add a connector for the device you just added, select **Cloud**.
Vendor*	From the dropdown list, select the device vendor. For this process, select **Azure**.
Service Type*	Select a service type to filter the available devices. For this process, select **Virtual Machine**.
Connector Name*	Enter a name for the connector. By default, the connector name is set to **Azure connector**.
Description	Enter a description for the connector.

4. In the **Service Endpoint** section, under **Available devices**, search for and select the available device that was created for the Virtual Machine.
5. Enter/Select the following **Certificate Details**:

Field	Description
Certificate Type*	From the dropdown list, select **PKCS#12 (*.pfx)**.
Certificate File Name*	Enter a name for the certificate file.
PFX Password*	Enter the password to access the certificate file
Push Root and Intermediate Certificates	To push the root and intermediate certificates along with the selected certificate, select this checkbox.

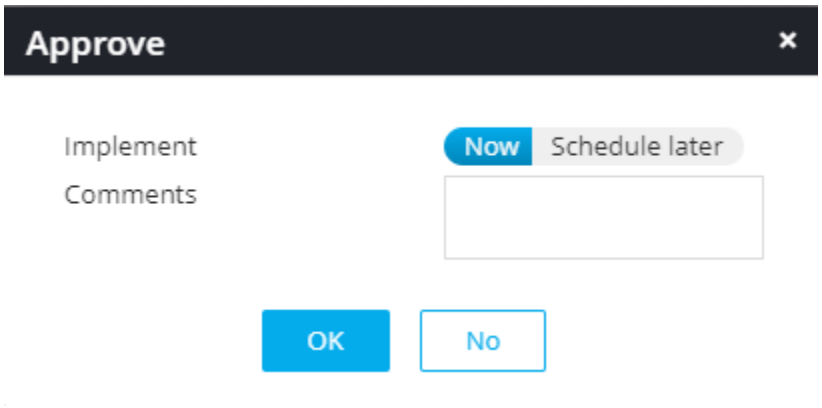
6. In the **Push Details** section, select the **Push automatically** checkbox.
   If the certificate attribute gets updated or renewed, this will automatically push the updated/renewed certificate to the device.
7. Click **Save**.
   The created connector will be displayed in the holistic view.
8. To push the certificate to a device, click **Push to Device**.
9. From the **Push to Device** dialog box, enter comments (optional) and click **OK**.

   The message **Push to device has been triggered successfully. Please refresh.** is displayed.
10. Click **Refresh**.



11. To approve the push operation, click **Approve**.

    The **Approve** dialog box is displayed.

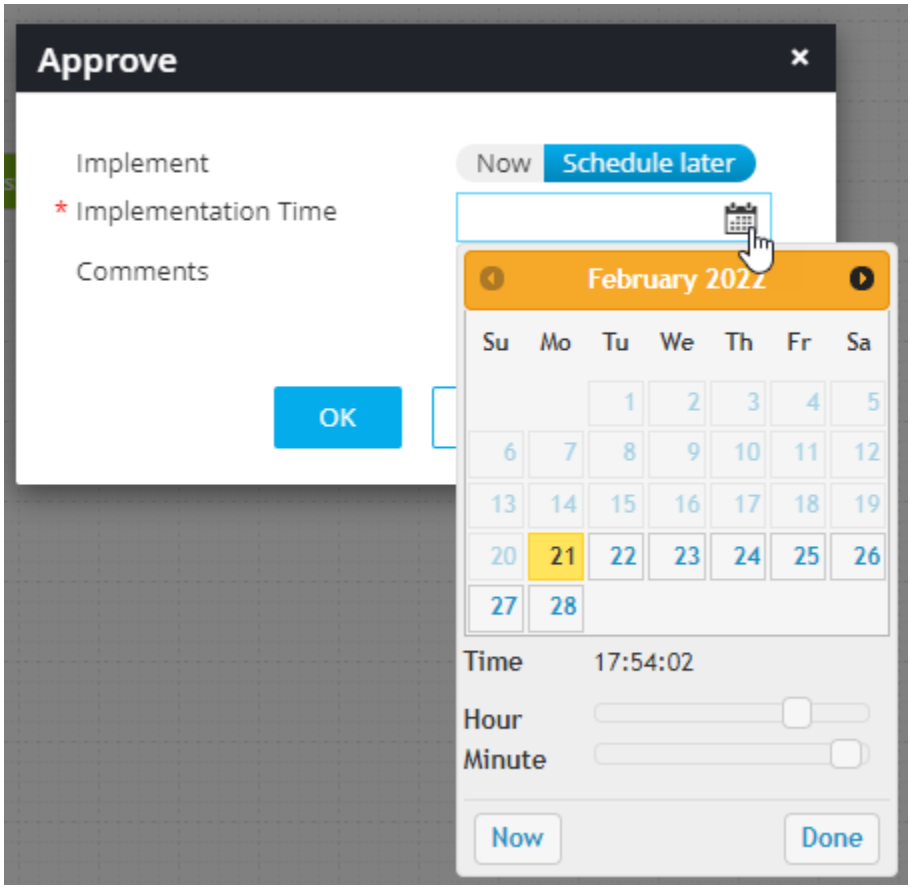


12. From the **Approve** dialog box:
    a. To implement the push operation immediately, select **Now**.

    OR

    a. To schedule the push operation for a later time, select **Schedule Later**.

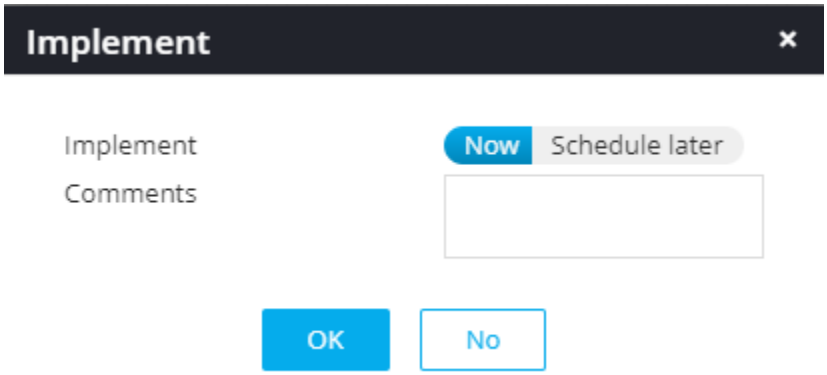
    b. To set a date and time for the implementation, click  and select as required.



13. Click **OK**.

The message **Work order action has been triggered. Please refresh.** is displayed.

14. To implement the push operation, click **Implement**.
15. From the Implement dialog box, click **OK**.



Note: You can also schedule the implementation for later. The process is similar to scheduling the **Approve** operation for later.

When the push operation is successfully completed, the color of the connector changes to green and the following message is displayed:

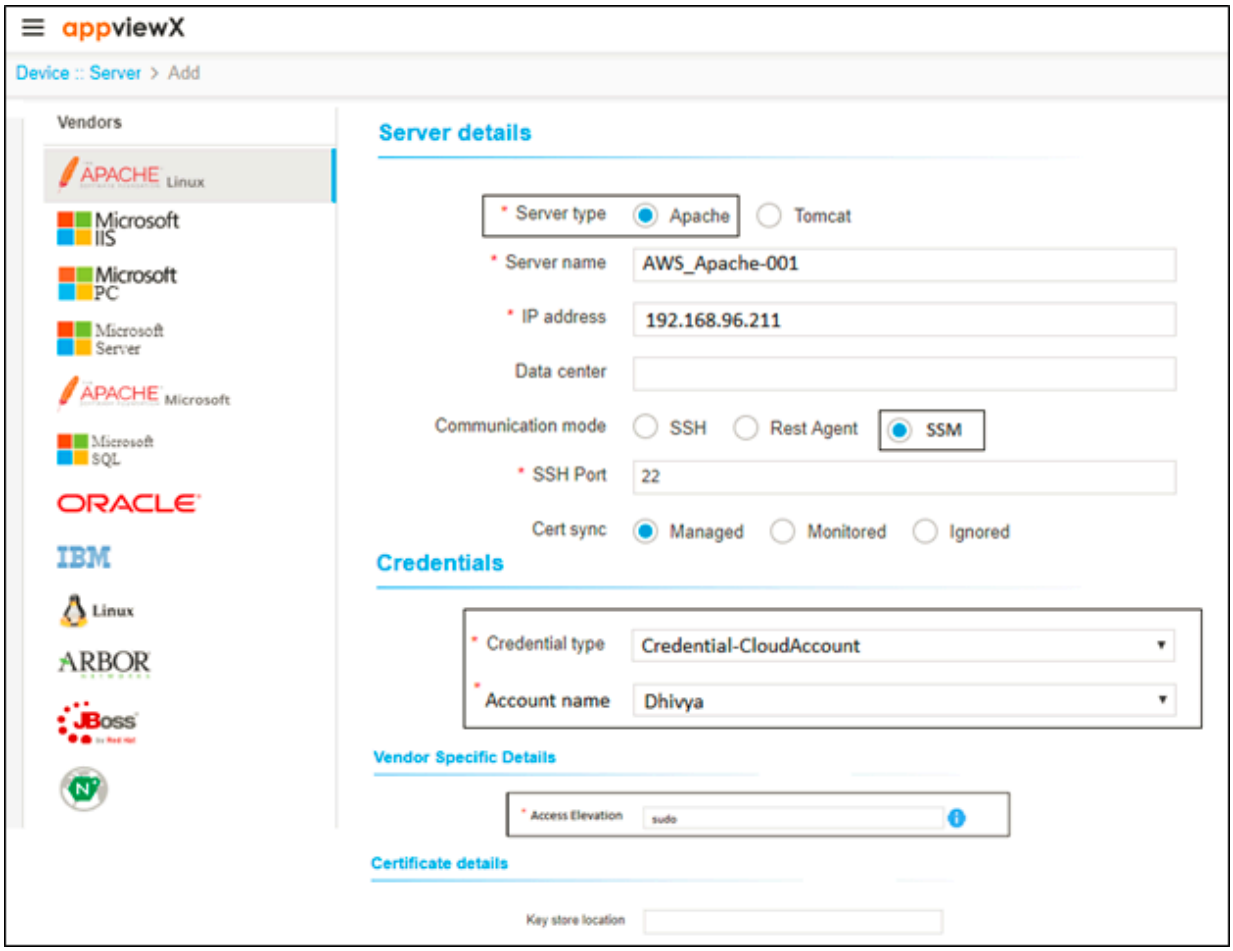
Note: To view the work order status, click the corresponding request ID.

Apache SSM integration specification

Device Addition

- **Apache (Linux)** serversdiscovered from Amazon EC2 instances should be added under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill in the Apache (Linux) device addition page.

- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.
- By default, access elevation should be selected as **Sudo.**



Credential management

- Credential Type is a mandatory field.
- When a device is added from a could account, **Credential-Cloud Account must** be displayed corresponding to the credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.
- While modifying the mandatory details in the Apache form, the user should be able to select a different cloud account credential that is added to the cloud inventory.

- Similarly, while modifying the mandatory details in the Apache form, the user should be able to provide credentials manually in the Apache device addition form.

> **Note:** Once the Apache instance is identified and successfully added, the user should be able to perform all the actions (device level as well as certificate level).

Functional Specification

Basic information specifications

- Users should be able to provide basic information such as Account name, Device description, and Account number.
- The account name should be maintained as a unique factor; the user should not be allowed to add the same account name more than once.
- When the user tries to submit the same Account name, a pop-up error message displays as **Account name already available in the inventory**.

Account name

- The account name is a mandatory field. Users should provide a valid name in this column.
- The account name field should be an alphanumeric field. Users should be able to provide alphabets and numbers.
- Users should not be able to provide any special characters in this field, except period (.)
- Users should not be able to provide [space] in this field.
- The account name field should support only 25 characters. Block users to enter more than 25 characters.
- Add an information icon next to the account name text box and displays a message as **Account name should be unique**. The account name already in the cloud inventory cannot be added again. Only alphanumeric and period (.) can be entered in this field.

Description

- Users can provide the description in this paragraph box.
- Allow a maximum of 250 characters in the description field.
- Allow numbers, alphabets, all the special characters, and [space] in the description field.

Account number

- The account number is an optional field. Users should provide a valid account number in this column.
- Users should be able to enter only numbers in the account number.
- Users should not be able to provide any special characters in this field.
- Users should not be able to provide [space] in this field.
- Users should be able to provide a maximum of 25 numbers. Users should not be able to provide more than 25 entries.

Proxy required

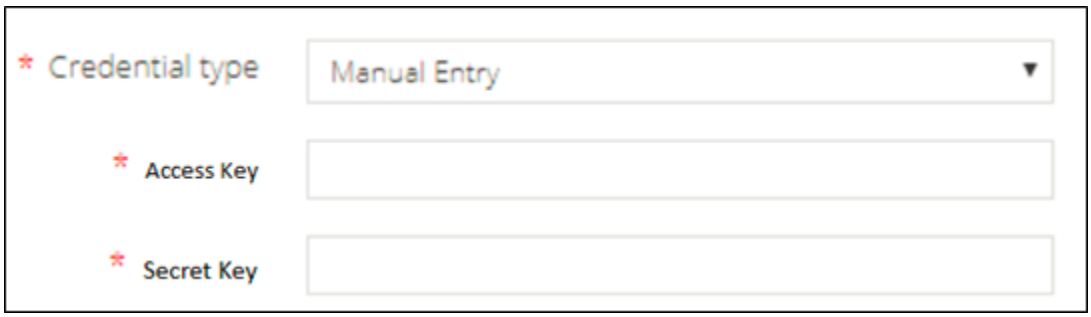
- Proxy required is an optional field, when the user selects this checkbox, AppViewX will try to communicate via Proxy in case of network failure/absence.
- If the user does not select this checkbox, then AppViewX will connect/communicate only via the internet/network, if there is network failure/absence, AppViewX will not try to communicate via provided Proxy.

Credentials Specifications

- Only when the Master credential is selected in the above section, the Credential section will be displayed in this form. When the user lands on this page to add a new cloud device, by default, the Master credential will be selected, hence the Credential section will be displayed as well.
- Users should be able to provide the credentials in this section; if the master credential is selected against the Credential type. It should be used to access all the services that are selected in the services section.

Credential input type

- The credential input type is a mandatory field. It is a single select dropdown. By default, Manual Entry will be displayed.



- Credential input type should list three options, they are

  - Manual entry
  - Credential list – CyberArk
  - Credential list – AppViewX
- When “Manual Entry” is selected, **Access Key** and **Secret key fields** should bedisplayed below Credential input type fields.
  - The access key and Secret Key are mandatory fields and Password encrypted fields.
  - Users should provide both Access Key and Secret Key corresponding to the account added.
  - These keys will be used to access all the services that are selected in the services section.
- When the “credential list – CyberArk” is selected, the **Credential list dropdown** should bedisplayed below the Credential input type fields.
  - Users should be able to select a credential that is saved in CyberArk. This credential will be used to access all the services that are selected in the services section.
- When the “credential list – AppViewX” is selected, the **Credential list dropdown** should bedisplayed below the Credential input type fields.
  - Users should be able to select a credential that is saved in AppViewX vault. This credential will be used to access all the services that are selected in the services section.

Access key

- When the user lands on this page to add a new cloud device, by default, Manual Entry will be displayed under the Credential input type. Hence, the Access Key field will be displayed as well.
- The access key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to provide (space) in this field.
- Minimum and Maximum Length of Access Key is 16 and 128 characters respectively.

Secret key

- When the user lands on this page to add a new cloud device, Manual Entry will be displayed under the Credential input type. Hence, the Secret Key field will be displayed as well.
- The secret key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to provide [space] in this field.
- The maximum length of the Secret key is 256 characters.

Key information specifications

- Users should be able to provide the key information such as Datacenter, Region, Credential type, and Account number.
- Users have to provide a data center, region, and service. If any of these fields are blank/ empty, while submitting the form, the X mark will be displayed against the field that is not filled. A message will be displayed when the user mouse over the X mark, “Value is missing in <*fieldName*> field”.

Data Center

- Data center is a mandatory field, the “**Select a data center**” message must be displayed as a play holder when the user lands on this page to add a new cloud device.

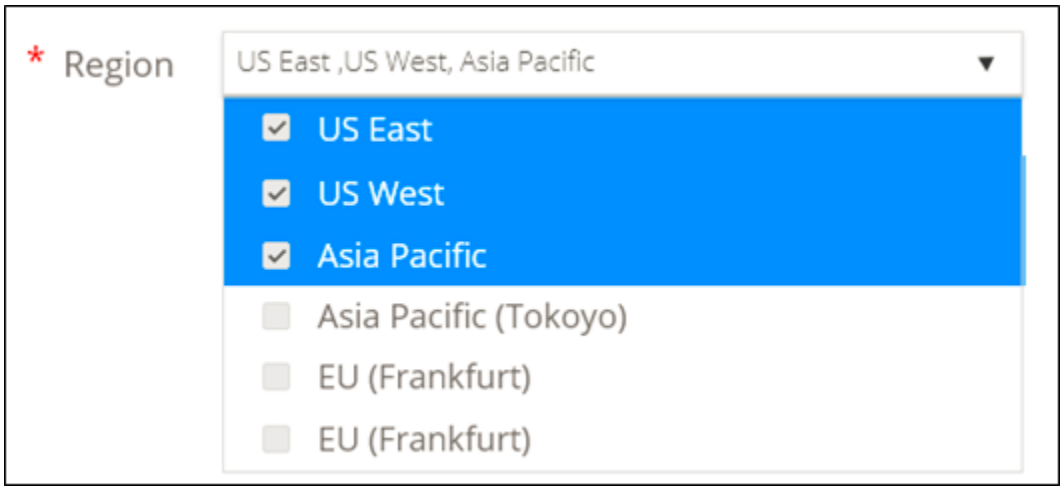
- Users can select a data center for the dropdown (single select dropdown).

- Based on the data center selected, the region corresponding to the selected data center will be listed below the field region field.
- Users should be restricted to submit this form, without filling a data center. If the user does not select a data center, while submitting the form, X mark will be displayed against the data center field. A message will be displayed when the user mouse over X mark, “Value is missing in datacenter field”.

Region

- Region is a mandatory field.
- Fetch region(s) button will be enabled only when the credentials are given. The user should provide the credentials to enable the fetch region(s)
- Once credentials are provided, the fetch region(s) will be enabled. Users should be able to click the fetch region(s) button.
- Once the user click fetch region(s) by providing valid credentials, a list of all the regions corresponding to the credential provided will be displayed in the drop-down,

- If provided credentials do not have any region (or) if the provided credential is invalid, then None will be displayed in the dropdown.



- The "**Select the region(s)"** message must be displayed as a play holder when the user lands on this page to add a new cloud device.
- Users can select single or multiple regions from this dropdown (multi-select dropdown).
- Users should be able to select all / unselect all the regions from this field.
- Users should be able to free-text search the region in the dropdown.
- Users should be restricted to submit this form, without selecting at least one region. If the user does not select a region, while submitting the form, the X mark will be displayed against the region field. A message will be displayed when the user mouse over X mark, "Value is missing in region field".

Service

1. Service is a mandatory field. It is a multi-select text box. By default, **ACM** and **IAM** will be selected.

2. Users can select single or multiple service(s) from this dropdown (multi-select text box).
3. ACM, IAM, ELB, and EC2 are the services that should be listed in the dropdown.
4. AppViewX should support four Amazon AWS services, they are, ACM, IAM, ELB, and EC2 instances. Users should be able to select any one of these services from this field.
5. Based on the selected service, the user should provide additional details in the below section.
6. Users should be able to select all / unselect all the services from this field.

7. Users should be able to free-text search the service from this field.
8. Users should be restricted to submit this form, without selecting at least one service. If the user does not select a service, while submitting the form, X mark will be displayed against the service field. A message will be displayed when the user mouse over X mark, “**Value is missing in-service field**”.

Additional attributes specifications

Service Input Status

- The services that are selected in the services section will be displayed as a tab in this section.
- Each tab will have a different set of fields that are required for accessing each service.
- There are a few mandatory fields corresponding to each service.
- When the user lands on this page to add a new cloud device, by default, **ACM** and **IAM** tabs will be displayed.
- Once mandatory fields are filled, each tab will be indicated with a GREEN tick mark. Only when all the selected services are marked with a GREEN tick, the user will be able to submit the form.
- If the user tries to save without filling in the required detail, an **X** mark should be displayed against each tab that is not completed.
- When the user mouse over **X**mark below message should be displayed, “Mandatory fields are not filled in this tab”

Cert sync

- Cert sync is a mandatory field. When the user lands on this page to add a new cloud device, by default, Managed will be selected.
- Cert sync should be available in all the tab.
- Cert sync have three options,
  - Managed – Certificates within the cloud (corresponding to the service selected), & its objects will be discovered and moved to inventory with managed status. Users can perform different AppViewX actions on the certificates that are in managed status. E.g., Cert Sync in the ACM tab is selected as Managed, then all the certificates in ACM will be discovered and moved to the inventory with managed status.
  - Monitored – Certificates within the cloud (corresponding to the service selected), and their objects will be discovered and moved to inventory with monitored status. Users can only monitor the certificates that are in monitored status, user cannot perform any AppViewX actions on these certificates. E.g.,

Cert Sync in the ACM tab is selected as Monitored, then all the certificates in ACM will be discovered and moved to the inventory with monitored status.

- Ignored – The cloud account will be added and managed in AppViewX. Certificates within the cloud (corresponding to the service selected), & its objects will **not** be discovered; only the profiles will be created.

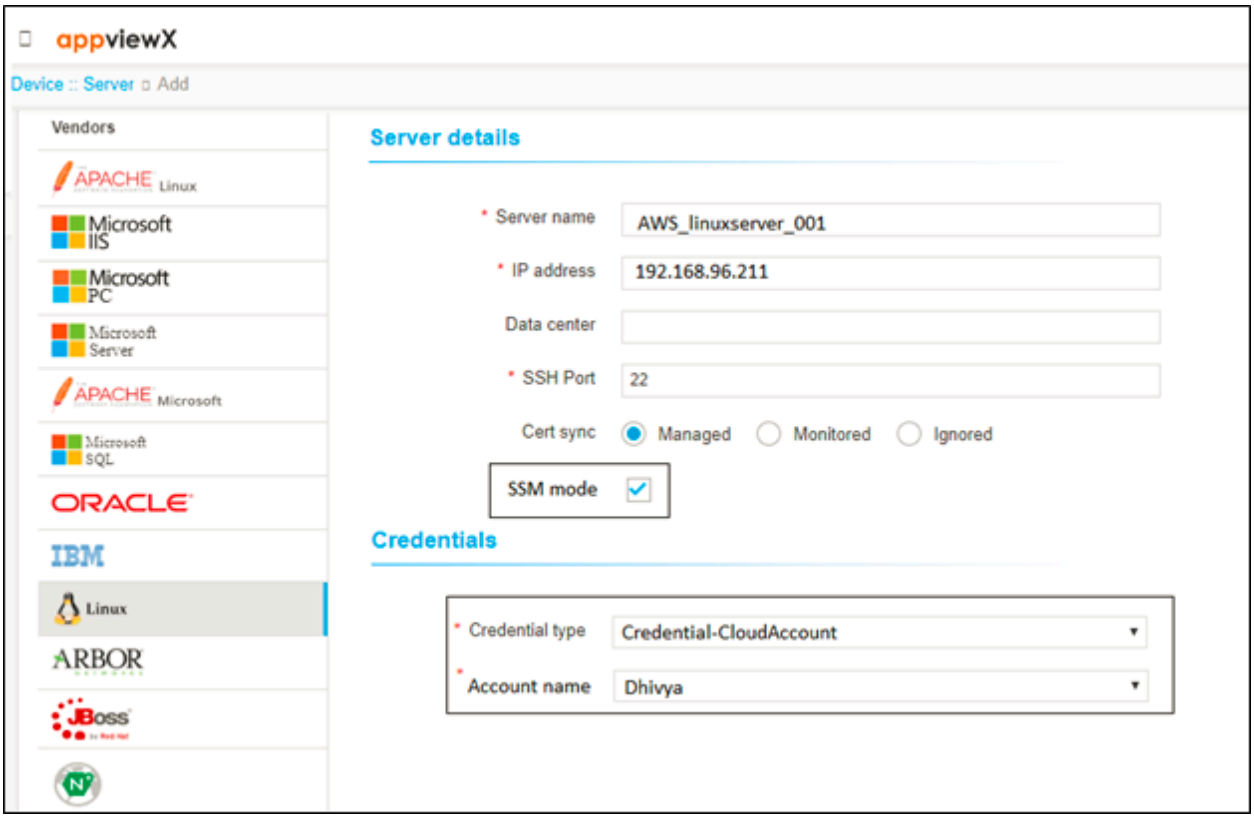
Collection type

1. The collection type field will be displayed only when the EC2 option is selected under the service section.
2. Collection type is an optional field.
3. All the regions selected by the user should be listed in the collection type section.
4. Users should be able to select a single S3 bucket for all the regions, also users should be able to select an individual S3 bucket for each region.
5. Data stored in S3 must be removed instantly.

Generic Linux SSM Integration Specification

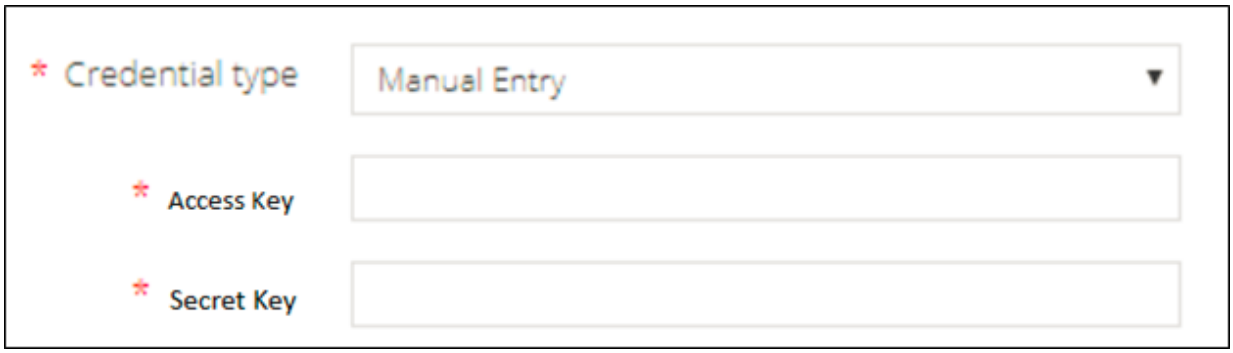
Device Addition

- ApartfromApache, all other instances identifiedfrom Amazon EC2 should be added under Generic Linux under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill on the Generic Linux device addition page.
- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.



Credential management

- Credential Type is a mandatory field.
- When a device is added from a Could account, **Credential-CloudAccount must** be displayed corresponding to a credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.
- While modifying the mandatory details in the Generic Linux form, the user should be able to select a different cloud account credential that is added to the cloud inventory.
- Similarly, while modifying the mandatory details in the Generic Linux form, the user should be able to provide credentials manually in the Generic Linux device addition form.



- Only when the mode of communication is SSM, Access key, and Secret key fields will be displayed under Credential type.

Instances Discovery Specification

Specifications

- It is mandatory for the user to provide credentials and S3 bucket details to identify instances within the Amazon EC2 service.
- With details provided, AppViewX should be able to identify Apache (Linux) server within the Amazon EC2 service and all other instances within the EC2 service will be mapped to Generic Linux in the server tab.
- AppViewX uses the SSM mode of communication to discover certificates within these instances.
- If multiple Apaches run in the same EC2 instance, then only one account will be added under the Apache server tab; if multiple apache running in different EC2 instances; then each instance (apache) will be added as a different account under the Apache server tab.
- All the certificates within these instances should be discovered by AppViewX (when the CERT+ sync field is selected as Managed/ Monitored.
- Should not support Push Certificates including Private Key via SSM. CSR must be generated in the device itself only a signed public key should be pushed to the device.

Chapter 4: Certificate Actions

Overview

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

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

- enroll a certificate
- renew a certificate
- push to device
- reissue a certificate
- revoke a certificate
- regenerate a certificate
- reinstate a certificate

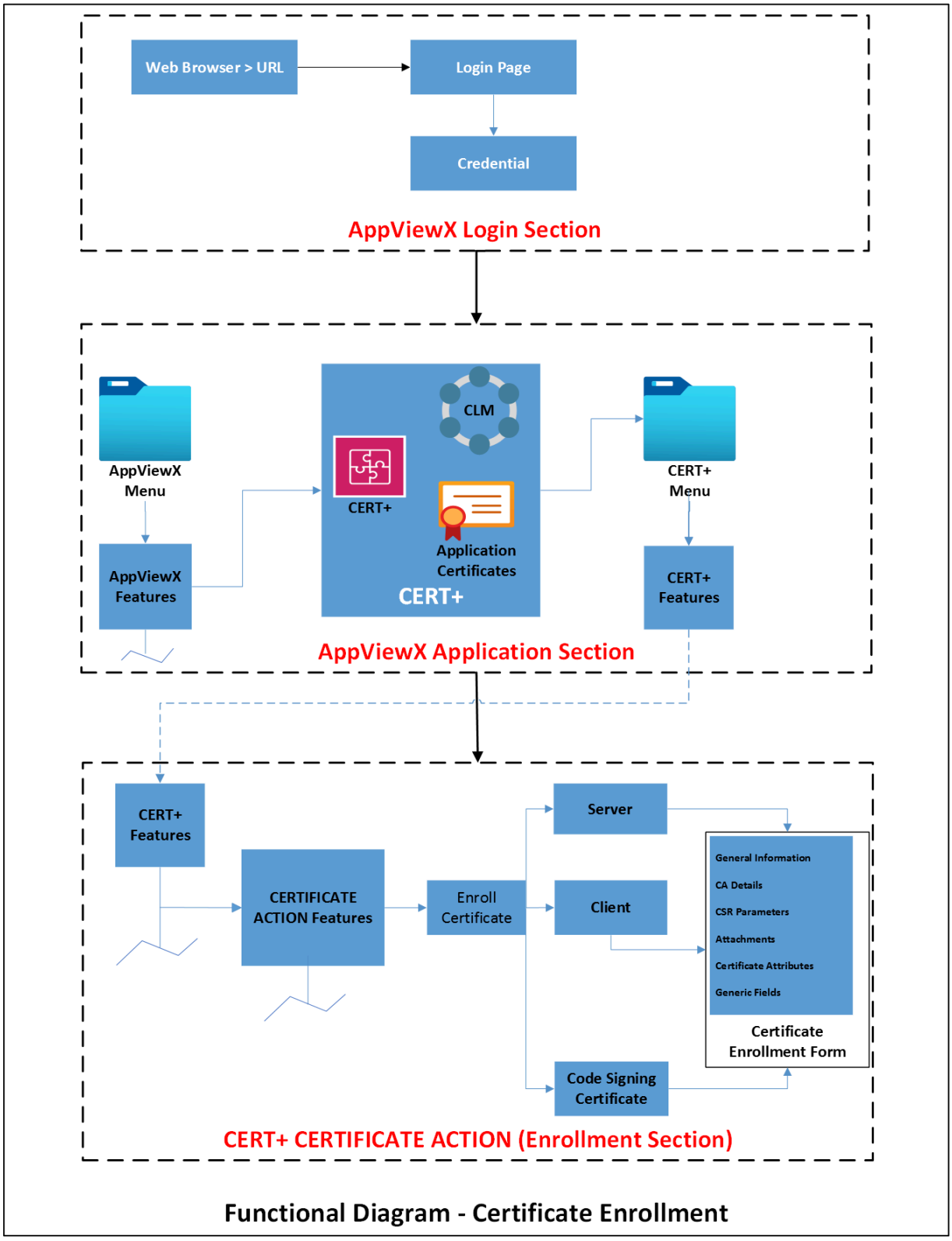
- revocation check
- generate a CSR
- migrate a CA
- run SSL checker.

Enrolling Certificate

Overview

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

For enrolling with any desired CA, the respective account details must be added in AppViewX. Refer to the link to Add a CA Account in AppViewX.



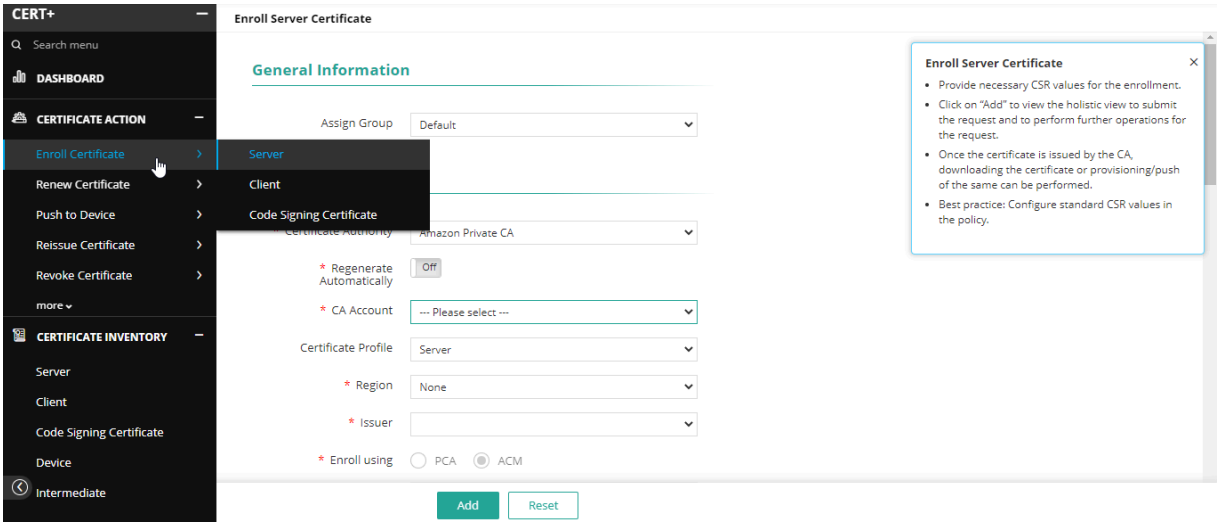
Functional Diagram - Certificate Enrollment

Server Certificate Enrollment

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

To enroll a server certificate:

1. 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 ACTION**.
5. Select **Enroll Certificate**, and then **Server**.
   The **Enroll Server Certificate** page appears.

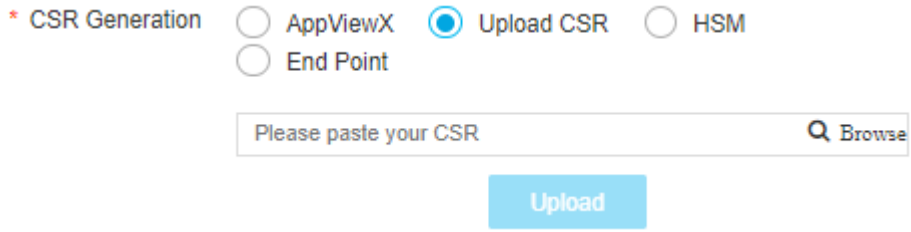


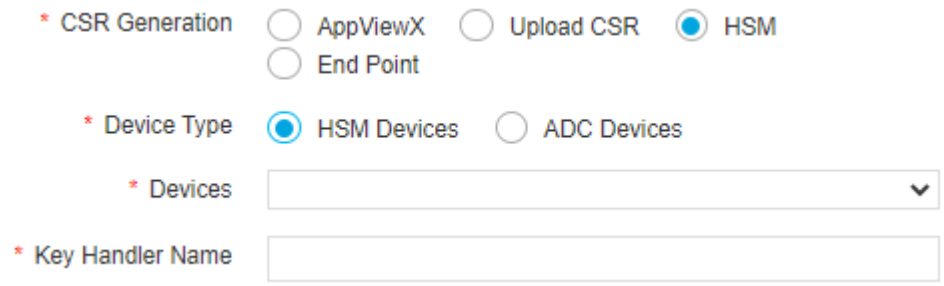
6. **Note:** The Default option is selected.

   In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list.
7. In the **CA Details** section, select/enter the details as follows:
   The following table describes the options available in the CA Details section:

Options	Description
*Certificate Authority	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA details are configured. The possible CAs are: • Amazon • Amazon Private CA • AppViewX • Comodo • Digicert • Entrust ECS • Entrust MPKI • EJBCA • GlobalSign • GoDaddy • Google • InCommon • LetsEncrypt • Microsoft • Enterprise • Microsoft • Standalone • NewCustomCA • Symantec • TATRA BANKA • Thawte • Trust Wave • Certificate Manager.
*Renew Automatically	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certificate.
*CA Account	To which account the enrollment request to be submitted.

Options	Description
Certificate Type	Select the desired certificate type from the dropdown list.
*Division	Select the division to which the certificate must be enrolled. **Note:** This field will be shown only for Digicert CA.
Certificate Profile	Select the Profile to which the Certificate must enroll. **Note:** This field is applicable only for AppViewX CA and Google CA.
*Issuer Location	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Issuer Name	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Region	From the dropdown list, select the region the issuer CA belongs to. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Issuer	From the dropdown list, select the name assigned to the issuer CA. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Enroll using	**Note:** This field is applicable only when Amazon Private CA is the issuer CA. Select the operation mode that was used to onboard the Amazon Private CA.

Options	Description
	Note: If only one of the two operation modes was select while adding the Amazon Private CA, by default, the other operation mode is disabled.
*Connector Name	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** You can enter a maximum of 2000 words in the field.
***CSR Generation**	Select the CSR generation option as required. Options are: • **UploadCSR** - Uploaded CSR will be taken as a source to populate CSR parameters and submit to CA.  • Click the **Browse** button, and then the file. • Click the **Upload** button to upload the selected file. • On uploading CSR successfully, CSR parameters are automatically filled in the CSR section.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• HSM - Private key and CSR will be created in the selected HSM device based on CSR parameters given.


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>Select the type of device as required.

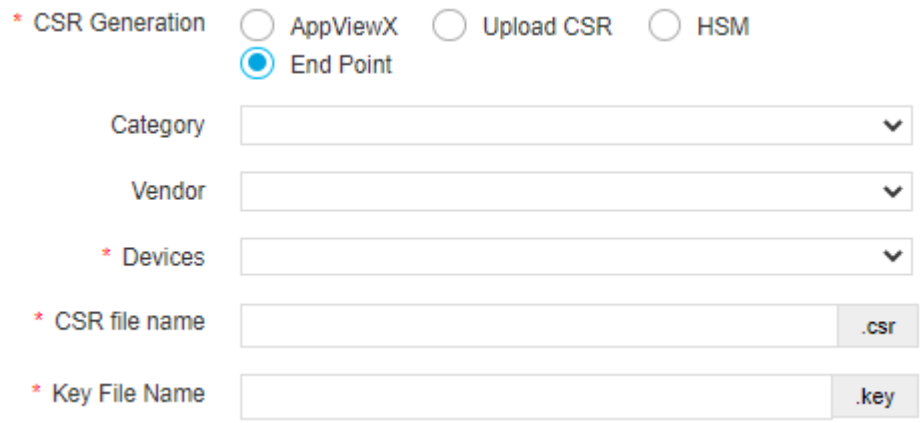
The possible options are:
• HSM Devices
• ADC Devices.</td></tr>
<tr><td>*Vendors</td><td>Select the desired vendors from the dropdown list.

The possible vendors are:
• Safenet
• Thales
• Fortanix.

Note: This option will be enabled only for the ADC device type selected.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.

Note: By default, the None Selected option is enabled.</td></tr>
<tr><td>*Key Handler Name</td><td>Enter the desired handler name in the field.</td></tr>
</table>
</td></tr>
</table>

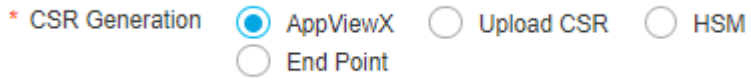
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• End Point - Private key and CSR will be created in the selected End Point device based on CSR parameters given.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>Select the desired category from the dropdown list. The possible options are:
• ADC
• Server
• Firewall.</td></tr>
<tr><td>Vendor</td><td>Select the desired vendor from the dropdown list. The possible options are:
• AVI
• Citrix
• F5
• Ngnix Plus
• HAProxy.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.
Note: By default, the None option is selected.</td></tr>
<tr><td>Tenant</td><td>Enter the tenant id in this field.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*CSR file name</td><td>Enter the name of the CSR file in this field.</td></tr>
<tr><td>*Key File Name</td><td>Enter the name of the key file in this field.</td></tr>
</table>

For all the CA types except Amazon, you have the option to generate the CSR.
• AppViewX - Private key and CSR will be created in AppViewX based on CSR parameters given.

</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

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

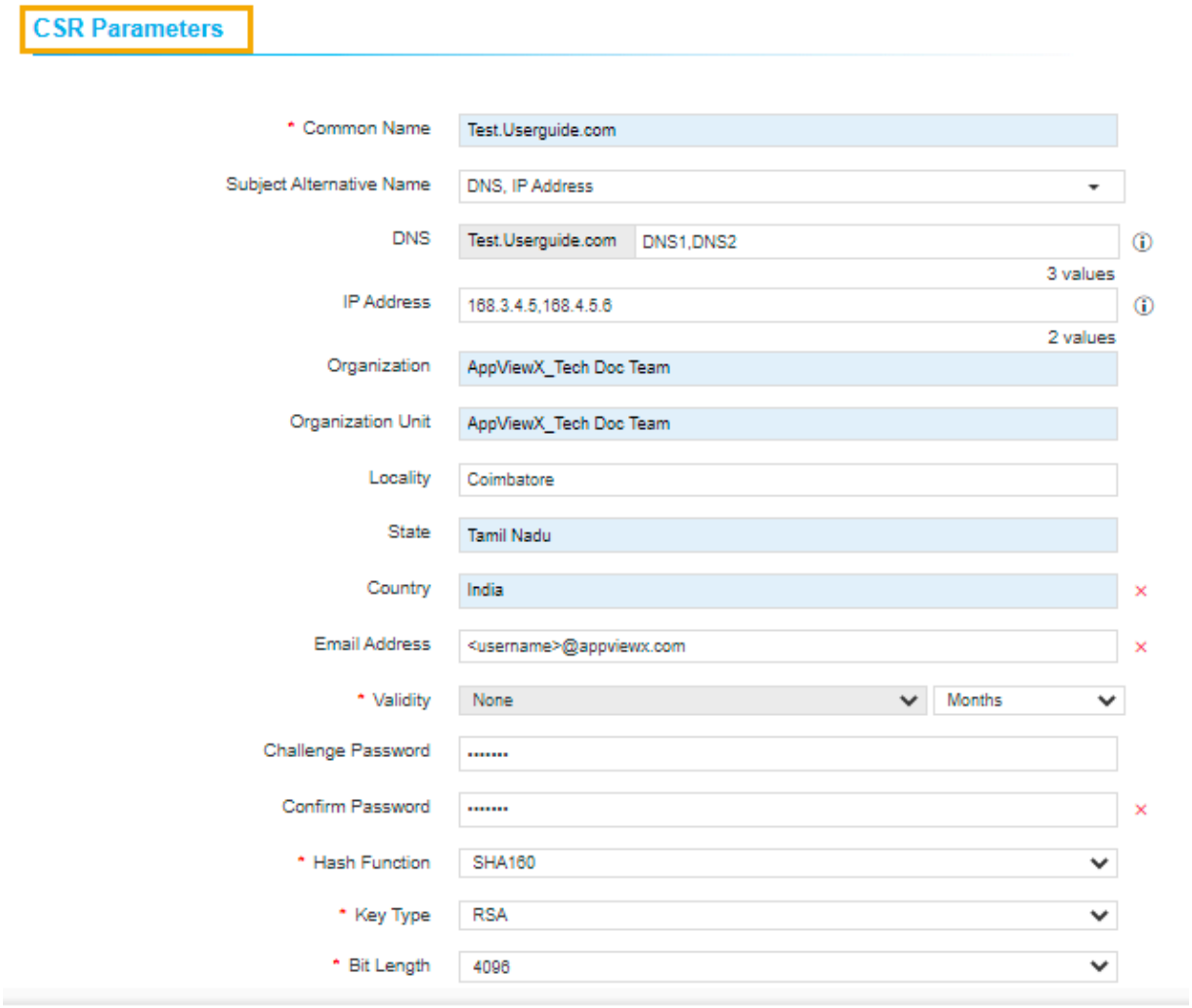
Certificate Enrollment - Strict Policy

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

Certificate Enrollment - Suggestive Policy

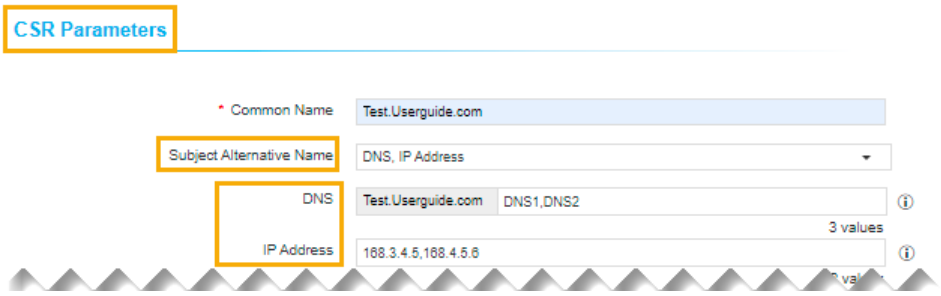
- The Common Name will not be pre-filled from the policy
- The following validation will be seen based on strict policy guidelines.
  - If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
  - If the Common Name's domain name is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

8. In the **CSR Parameters** section, select/enter the details as follows:



The following table describes the options available in the CSR Parameters section:

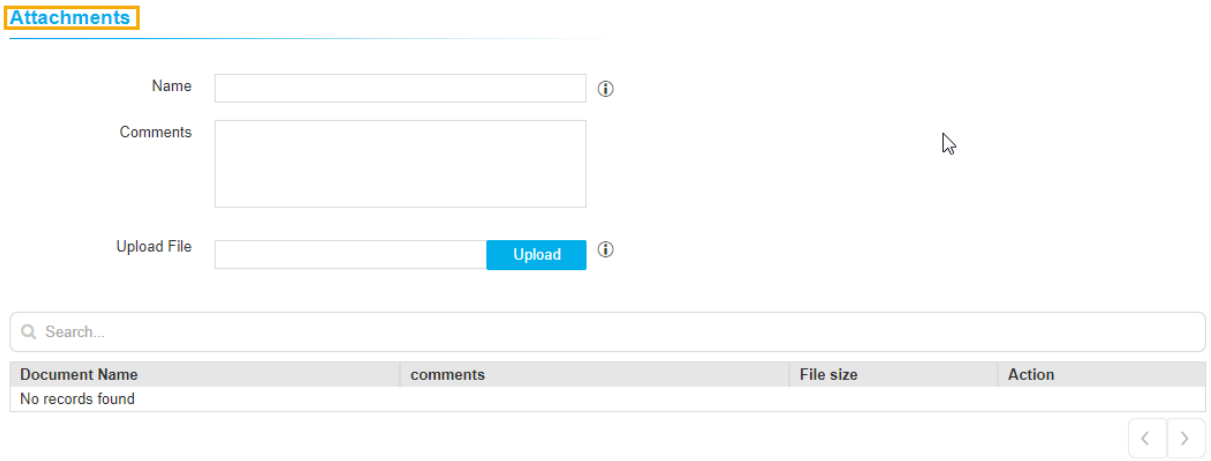
Field	
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parame Select the subject alternative subject name from the dropdown list.

Field	
	 The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holis
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be a
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-f
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-fille
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-ma
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must con

Field	
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editab
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and edita

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

9. In the **Attachments** section is an optional field where the user/admin wants to keep any relevant attachment for the certificate enrollment like approval email, enter the details as follows:

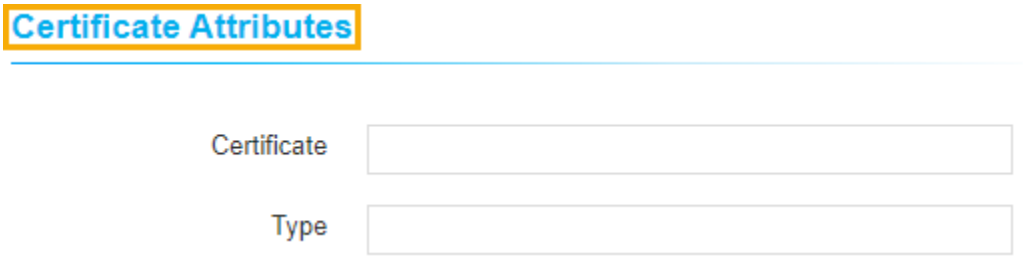


The following table describes the options available in the attachments section:

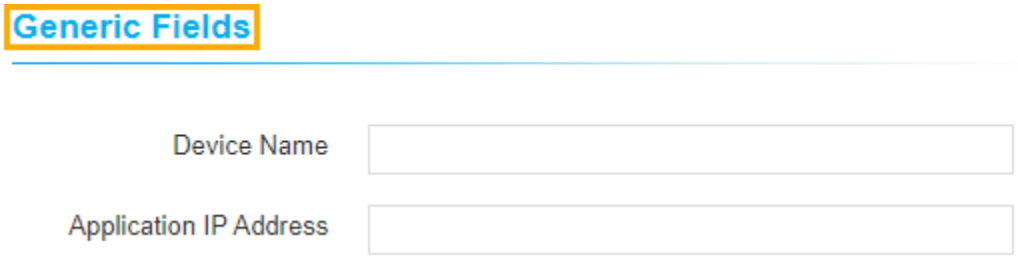
Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** You can enter a maximum of 2000 words in the field.
Upload File	Click the Upload button to select the file.

Field	Description
	Note: During certificate actions, the user can upload and maintain the additional necessary documents.

10. Other than the CSR fields, the user can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration --> certificate attributes, it will be reflected on the enrolment page:



11. Enter the **Device Name** and the **Application IP Address** in the **Generic Fields** section.



The following table describes the options available in the generic fields section:

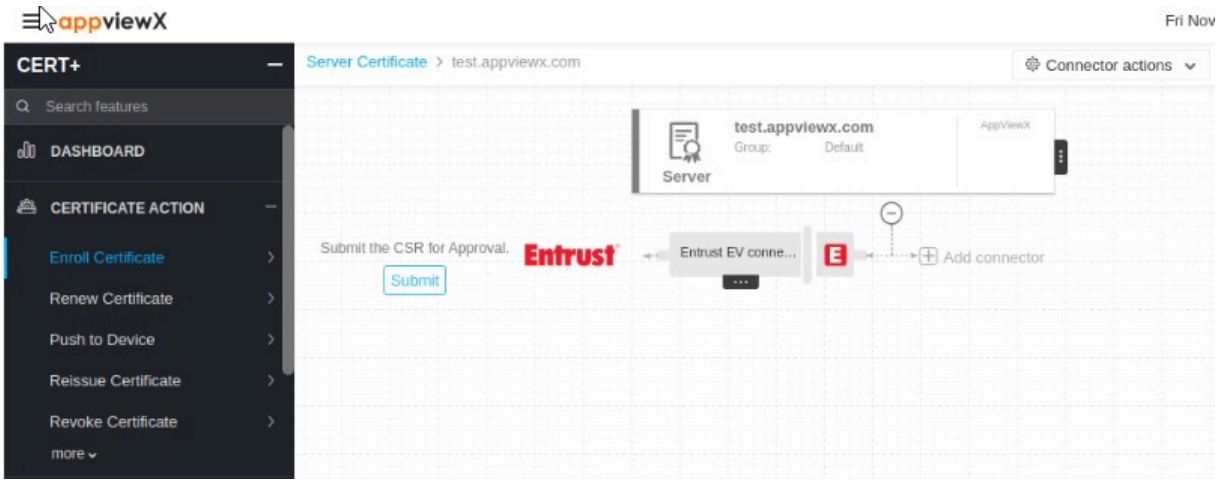
Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the application IP address in this field.
	Note: Application IP address and Device name are the default fields to maintain IP address and device information if needed. Non-mandatory fields, skip this if you do not want to enter values.

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

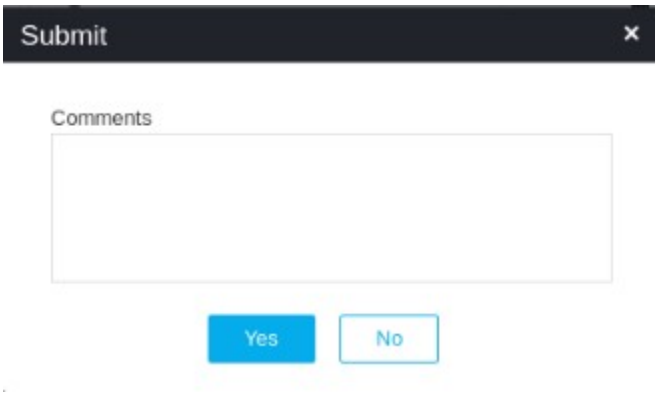
    Note: Vendor-specific details are required only for certificates issued by Google CA.

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

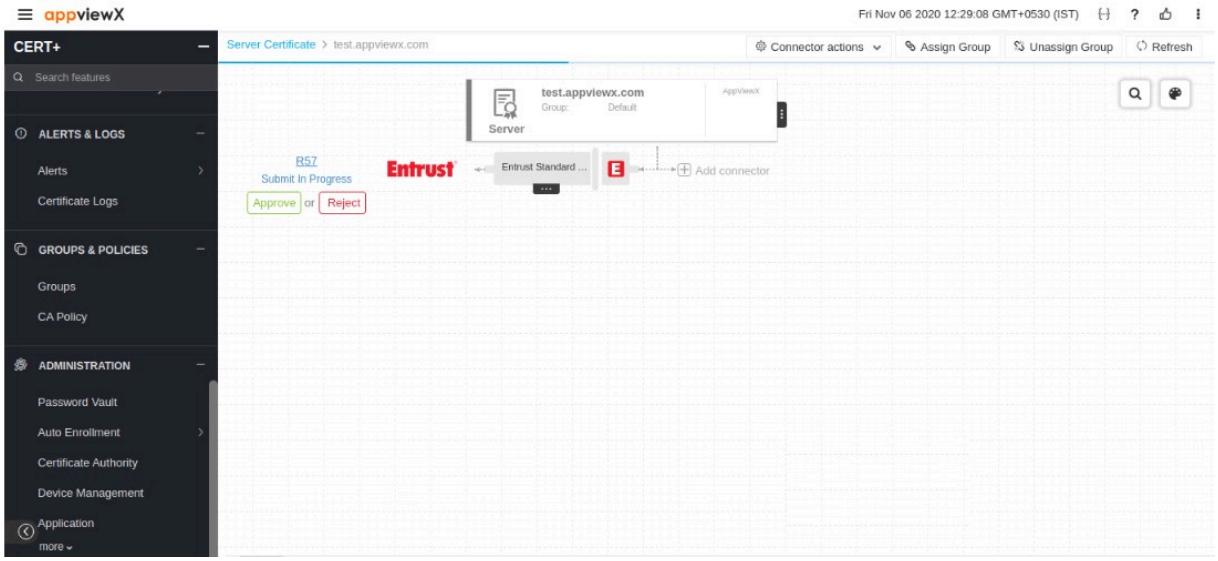
13. Click the **Add** button.
14. Once the details are added, it will redirect to the page where the user can see the respective CSR and CA details added as a connector. This page is called holistic view and from here any action on the certificate can be performed including provisioning the certificate to a server.



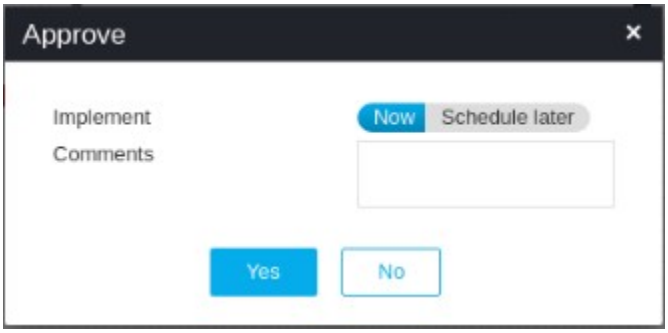
15. Click the **Submit** button to trigger the request.
16. Once the submit action is triggered, the **Submit** pop-up window appears. Add comments if needed, and then click the **Yes** button. If an approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.



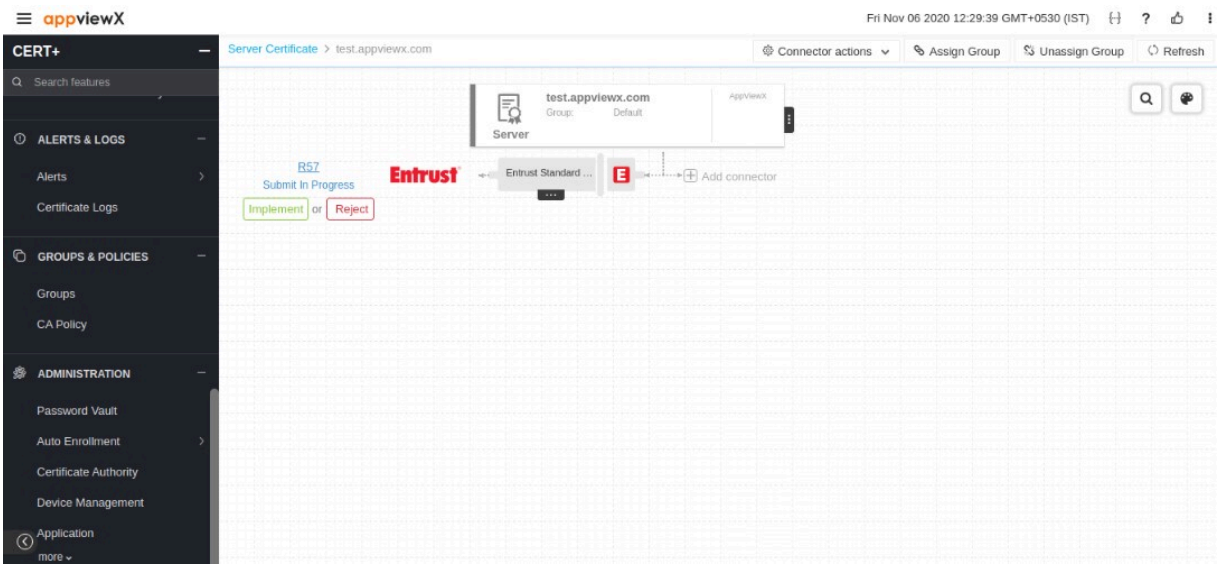
17. Click **Approve** to proceed.



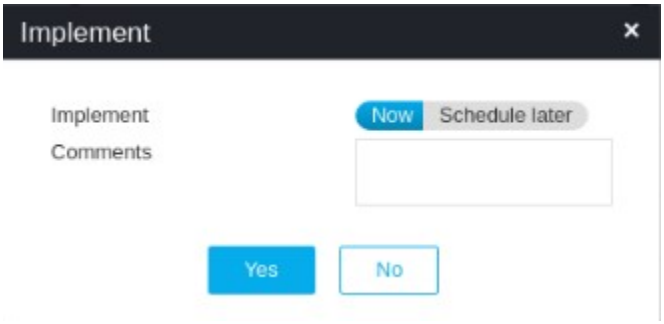
18. The **Approve** pop-up window appears. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.



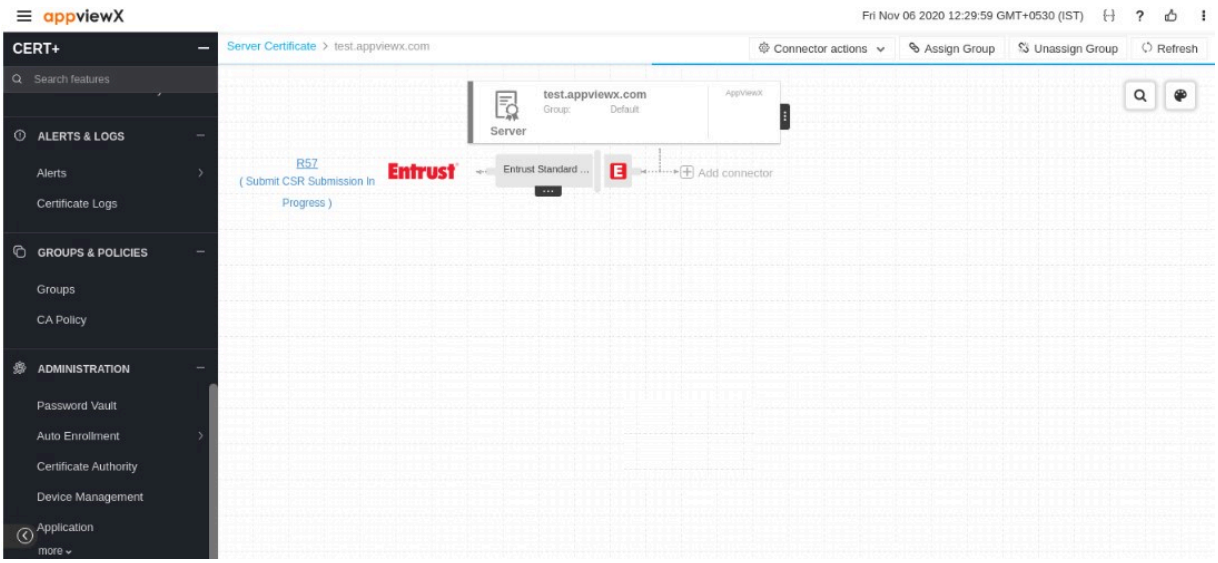
19. Enter the comments in the field.
20. Click **Yes**.
21. Once approved, the user can see the Implement option in the holistic view. Click **Implement**.



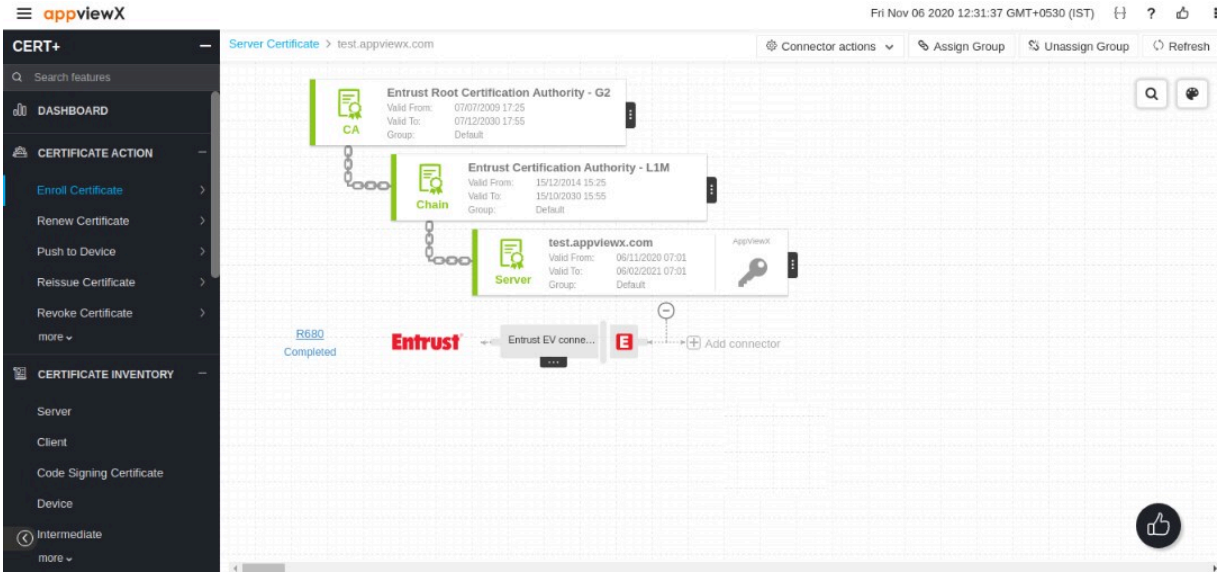
22. The **Implement** pop-up window appears. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



23. Enter the comments in the field.
24. Click **Yes**.
25. CSR Submission to CA is in progress.



26. Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.
27. If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.
28. If auto-approval disabled in the targeted CA, the user has to be logged into CA and approve the request.



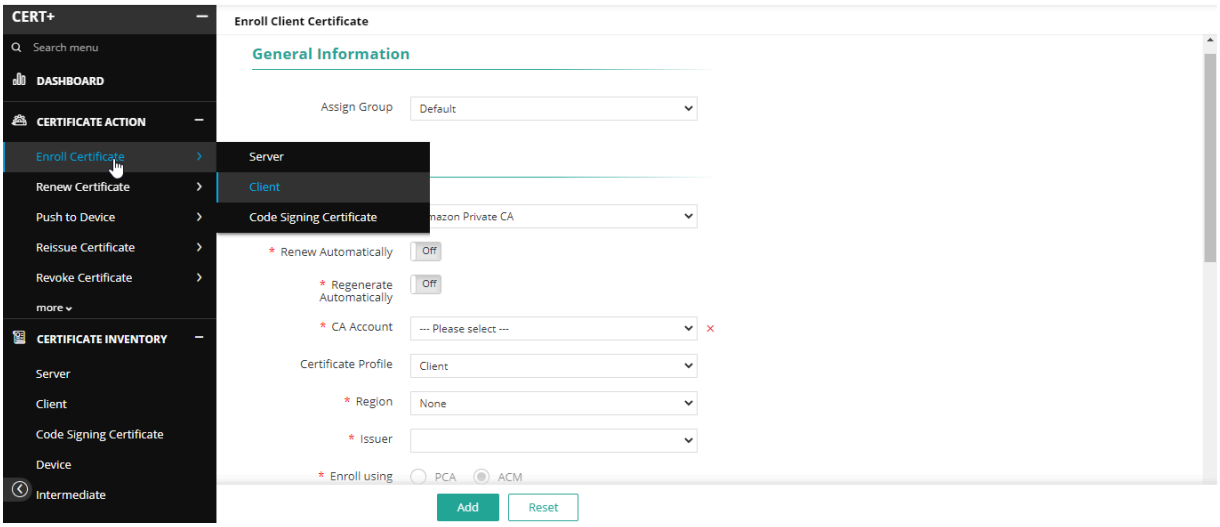
29. Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

Client Certificate Enrollment

Client certificate enrollment refers to the process of creating a digital ID for an individual/device for authentication/encryption purposes. It follows the same process as a Client certificate. These certificates can not be hosted on Clients.

Steps to enroll a client certificate,

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 ACTION**.
5. Select **Enroll Certificate**, and then **Client**.
   The **Enroll Client Certificate** page appears.



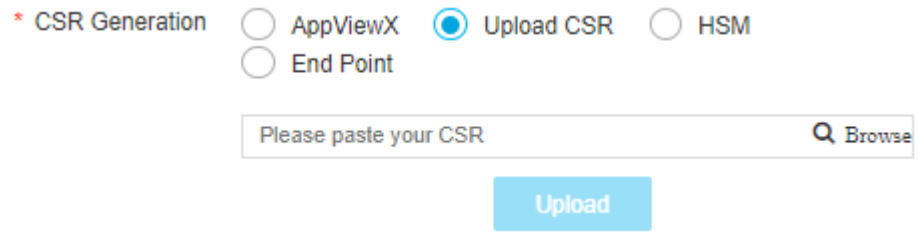
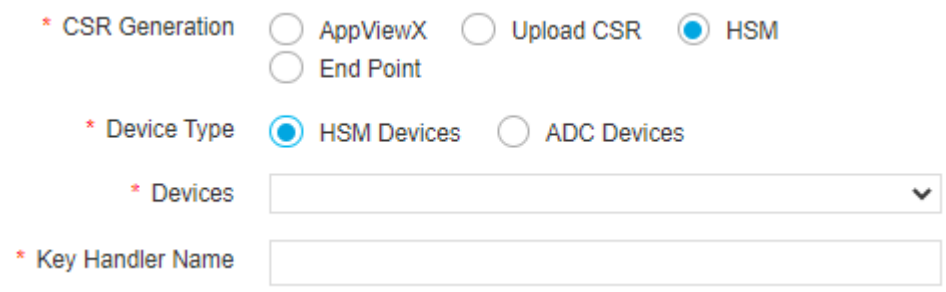
6. **Note:** The Default option is selected.

   In the **General Information** section of the **Enroll Client Certificate** page, select the desired **Assign Group** from the dropdown list.
7. In the **CA Details** section, select/enter the details as follows:

Options	Description
*Certificate Authority	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA details are configured. The possible CAs are:

Options	Description
	• Amazon • AppViewX • Comodo • Digicert • Entrust ECS • Entrust MPKI • EJBCA • GlobalSign • GoDaddy • Google • InCommon • LetsEncrypt • Microsoft • Enterprise • Microsoft • Standalone • NewCustomCA • Symantec • TATRA BANKA • Thawte • Trust Wave • Certificate Manager.
*Renew Automatically	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certificate.
*CA Account	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
*Division	Select the division to which the certificate must be enrolled.

Options	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	Select the Profile to which the Certificate must enroll. **Note:** This field is applicable only for AppViewX CA and Google CA.
*Issuer Location	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Issuer Name	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Region	From the dropdown list, select the region the issuer CA belongs to. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Issuer	From the dropdown list, select the name assigned to the issuer CA. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Enroll using	**Note:** This field is applicable only when Amazon Private CA is the issuer CA. Select the operation mode that was used to onboard the Amazon Private CA. **Note:** If only one of the two operation modes was select while adding the Amazon Private CA, by default, the other operation mode is disabled.

Options	Description
*Connector Name	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** You can enter a maximum of 2000 words in the field.
***CSR Generation**	Select the CSR generation option as required. Options are: • **UploadCSR** - Uploaded CSR will be taken as a source to populate CSR parameters and submit to CA.  • Click the **Browse** button, and then the file. • Click the **Upload** button to upload the selected file. • On uploading CSR successfully, CSR parameters are automatically filled in the CSR section. • **HSM** - Private key and CSR will be created in the selected HSM device based on CSR parameters given. 

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>Select the type of device as required.

The possible options are:

• HSM Devices
• ADC Devices.</td></tr>
<tr><td>*Vendors</td><td>Select the desired vendors from the dropdown list.

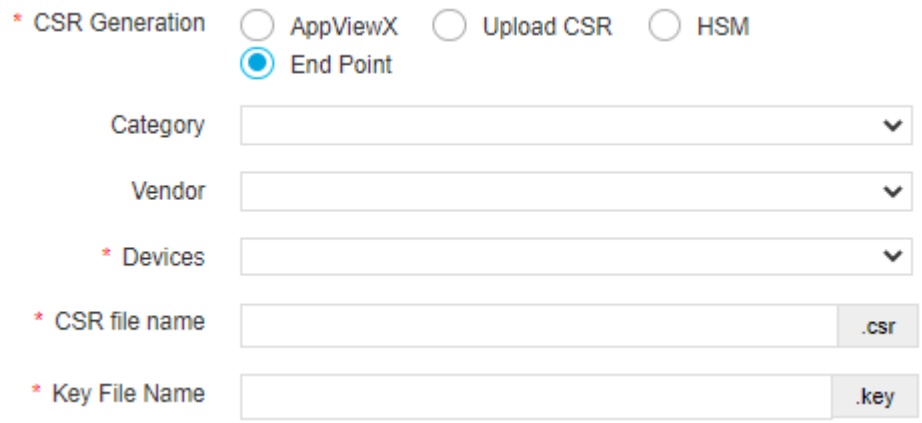
The possible vendors are:

• Safenet
• Thales
• Fortanix.

Note: This option will be enabled only for the ADC device type selected.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.

Note: By default, the None Selected option is enabled.</td></tr>
<tr><td>*Key Handler Name</td><td>Enter the desired handler name in the field.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• End Point - Private key and CSR will be created in the selected End Point device based on CSR parameters given.

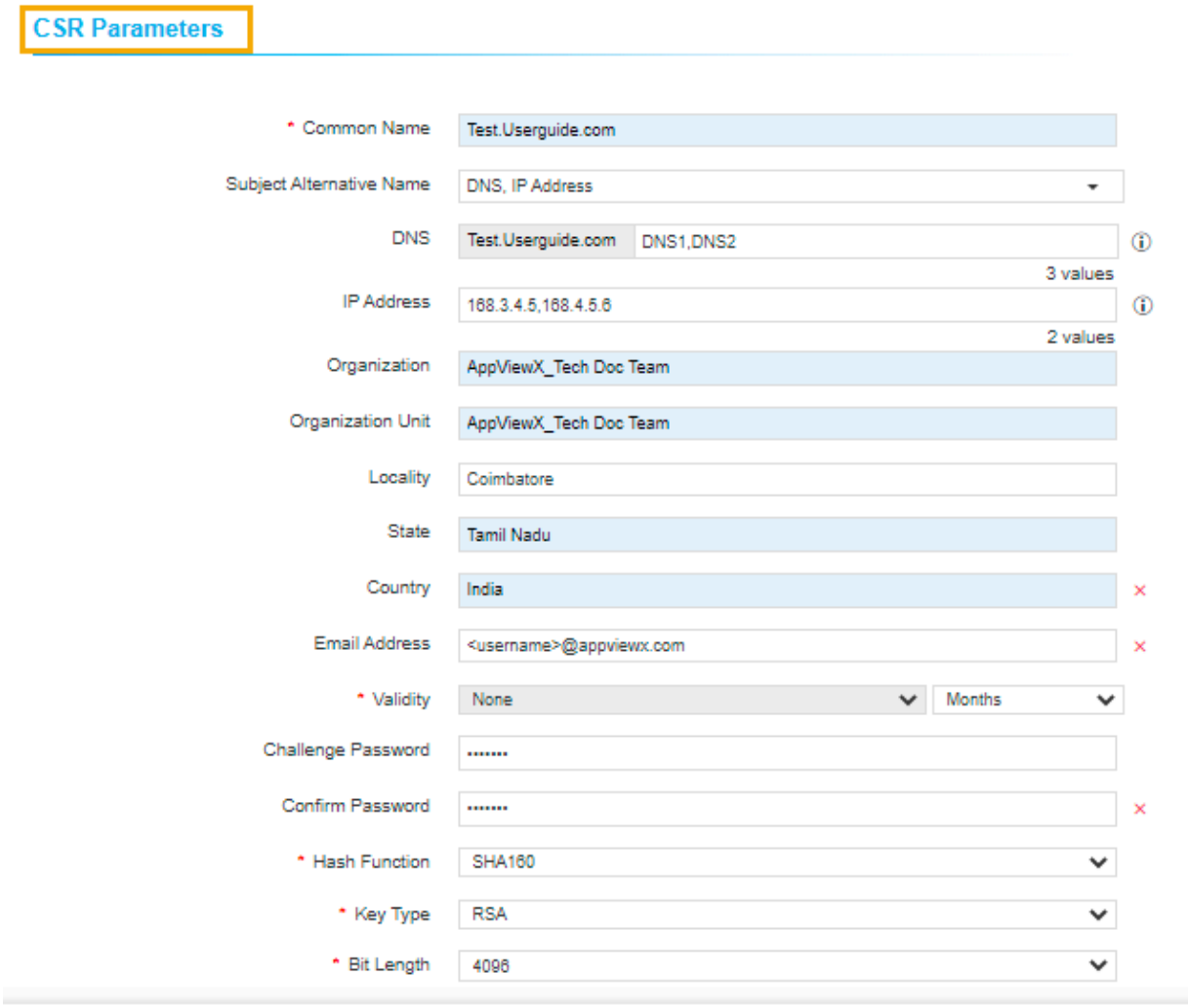


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>Select the desired category from the dropdown list. The possible options are:
• ADC
• Client
• Firewall.</td></tr>
<tr><td>Vendor</td><td>Select the desired vendor from the dropdown list. The possible options are:
• AVI
• Citrix
• F5
• Ngnix Plus
• HAProxy.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.
Note: By default, the None option is selected.</td></tr>
<tr><td>Tenant</td><td>Enter the tenant id in this field.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*CSR file name</td><td>Enter the name of the CSR file in this field.</td></tr>
<tr><td>*Key File Name</td><td>Enter the name of the key file in this field.</td></tr>
</table>
For all the CA types except Amazon, you have the option to generate the CSR.
• AppViewX - Private key and CSR will be created in AppViewX based on CSR parameters given.

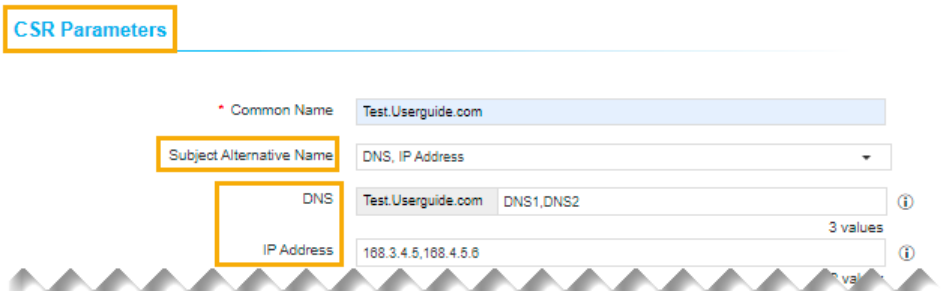
* CSR Generation ◉ AppViewX ○ Upload CSR ○ HSM ○ End Point
</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

8. In the **CSR Parameters** section, select/enter the details as follows:



The following table describes the options available in the CSR Parameters section:

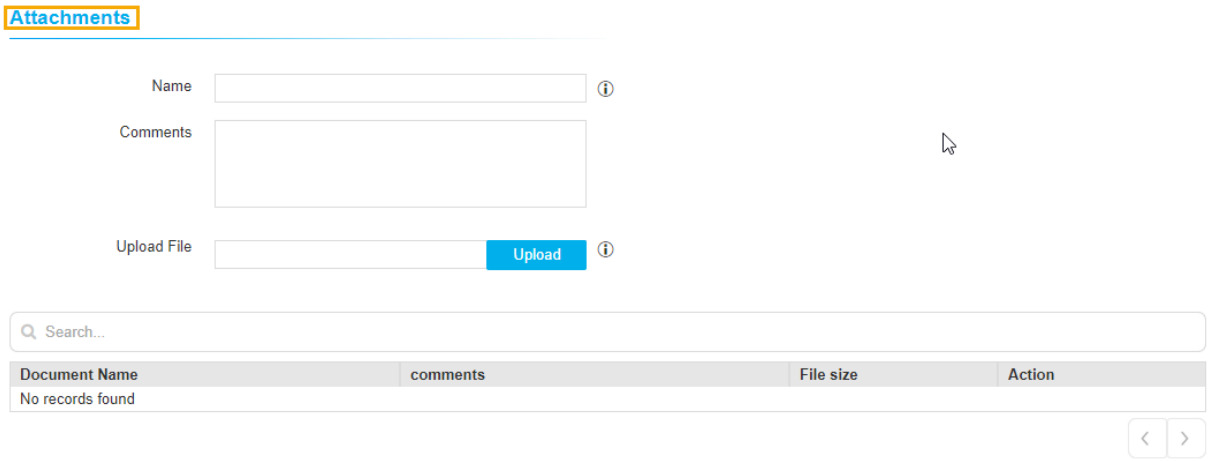
Field	
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parame Select the subject alternative subject name from the dropdown list.

Field	
	 The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holis
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be a
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-f
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-fille
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-ma
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must con

Field	
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editab
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and edita

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

9. In the **Attachments** section is an optional field where the user/admin wants to keep any relevant attachment for the certificate enrollment like approval email, enter the details as follows:

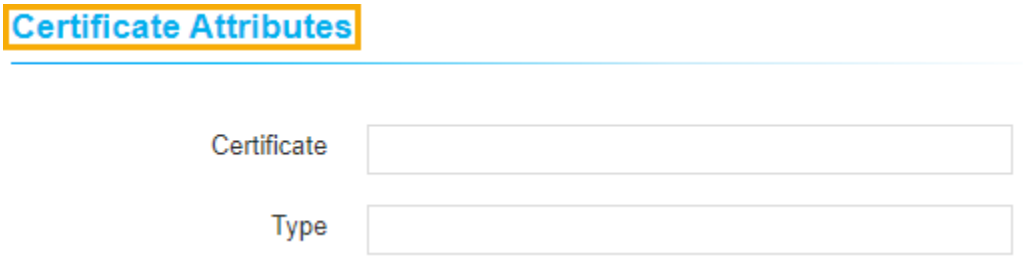


The following table describes the options available in the attachments section:

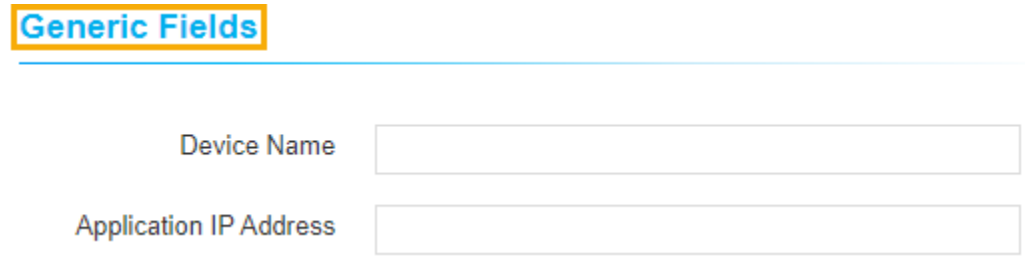
Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** You can enter a maximum of 2000 words in the field.
Upload File	Click the Upload button to select the file.

Field	Description
	Note: During certificate actions, the user can upload and maintain the additional necessary documents.

10. Other than the CSR fields, the user can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration --> certificate attributes, it will be reflected on the enrolment page:



11. Enter the **Device Name** and the **Application IP Address** in the **Generic Fields** section.



The following table describes the options available in the generic fields section:

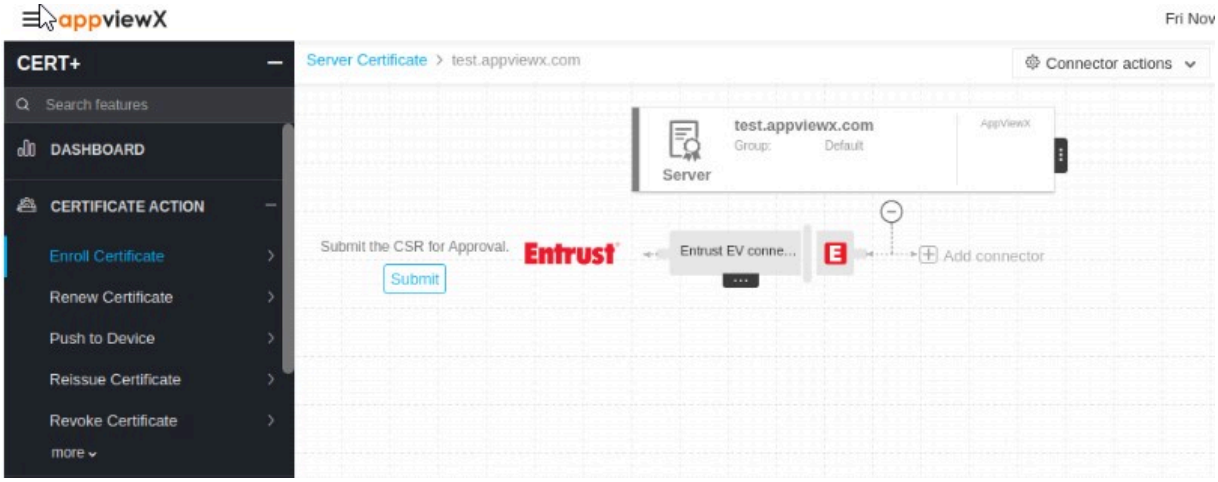
Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the application IP address in this field.
	Note: Application IP address and Device name are the default fields to maintain IP address and device information if needed. Non-mandatory fields, skip this if you do not want to enter values.

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

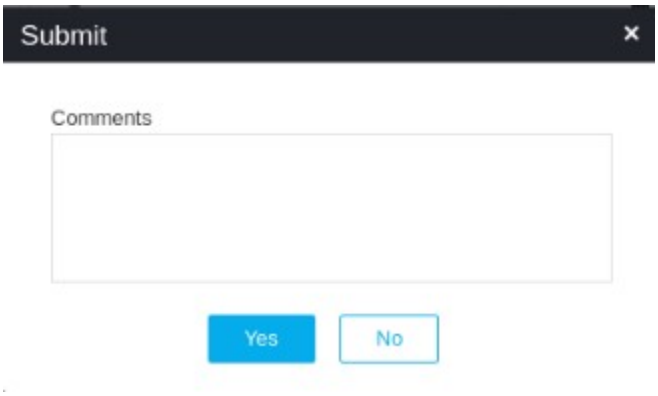
    Note: Vendor-specific details are required only for certificates issued by Google CA.

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

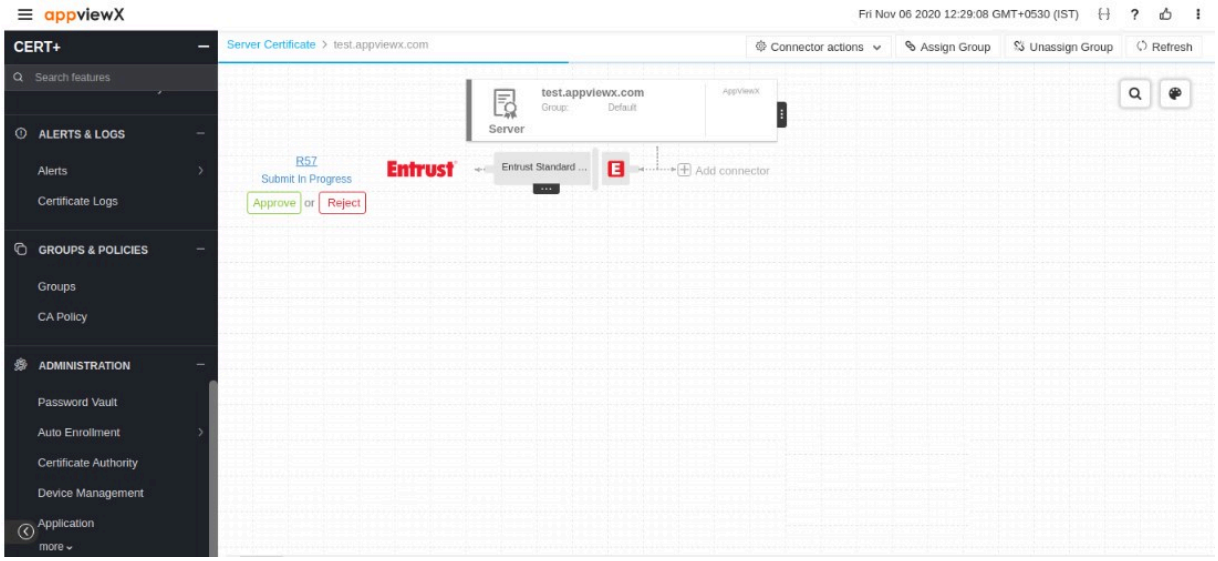
13. Click the **Add** button.
14. Once the details are added, it will redirect to the page where the user can see the respective CSR and CA details added as a connector. This page is called holistic view and from here any action on the certificate can be performed including provisioning the certificate to a Client.



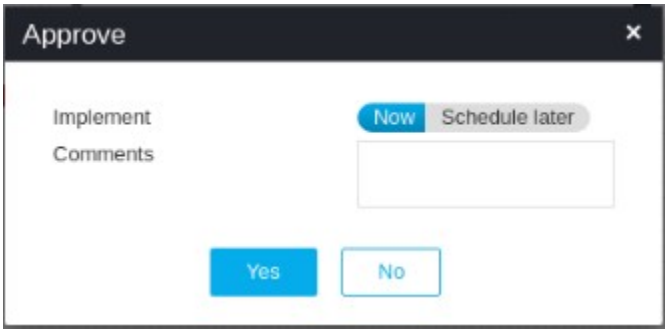
15. Click the **Submit** button to trigger the request.
16. Once the submit action is triggered, the **Submit** pop-up window appears. Add comments if needed, and then click the **Yes** button. If an approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.



17. Click **Approve** to proceed.

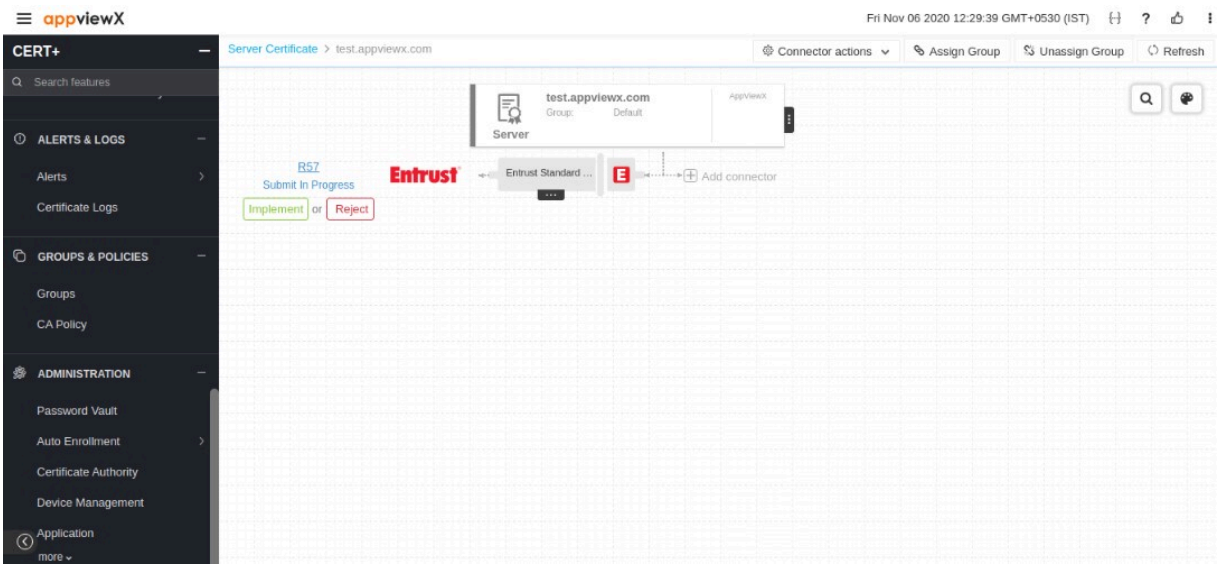


18. The **Approve** pop-up window appears. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.

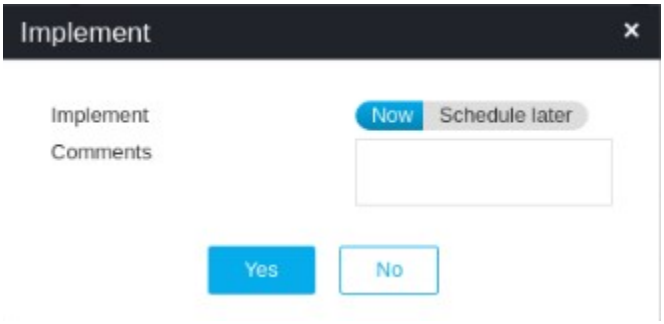


   a. Enter the comments in the field.
   b. Click **Yes**.

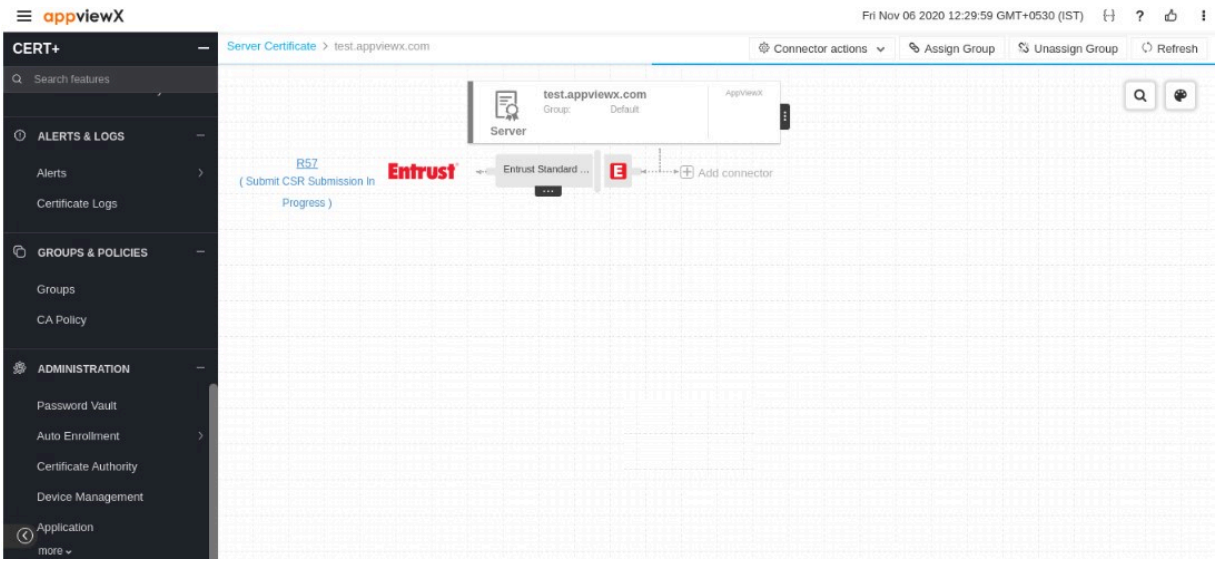
19. Once approved, the user can see the Implement option in the holistic view. Click **Implement**.



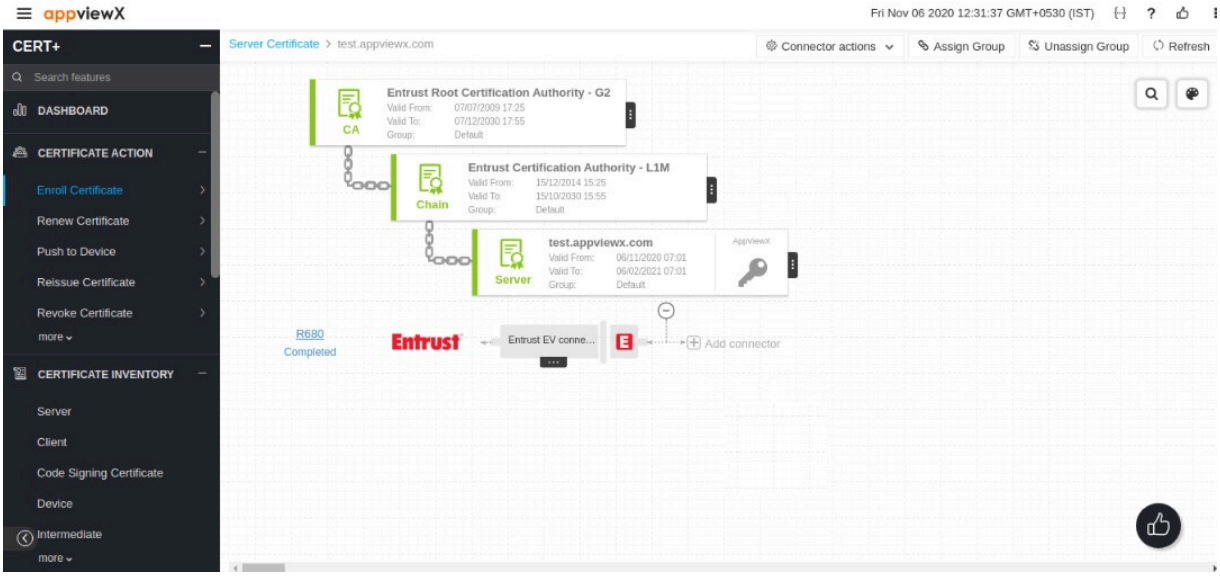
20. The **Implement** pop-up window appears. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



    a. Enter the comments in the field.
    b. Click **Yes**.
21. CSR Submission to CA is in progress.



22. Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.
23. If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.
24. If auto-approval disabled in the targeted CA, the user has to be logged into CA and approve the request.



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

Code Signing Certificate Enrollment

Overview

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

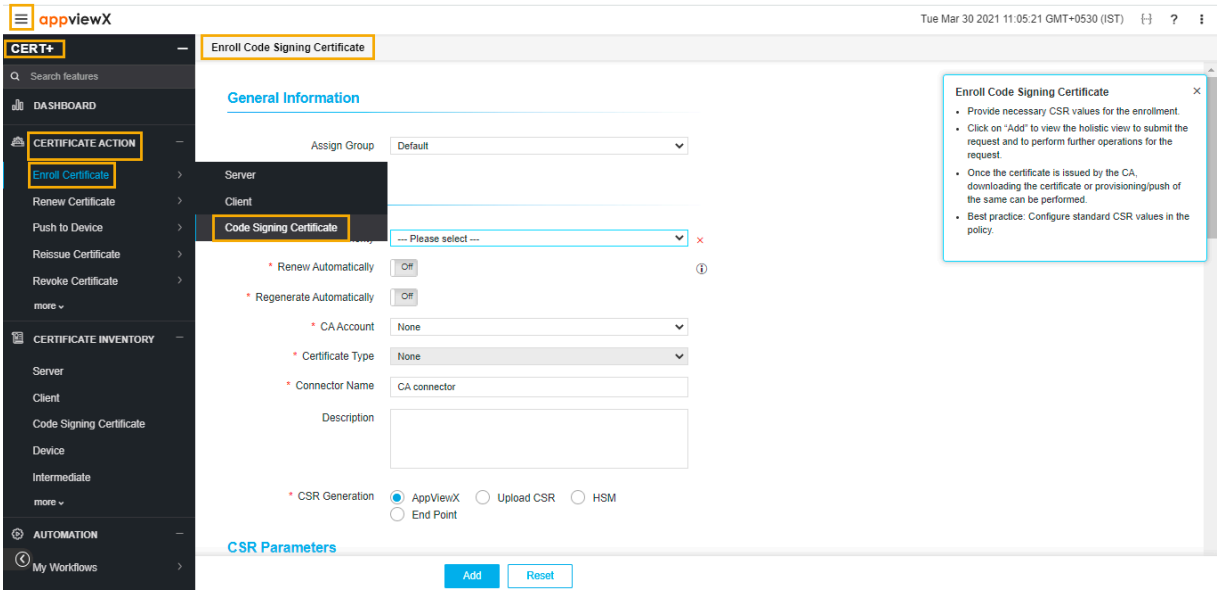
• Code Signing Certificate Enrollment

Code Signing Certificate Enrollment

Code Signing certificate enrollment refers to the process of creating a digital ID for an individual/device for authentication/encryption purposes. It follows the same process as a server certificate. These certificates can not be hosted on servers.

Steps to enroll a Code Signing certificate,

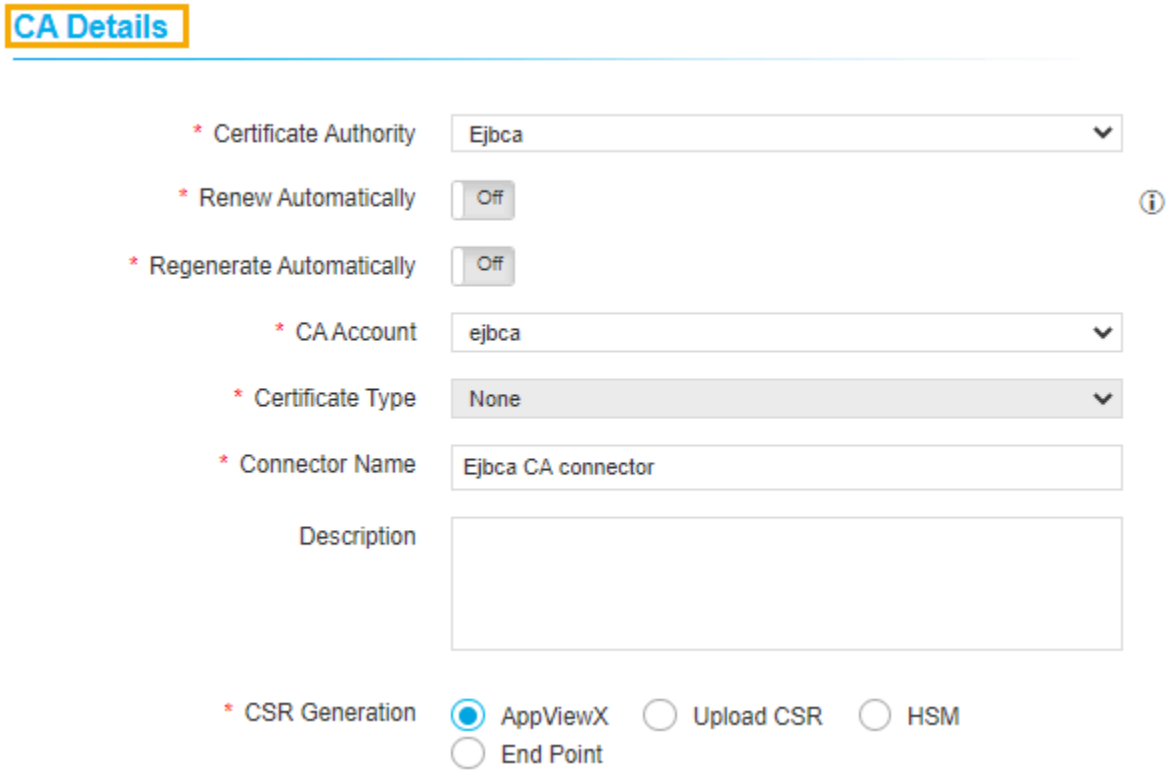
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Enroll Certificate**, and then **Client**.
   The **Enroll Code Signing Certificate** page appears.



6. **Note:** The Default option is selected.

   In the **General Information** section of the **Enroll Code Signing Certificate** page, select the desired **Assign Group** from the dropdown list.

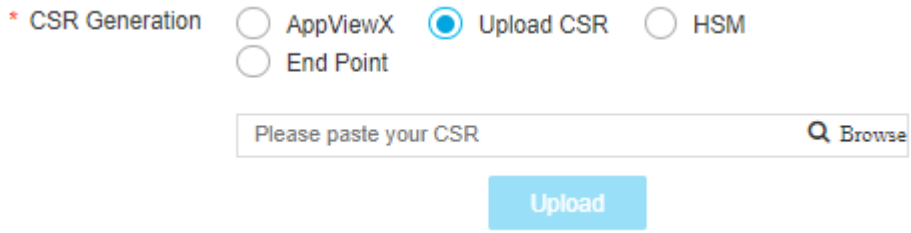
7. In the **CA Details** section, select/enter the details as follows:

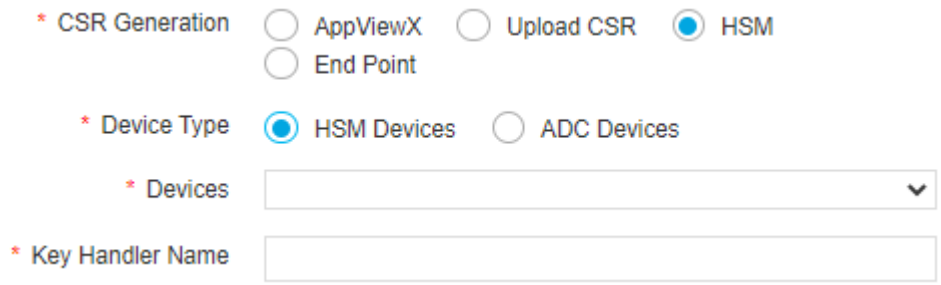


The following table describes the options available in the CA Details section:

Options	Description
*Certificate Authority	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA details are configured. The possible CAs are: • Amazon • AppViewX • Comodo • Digicert • Entrust ECS • Entrust MPKI • EJBCA • GlobalSign • GoDaddy • Google • InCommon • LetsEncrypt • Microsoft • Enterprise • Microsoft • Standalone • NewCustomCA • Symantec • TATRA BANKA • Thawte • Trust Wave • Certificate Manager.
*Renew Automatically	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certificate.

Options	Description
*CA Account	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
*Division	Select the division to which the certificate must be enrolled. **Note:** This field will be shown only for Digicert CA.
Certificate Profile	Select the Profile to which the Certificate must enroll. **Note:** This field is applicable only for AppViewX CA and Google CA.
*Issuer Location	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Issuer Name	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Connector Name	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** You can enter a maximum of 2000 words in the field.
***CSR Generation**	Select the CSR generation option as required. Options are:

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• UploadCSR - Uploaded CSR will be taken as a source to populate CSR parameters and submit to CA.


• Click the Browse button, and then the file.
• Click the Upload button to upload the selected file.
• On uploading CSR successfully, CSR parameters are automatically filled in the CSR section.
• HSM - Private key and CSR will be created in the selected HSM device based on CSR parameters given.


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>Select the type of device as required.

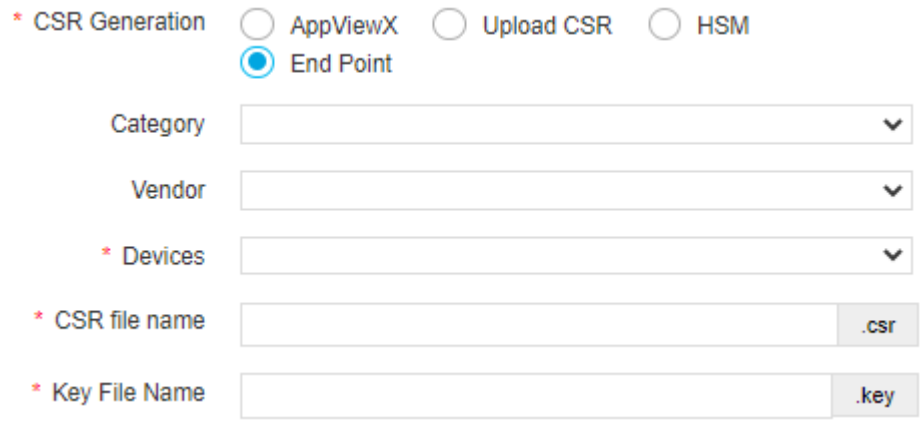
The possible options are:
• HSM Devices
• ADC Devices.</td></tr>
<tr><td>*Vendors</td><td>Select the desired vendors from the dropdown list.

The possible vendors are:</td></tr>
</table>
</td></tr>
</table>

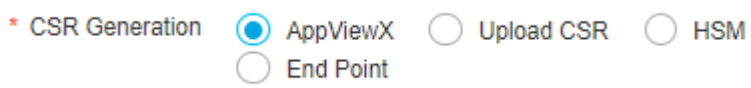
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>• Safenet
• Thales
• Fortanix.

Note: This option will be enabled only for the ADC device type selected.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.

Note: By default, the None Selected option is enabled.</td></tr>
<tr><td>*Key Handler Name</td><td>Enter the desired handler name in the field.</td></tr>
</table>
• End Point - Private key and CSR will be created in the selected End Point device based on CSR parameters given.

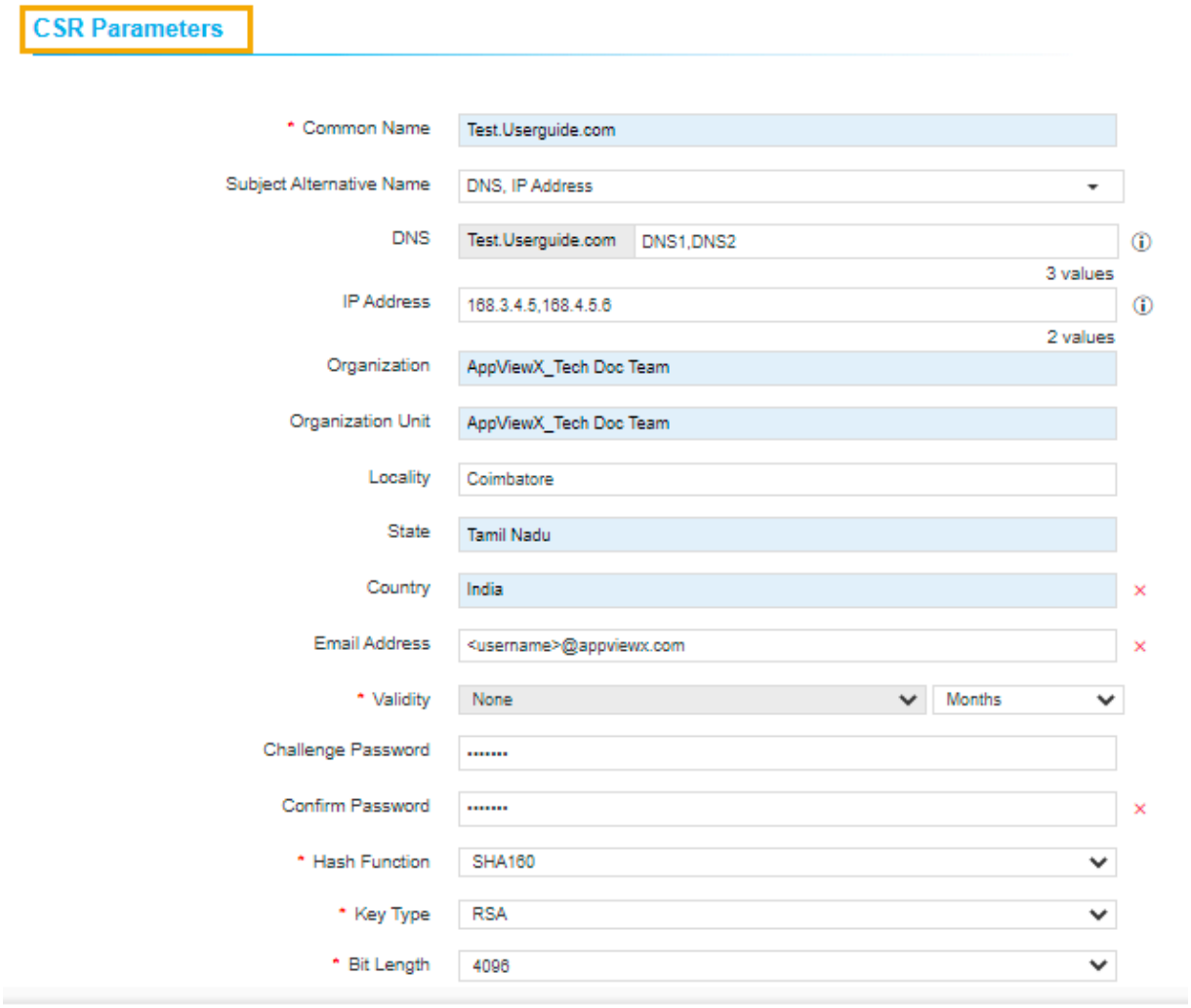


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>Select the desired category from the dropdown list. The possible options are:</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>• ADC
• Code Signing
• Firewall.</td></tr>
<tr><td>Vendor</td><td>Select the desired vendor from the dropdown list. The possible options are:
• AVI
• Citrix
• F5
• Ngnix Plus
• HAProxy.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.
Note: By default, the None option is selected.</td></tr>
<tr><td>Tenant</td><td>Enter the tenant id in this field.</td></tr>
<tr><td>*CSR file name</td><td>Enter the name of the CSR file in this field.</td></tr>
<tr><td>*Key File Name</td><td>Enter the name of the key file in this field.</td></tr>
</table>
For all the CA types except Amazon, you have the option to generate the CSR.
• AppViewX - Private key and CSR will be created in AppViewX based on CSR parameters given.
 

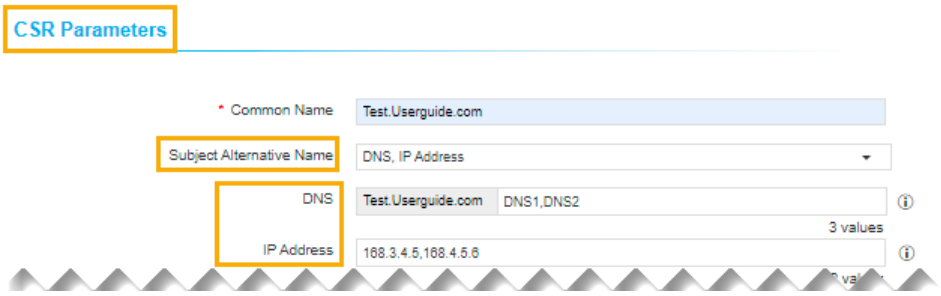
</td></tr>
<tr><td colspan="2">Note: The asterisk (*) symbol indicates a mandatory field.</td></tr>
</table>

8. In the **CSR Parameters** section, select/enter the details as follows:



The following table describes the options available in the CSR Parameters section:

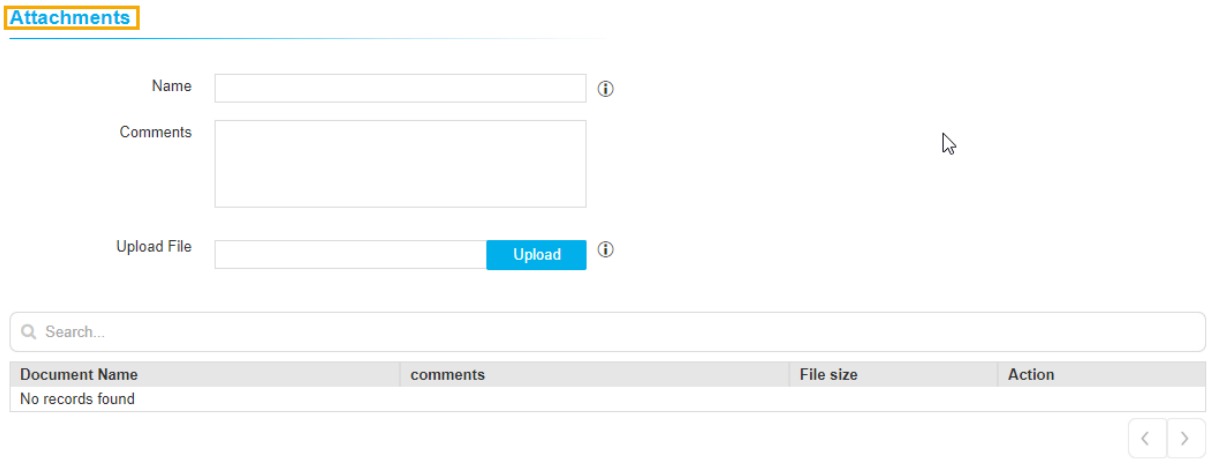
Field	
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parame Select the subject alternative subject name from the dropdown list.

Field	
	 The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holis
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be a
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-f
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-fille
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-ma
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must con

Field	
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editab
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and edita

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

9. In the **Attachments** section is an optional field where the user/admin wants to keep any relevant attachment for the certificate enrollment like approval email, enter the details as follows:

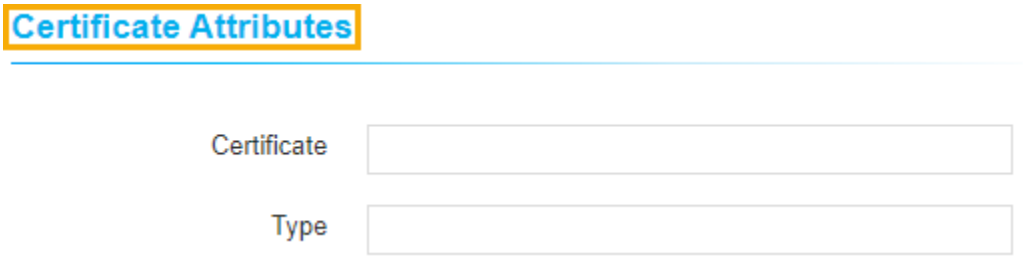


The following table describes the options available in the attachments section:

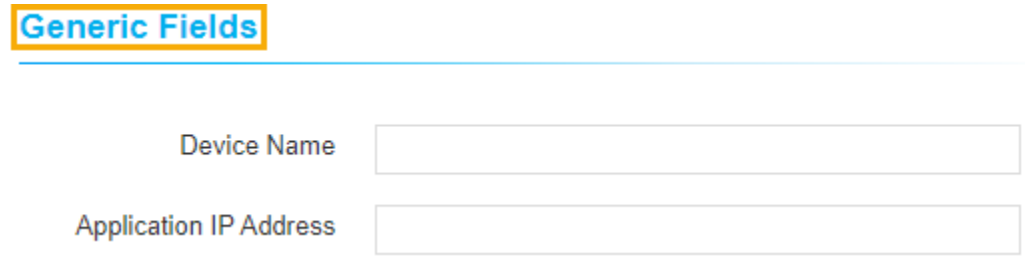
Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** You can enter a maximum of 2000 words in the field.
Upload File	Click the Upload button to select the file.

Field	Description
	Note: During certificate actions, the user can upload and maintain the additional necessary documents.

10. Other than the CSR fields, the user can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration --> certificate attributes, it will be reflected on the enrolment page:



11. Enter the **Device Name** and the **Application IP Address** in the **Generic Fields** section.



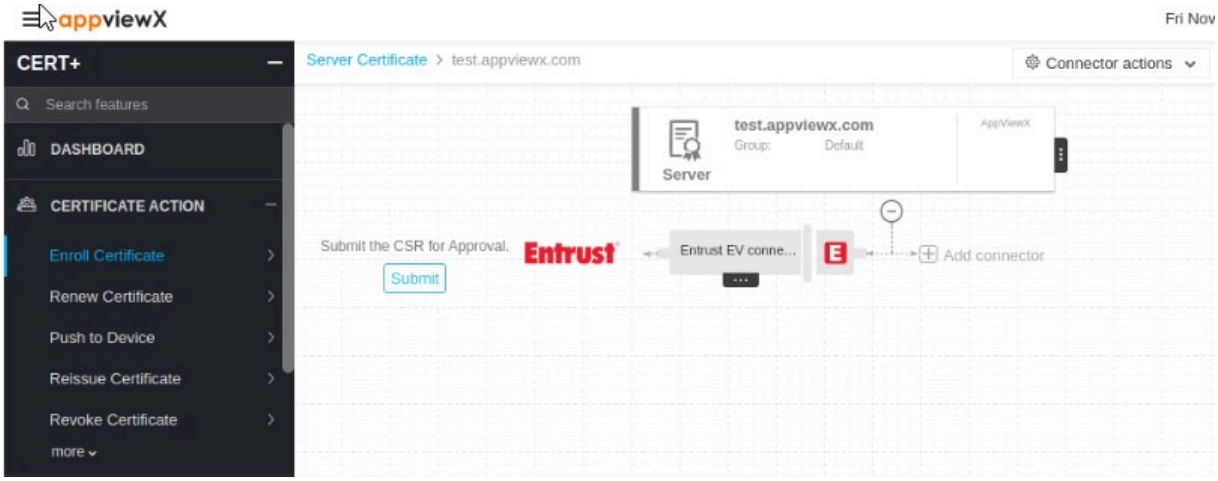
The following table describes the options available in the generic fields section:

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the application IP address in this field.
	Note: Application IP address and Device name are the default fields to maintain IP address and device information if needed. Non-mandatory fields, skip this if you do not want to enter values.

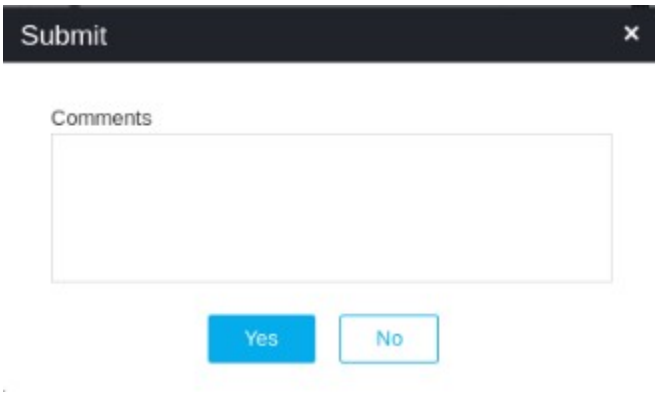
12. In the **Vendor-Specific Details** section, CA-specific details can be provided here (Template name for Microsoft CA). Some of the CAs will expect additional details other than CSR parameters for their operational purposes.
    - By default, the **Certificate ID** is auto-populated based on the value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

    Note: Vendor-specific details are required only for certificates issued by Google CA.

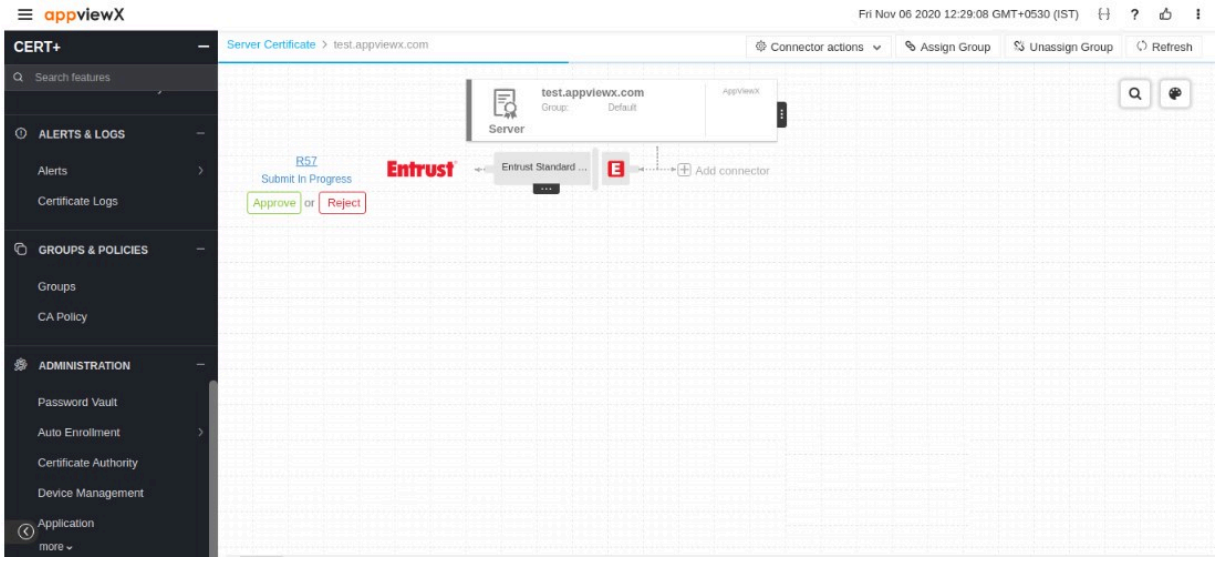
13. Click the **Add** button.
14. Once the details are added, it will redirect to the page where the user can see the respective CSR and CA details added as a connector. This page is called holistic view and from here any action on the certificate can be performed including provisioning the certificate to a Code Signing.



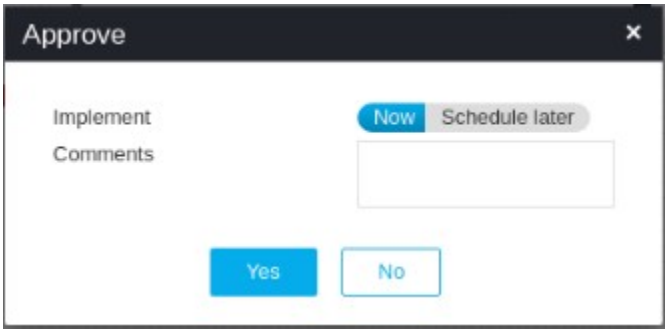
15. Click the **Submit** button to trigger the request.
16. Once the submit action is triggered, the **Submit** pop-up window appears. Add comments if needed, and then click the **Yes** button. If an approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.



17. Click **Approve** to proceed.

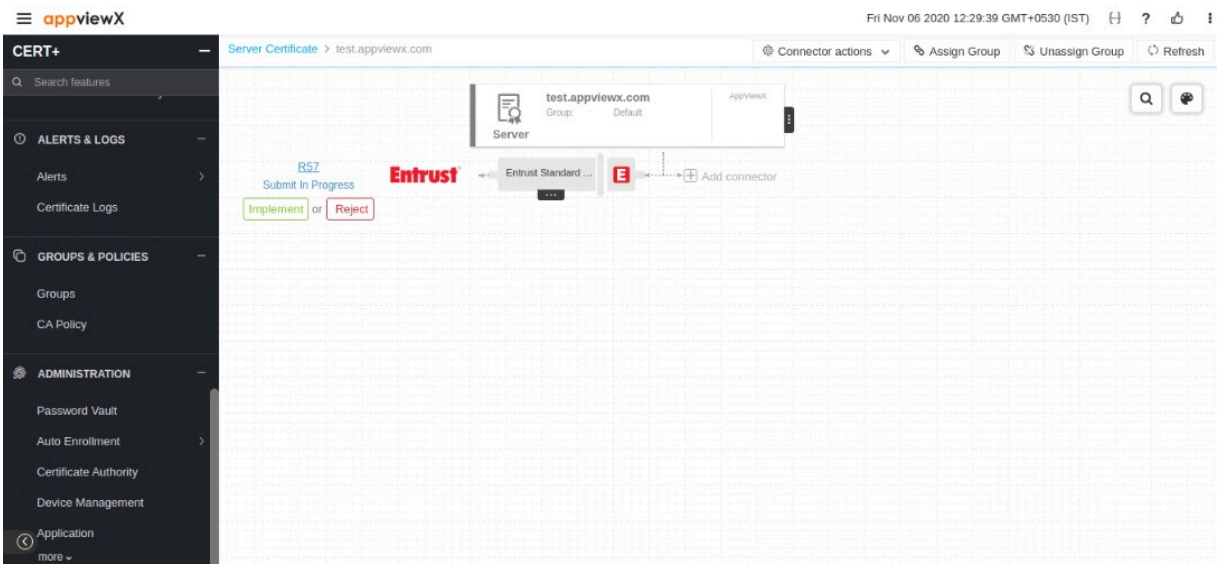


18. The **Approve** pop-up window appears. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.

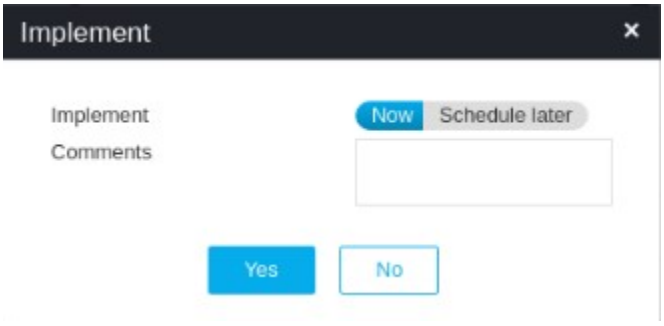


   a. Enter the comments in the field.
   b. Click **Yes**.

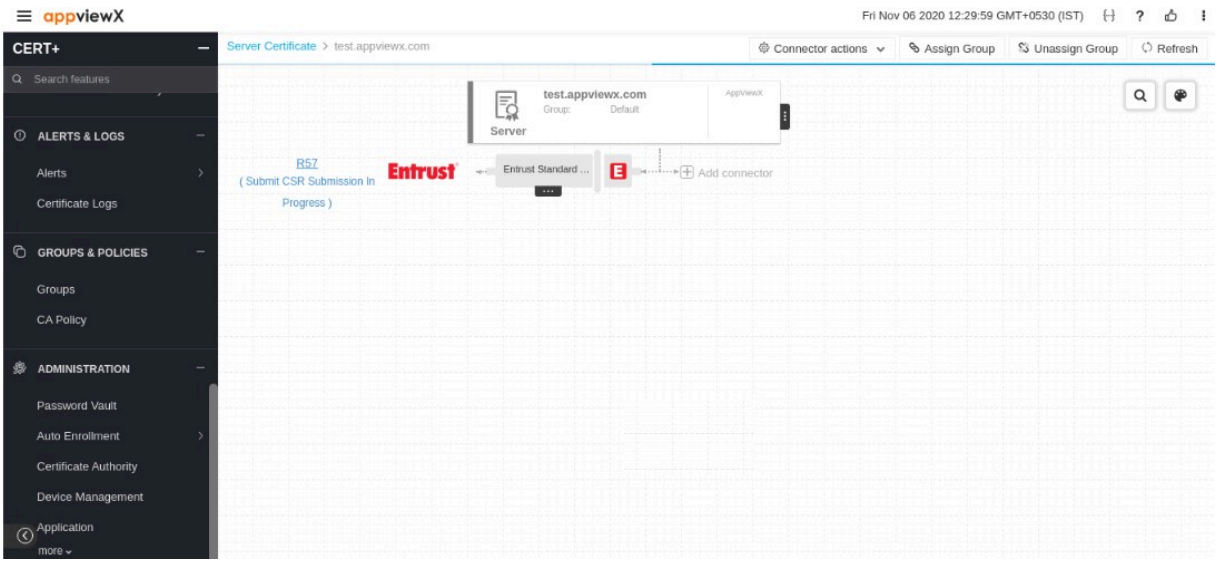
19. Once approved, the user can see the Implement option in the holistic view. Click **Implement**.



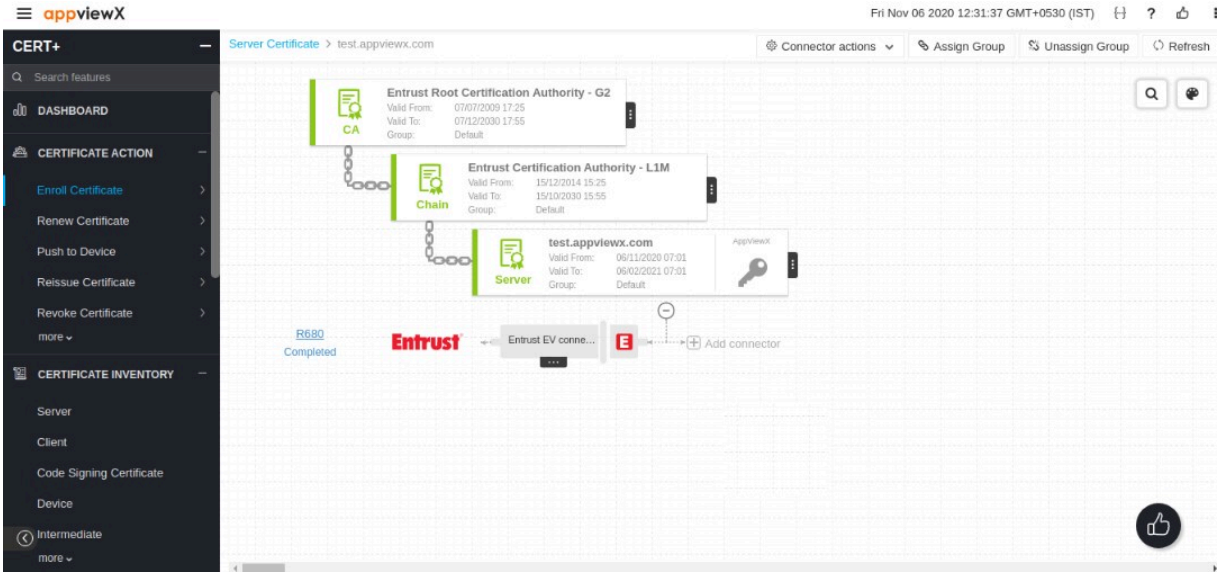
20. The **Implement** pop-up window appears. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



    a. Enter the comments in the field.
    b. Click **Yes**.
21. CSR Submission to CA is in progress.



22. Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.
23. If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.
24. If auto-approval disabled in the targeted CA, the user has to be logged into CA and approve the request.



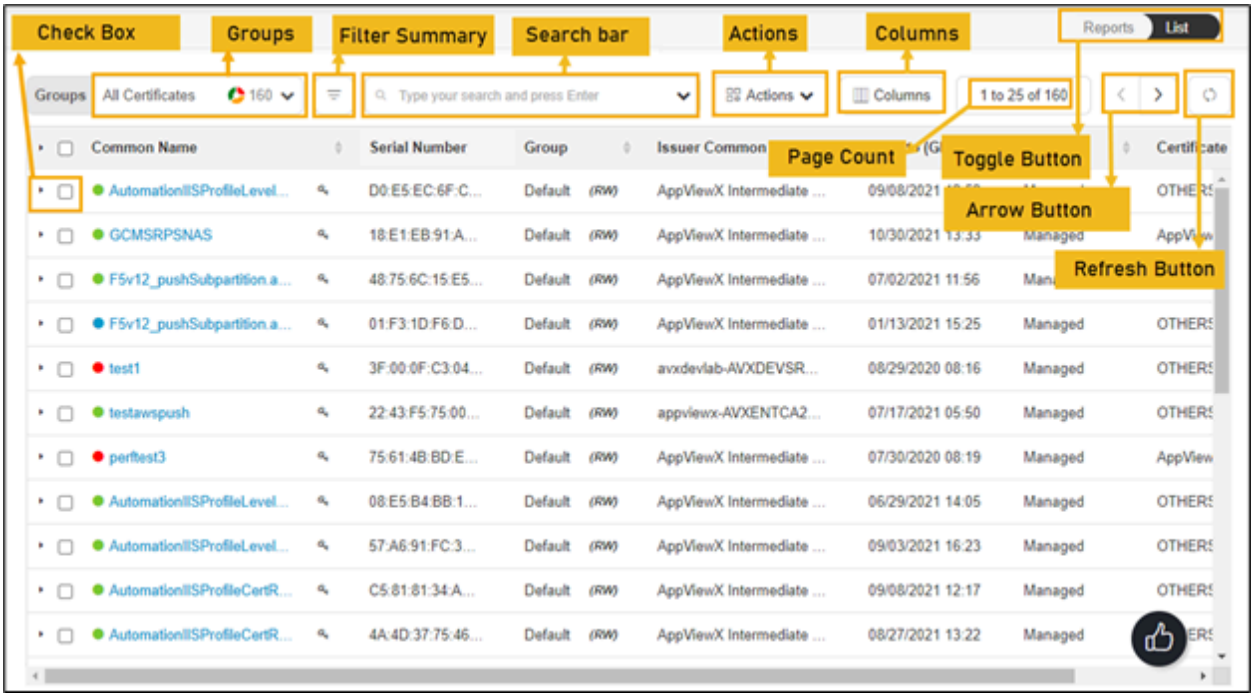
25. Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

Renewing Certificate

Overview

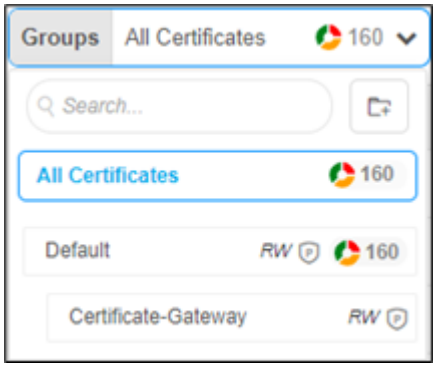
The digital certificates are issued with a limited validity period. Before the expiration of its validity, it has to be renewed and placed on the server for service continuity. The renewal process may vary from CA to CA based on their operations. The result will be the issuance of the certificate with extended validity. CERT+ enables users to trigger certificate renewal in different ways. The user can trigger renewal from the certificate inventory or the certificate details and its provisioned details can be verified and trigger the renewal from a holistic view. Group policy auto-renewal takes care of the certificate renewal automatically and it can be combined with auto-push for hassle-free automation.

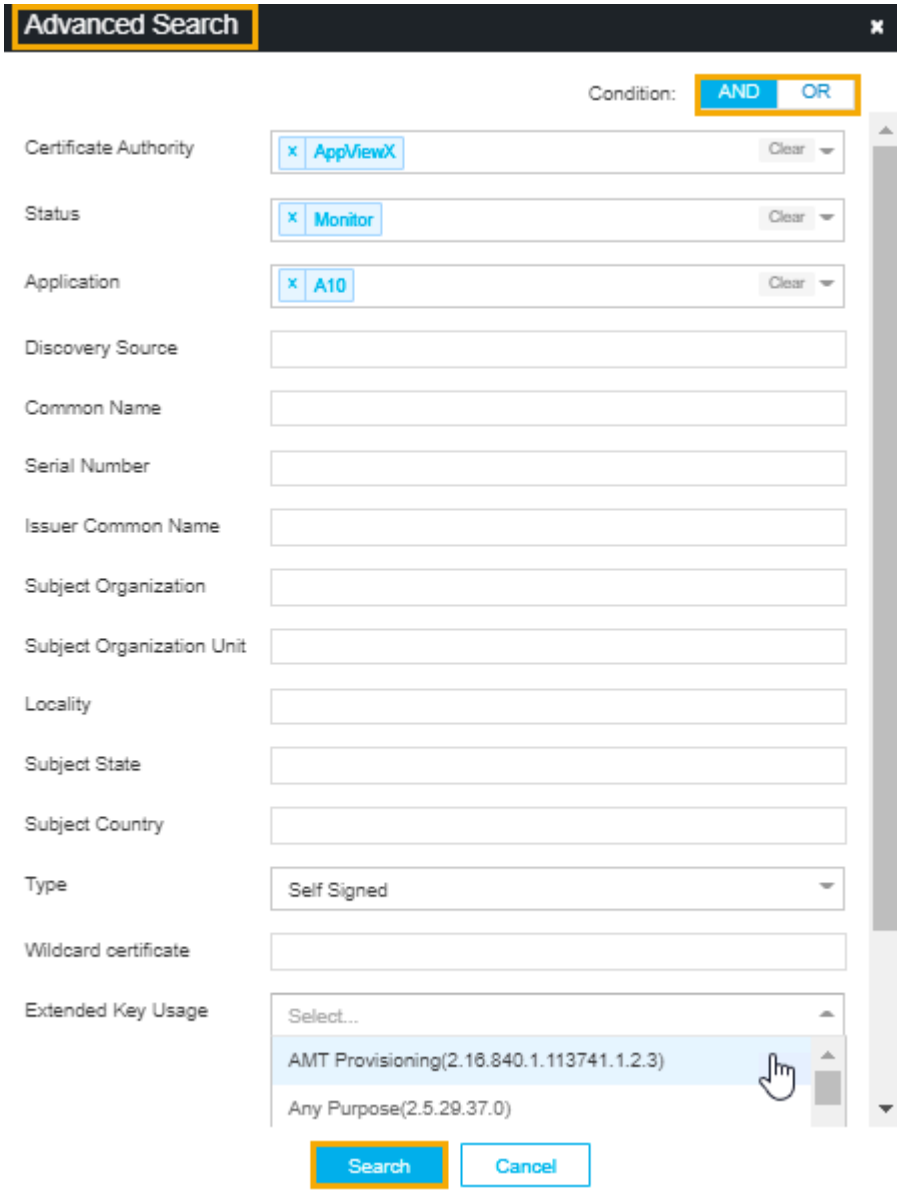
Note: You can renew the certificates via the Certificate Inventory section also.



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

The following table describes the options available on the renew certificate page:

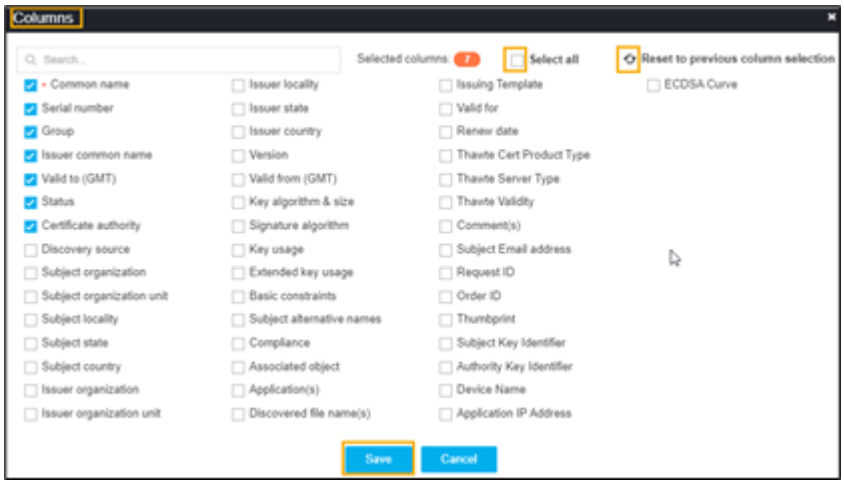
Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description
	 The following table describes the options available in the Advanced Search feature. **Options** | **Description** **Condition** | Displays the type of the desired search on the page. The possible options are, • AND • OR

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Certificate Authority</td><td>Allows you to select the desired CA from the dropdown list.</td></tr>
<tr><td>Status</td><td>Allows you to select the desired status certificate. The possible options are,

• Manage
• Monitor
• New certificate</td></tr>
<tr><td>Discovery Source</td><td>Enter the source of the discovery.</td></tr>
<tr><td>Common Name</td><td>Enter the common name of the certificate.</td></tr>
<tr><td>Serial Number</td><td>Enter the serial number of the certificate.</td></tr>
<tr><td>Issuer Common Name</td><td>Enter the name of the certificate issuer.</td></tr>
<tr><td>Subject Organization</td><td>Enter the subject of the organization.</td></tr>
<tr><td>Subject Organization Unit</td><td>Enter the subject of the organization’s unit.</td></tr>
<tr><td>Locality</td><td>Enter the specific locality.</td></tr>
<tr><td>Subject State</td><td>State Enter the state of the certificate’s subject.</td></tr>
<tr><td>Subject Country</td><td>Country of the subject.</td></tr>
<tr><td>Type</td><td>Type of the certificate.</td></tr>
<tr><td>Wildcard certificate</td><td>Enter the wildcard certificates.</td></tr>
<tr><td>Extended Key Usage</td><td>Allows you to select the EKU from the dropdown list.</td></tr>
<tr><td>Search</td><td>Click the Search button to get the results from the search.</td></tr>
</table>
</td></tr>
<tr><td>Actions</td><td>Displays the list of actions. The possible actions are,

• Export Certificates
• Import Certificates</td></tr>
</table>

Options	Description
	• Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are,

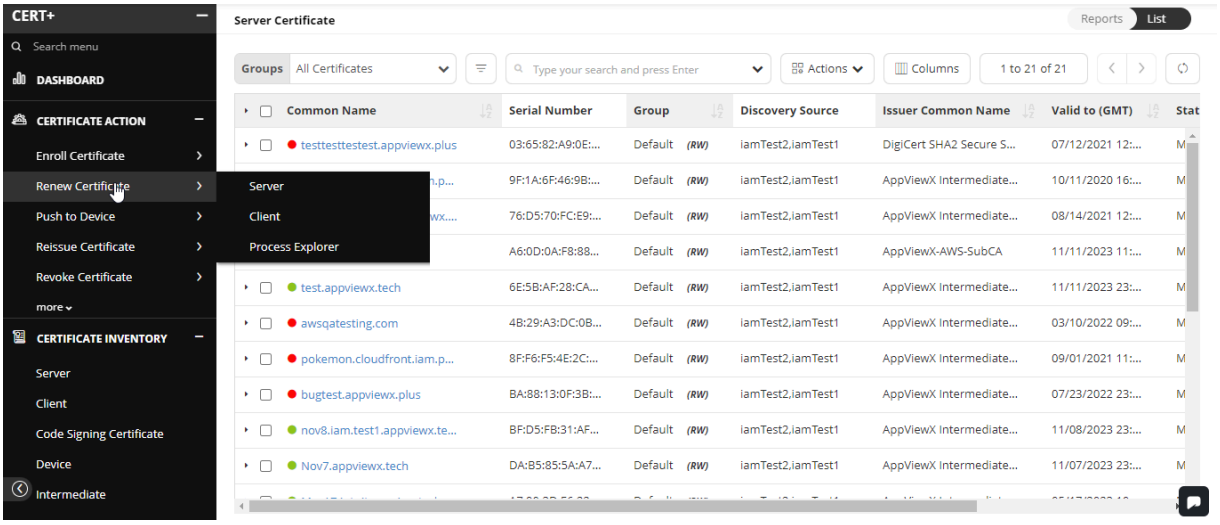
Options	Description
	• Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Renewing Server Certificate

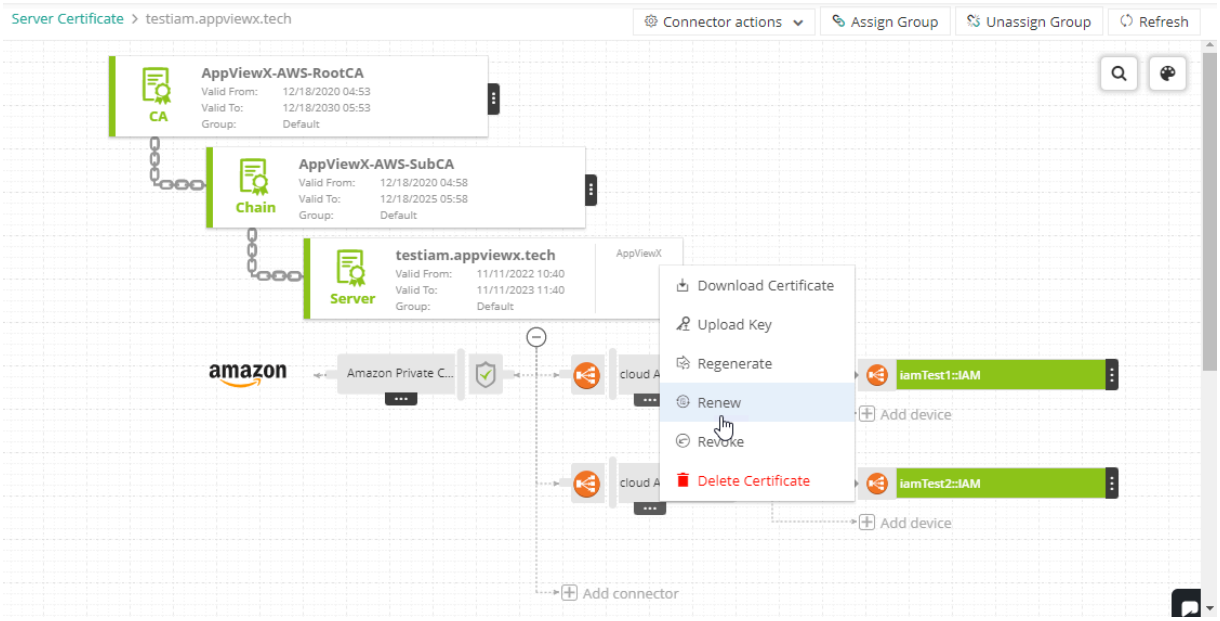
Note: AppViewX v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

If you are renewing the single certificate, you can prefer the renewal from a holistic view as they can verify all the details before initiating renewal. Steps to renew a server certificate:

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 ACTION**.
5. Select **Renew Certificate**, and then **Server**.
   The **Server Certificate** page appears.

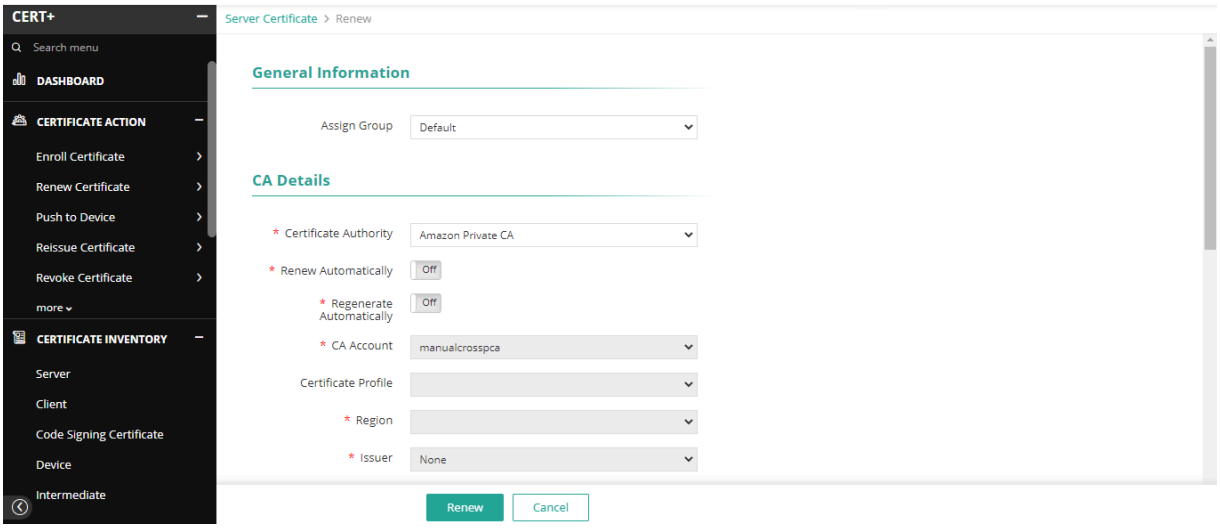


6. In the **certificate list** view, click **Common Name** of the certificate navigate to a holistic view.
7. Hover over the vertical eclipse on the certificate and click **Renew**.



The **Server Certificate > Renew** screen is displayed.

> **Note:** Depends on the type of certificate, the renew page might appear. If necessary, in the **Renew Automatically** field, toggle **Off** to **On**. Enter the number of days before you initiate the renewal process. based on the settings it will renew automatically in the future.

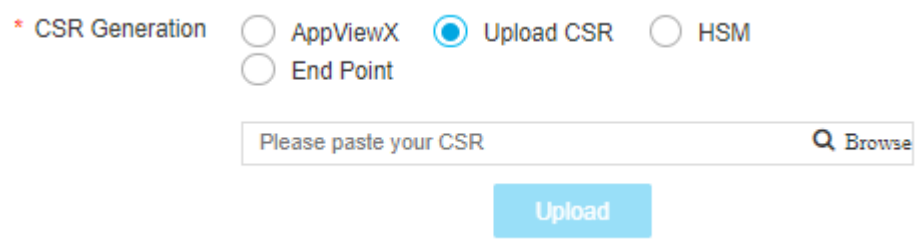


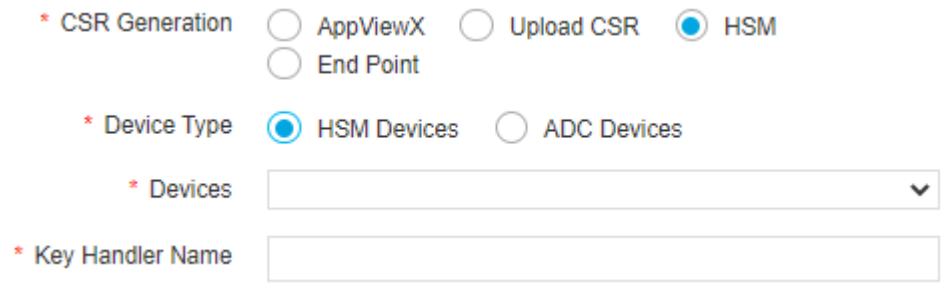
8. On the **Server Certificate > Renew** screen, in the **General Information** section, from the dropdown list, select the required **Assign Group**.

9. In the **CA Details** section, enter/select the following details:

Options	Description
*Certificate Authority	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA details are configured. The possible CAs are: • Amazon • Amazon Private CA • AppViewX • Comodo • Digicert • Entrust ECS • Entrust MPKI • EJBCA • GlobalSign • GoDaddy • Google • InCommon • LetsEncrypt • Microsoft • Enterprise • Microsoft • Standalone • NewCustomCA • Symantec • TATRA BANKA • Thawte • Trust Wave • Certificate Manager.
*Renew Automatically	Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option will be enabled. • Enter the number of days to renew the certificate automatically. **Note:** Changing the group inherited renew period overwrites the renewal period for this certificate.

Options	Description
*CA Account	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
*Division	Select the division to which the certificate must be enrolled. **Note:** This field will be shown only for Digicert CA.
Certificate Profile	Select the Profile to which the Certificate must enroll. **Note:** This field is applicable only for AppViewX CA and Google CA.
*Issuer Location	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Issuer Name	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
*Region	From the dropdown list, select the region the issuer CA belongs to. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Issuer	From the dropdown list, select the name assigned to the issuer CA. **Note:** This field is applicable only when Amazon Private CA is the issuer CA.
*Enroll using	**Note:** This field is applicable only when Amazon Private CA is the issuer CA.

Options	Description
	Select the operation mode that was used to onboard the Amazon Private CA. **Note:** If only one of the two operation modes was select while adding the Amazon Private CA, by default, the other operation mode is disabled.
*Connector Name	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** You can enter a maximum of 2000 words in the field.
***CSR Generation**	Select the CSR generation option as required. Options are: • **UploadCSR** - Uploaded CSR will be taken as a source to populate CSR parameters and submit to CA.  • Click the **Browse** button, and then the file. • Click the **Upload** button to upload the selected file. • On uploading CSR successfully, CSR parameters are automatically filled in the CSR section.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• HSM - Private key and CSR will be created in the selected HSM device based on CSR parameters given.


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>Select the type of device as required.

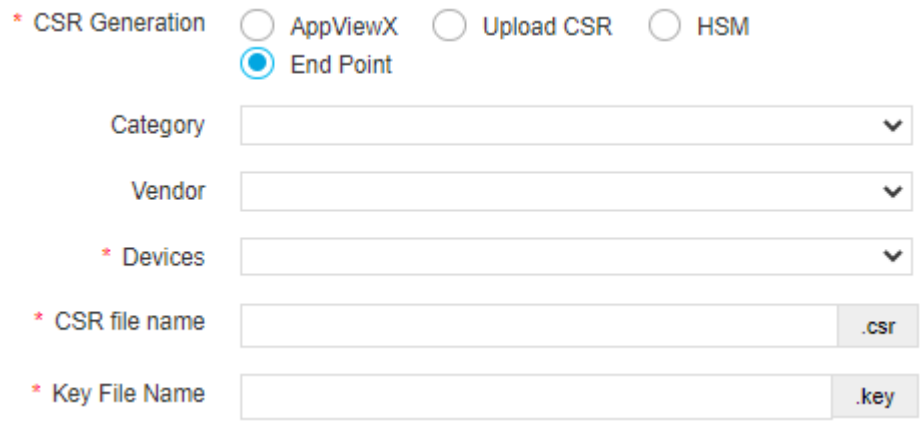
The possible options are:
• HSM Devices
• ADC Devices.</td></tr>
<tr><td>*Vendors</td><td>Select the desired vendors from the dropdown list.

The possible vendors are:
• Safenet
• Thales
• Fortanix.

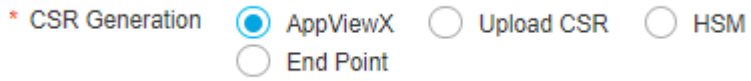
Note: This option will be enabled only for the ADC device type selected.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.

Note: By default, the None Selected option is enabled.</td></tr>
<tr><td>*Key Handler Name</td><td>Enter the desired handler name in the field.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
• End Point - Private key and CSR will be created in the selected End Point device based on CSR parameters given.

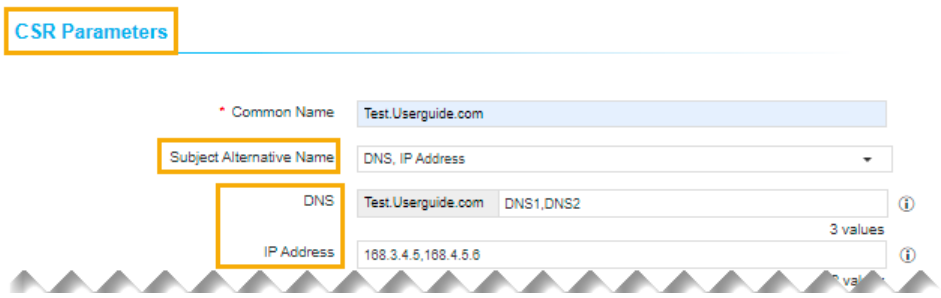


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>Select the desired category from the dropdown list. The possible options are:
• ADC
• Server
• Firewall.</td></tr>
<tr><td>Vendor</td><td>Select the desired vendor from the dropdown list. The possible options are:
• AVI
• Citrix
• F5
• Ngnix Plus
• HAProxy.</td></tr>
<tr><td>*Devices</td><td>Select the desired device from the dropdown list.
Note: By default, the None option is selected.</td></tr>
<tr><td>Tenant</td><td>Enter the tenant id in this field.</td></tr>
</table>
</td></tr>
</table>

Options	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>*CSR file name</td><td>Enter the name of the CSR file in this field.</td></tr><tr><td>*Key File Name</td><td>Enter the name of the key file in this field.</td></tr></table> For all the CA types except Amazon, you have the option to generate the CSR. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. 

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

10. Enter the following details for the **CSR Parameters**:

Field	
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parame Select the subject alternative subject name from the dropdown list. 

Field	
	The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holis
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be a
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-f
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-fille
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-ma
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must con
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editab
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and edita

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

11. In the **Attachment** section, upload any additional documentation required for certificate enrollment (like an approval email).

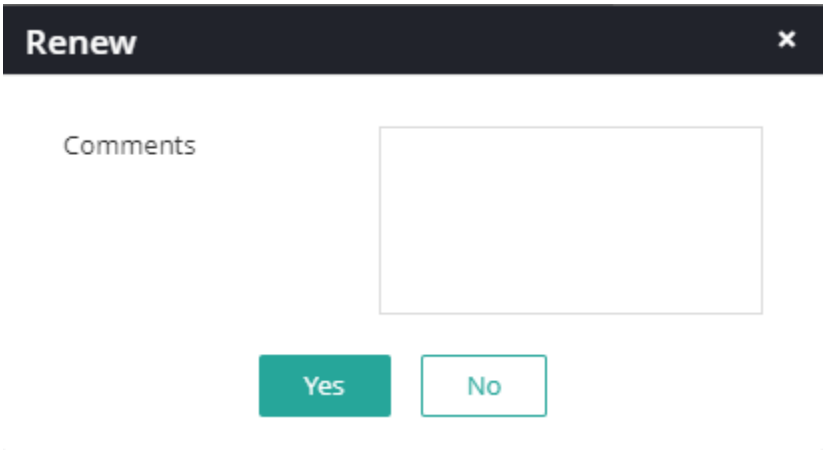
Note: This is an optional step.

To do this, enter the following details:

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** You can enter a maximum of 2000 words in the field.
Upload File	Click the Upload button to select the file.
Note: During certificate actions, the user can upload and maintain the additional necessary documents.	

12. Click **Renew**.

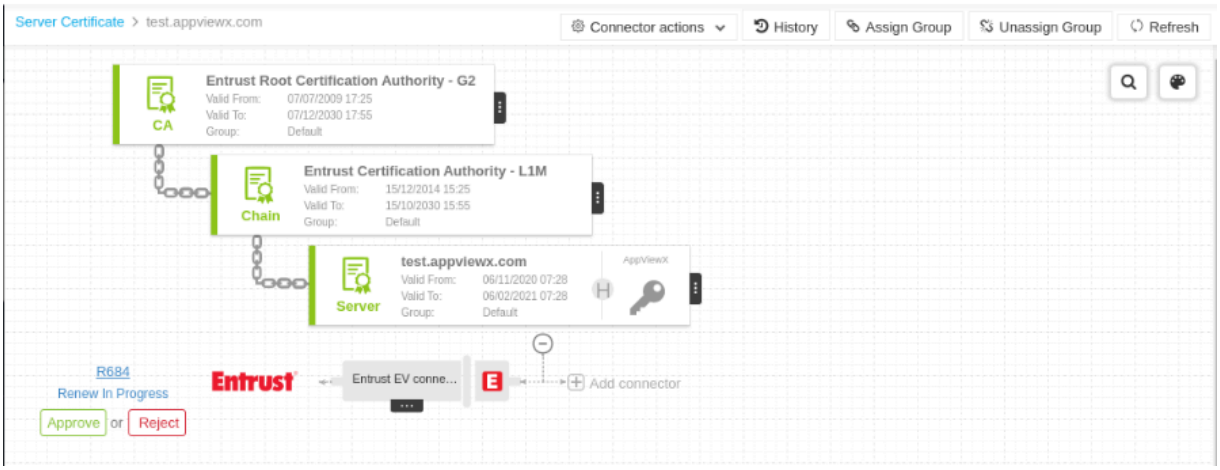
The **Renew** dialog box is displayed.



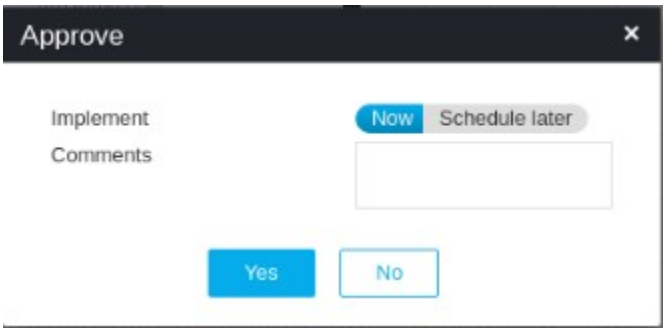
13. In the **Renew** dialog box, enter any comments related to the certificate renewal.
    This is an optional step.
14. Click **Yes**.
    You will be redirected to the holistic view of the certificate you want to renew.

    A request ID, the work order ID is generated automatically, and then work order status is displayed beside the certificate on the holistic view. If an approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.

15. Click **Approve** to proceed with the **Renew** action.

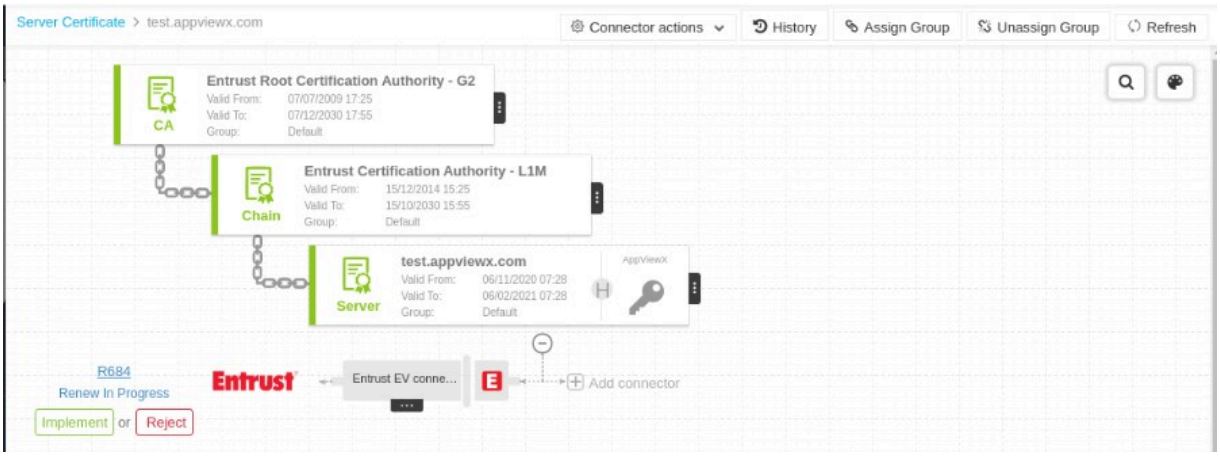


On the Approve page that pops up:

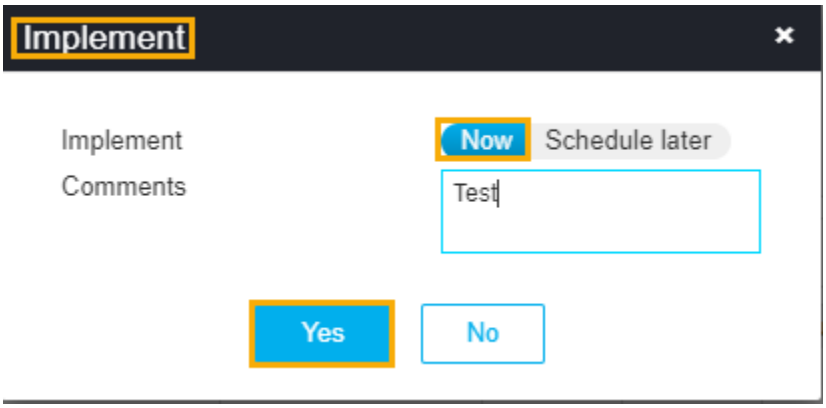


- Click Schedule later if the workflow request has to be approved automatically in the future.
- Enter comments to approve the renewal and then click Yes. The work order status is displayed beside the connector.

16. Click Implement to proceed with renewing action.

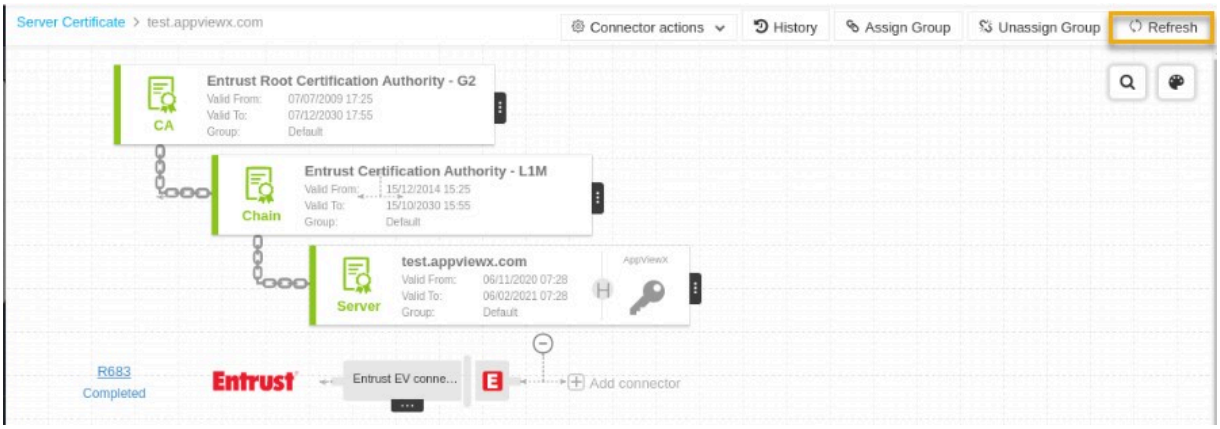


On the **Implement** page that pops up:



- Click **Schedule later** if the workflow request has to be approved automatically in the future.
- Enter comments to approve the renewal, then click **Yes**.

17. Click the **Refresh** button on the top right until the renew status updates.



18. After the renewal action is completed, the status updates to **Completed**.

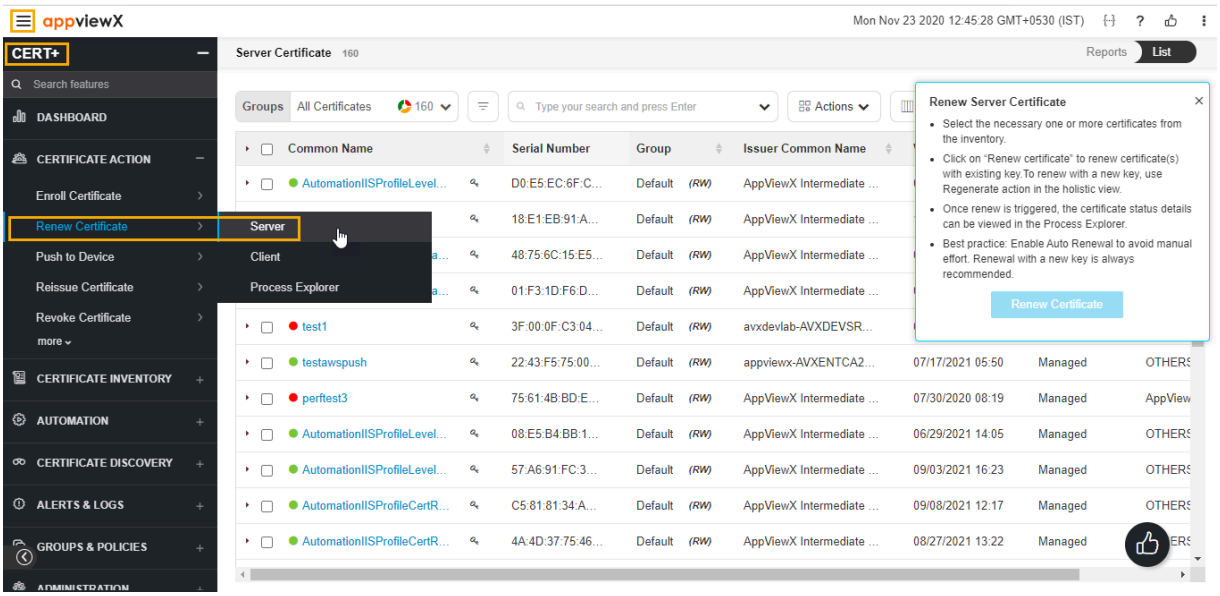
Bulk Renew of the Server Certificates

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

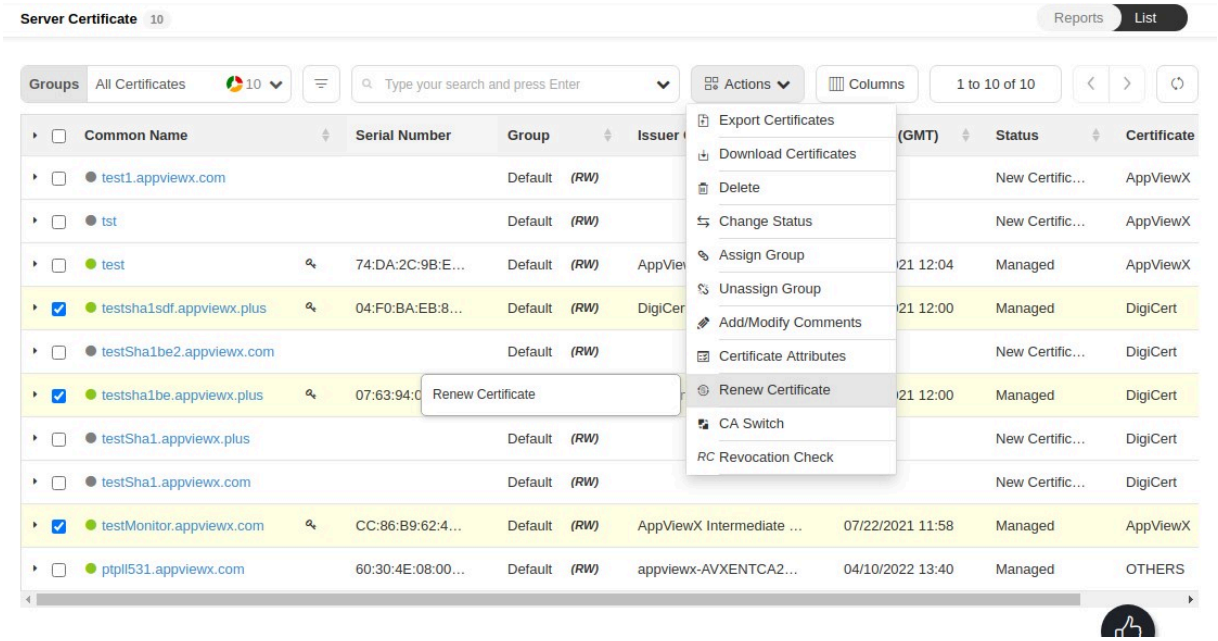
Bulk renewal of the certificates can be triggered from the inventory by multiselection certificates.

Users can renew certificates in bulk. Steps to renew certs in bulk:

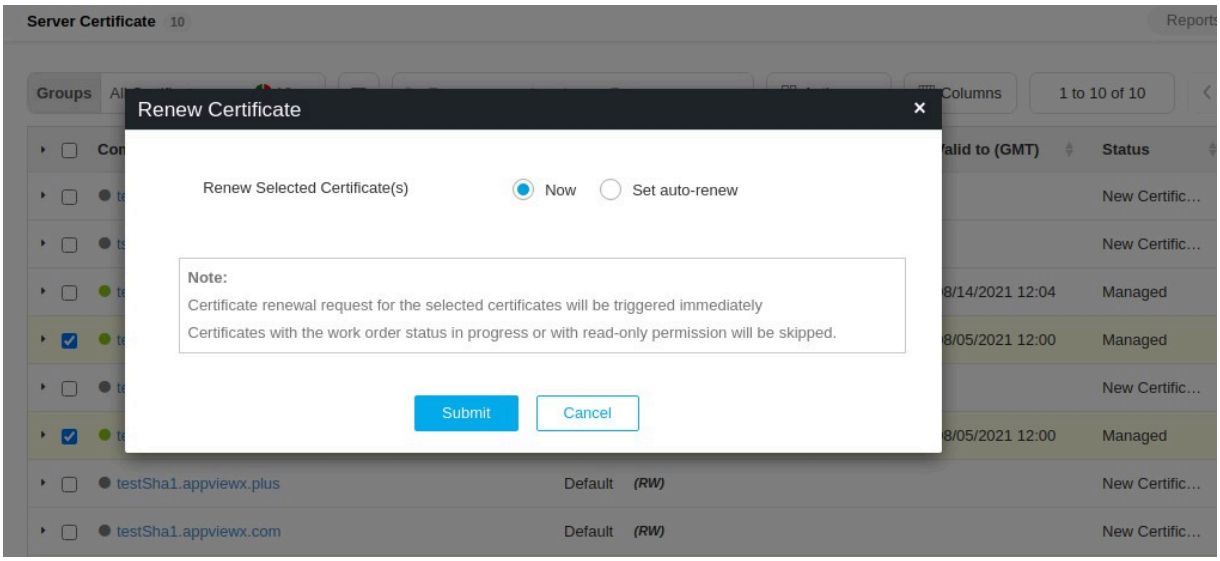
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Renew Certificate**, and then **Server**.
   The **Server Certificate** page appears.

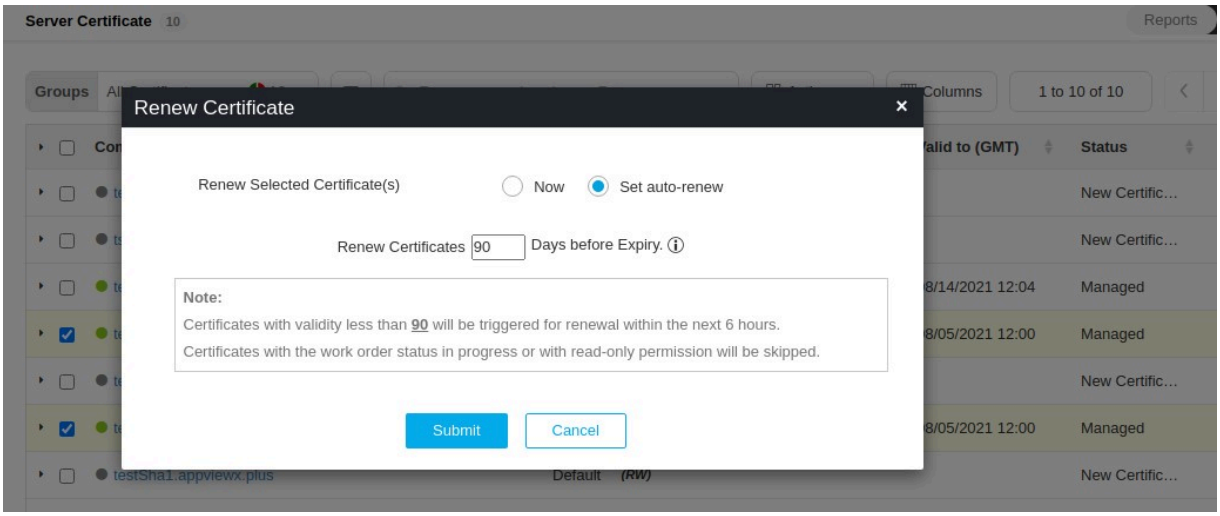


6. Click **Actions**, and then select **Renew Certificate**.



7. In the **Certificate Renew** pop-up window, based on the requirement select the type of certificate renewal **Now** or **Set auto-renew**.





8. Select **Submit**.
9. Certificate renewal can be triggered now or auto-renew can be configured for all the certificates selected.
10. The status of the trigger now can be monitored under process explorer.

Renewing Client Certificate

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

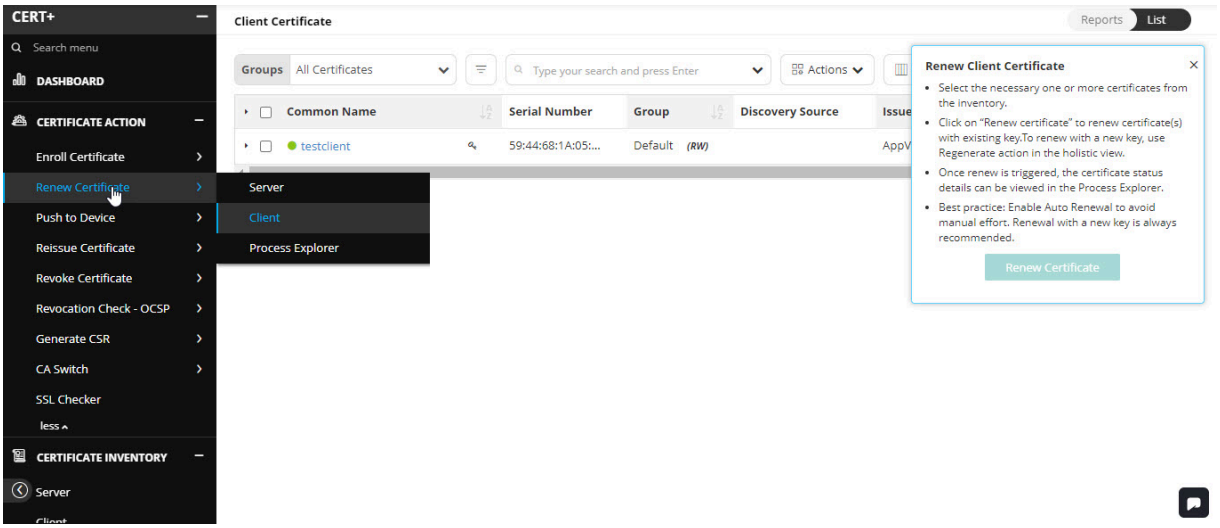
Steps to renew client certificate:

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

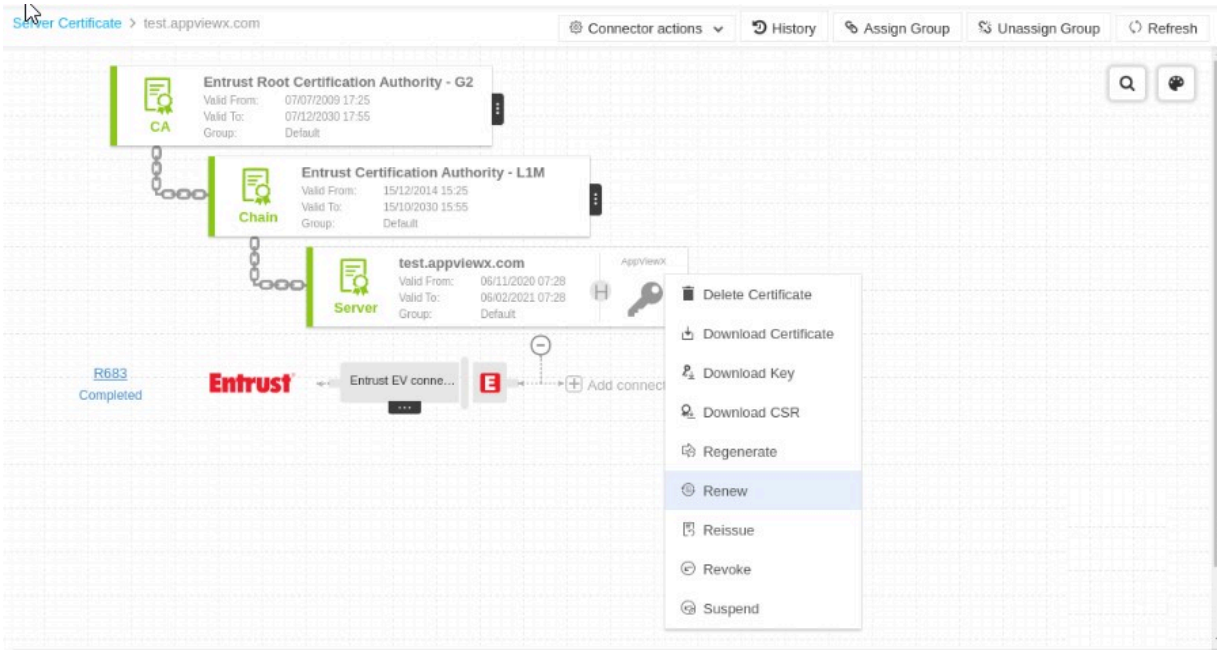
   The left navigation pane appears.
3. Click **CERT+**.

   The CERT+ left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Renew Certificate**, and then **Client**.

   The **Client Certificate** page appears.

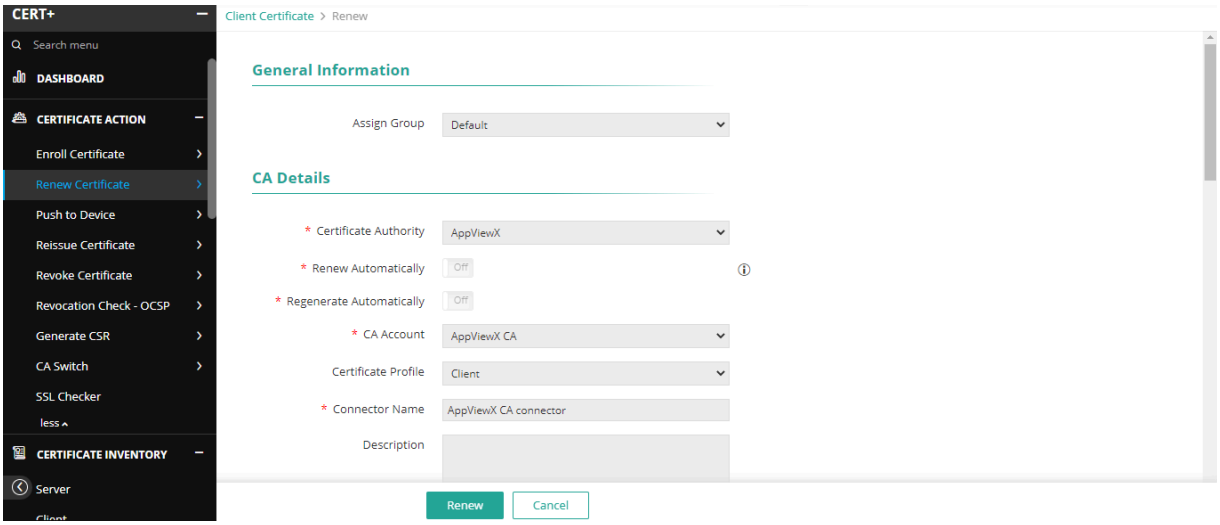


6. On the **ClientCertificate** page, click **List** on the upper-right.
7. In the certificate list view, click Common Name of the certificate to navigate the holistic view.
8. Hover over the vertical eclipse on the certificate and click Renew.

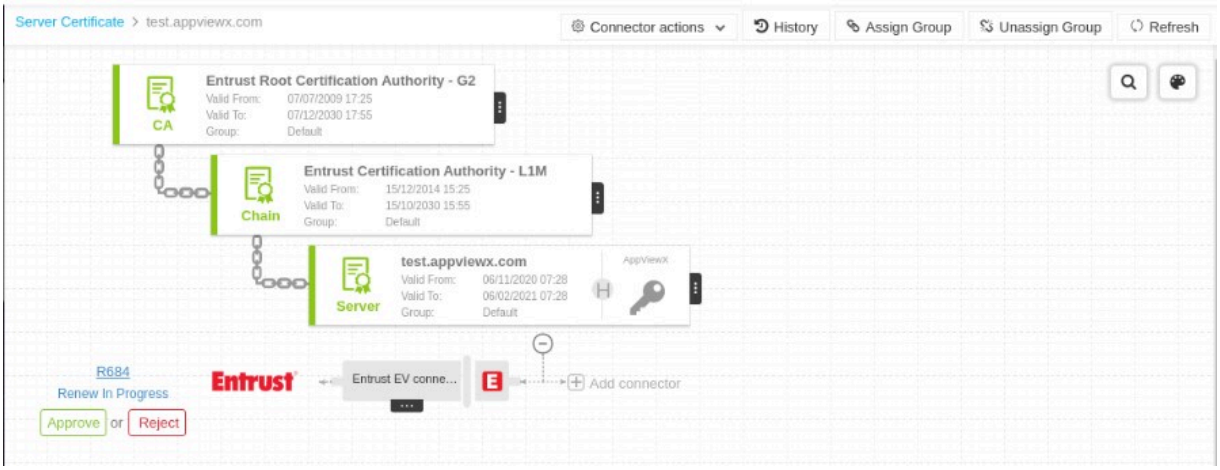


The **Server Certificate > Renew** screen is displayed.

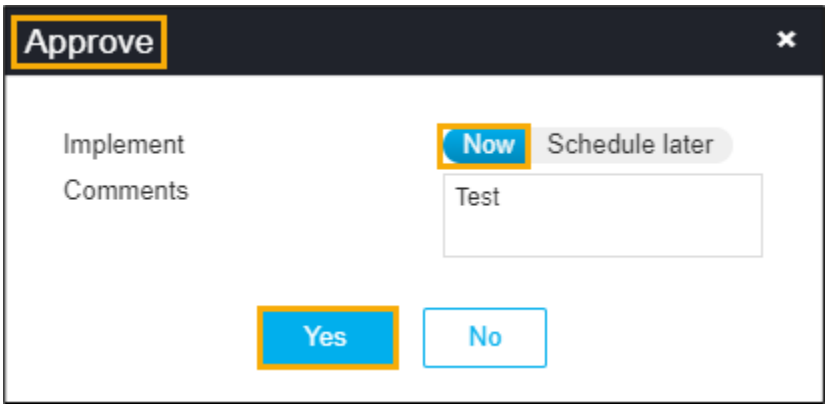
Note: Depends on the type of certificate, the renew page might appear. If necessary, in the **Renew Automatically** field, toggle **Off** to **On**. Enter the number of days before you initiate the renewal process. based on the settings it will renew automatically in the future.



9. Click **Renew**.
10. On the Renew pop-up window, enter comments, and click **Yes**. A request ID, work order ID are generated automatically and then work order status is displayed beside the certificate on the holistic view. If an approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.
11. Click Approve to proceed with the Renew action.



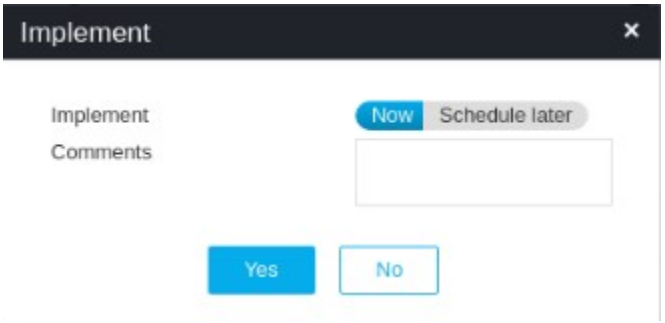
On the Approve page that pops up:



- Click Schedule later if the workflow request has to be approved automatically in future.
- Enter comments to approve the renewal and then click Yes. The work order status is displayed beside the connector.

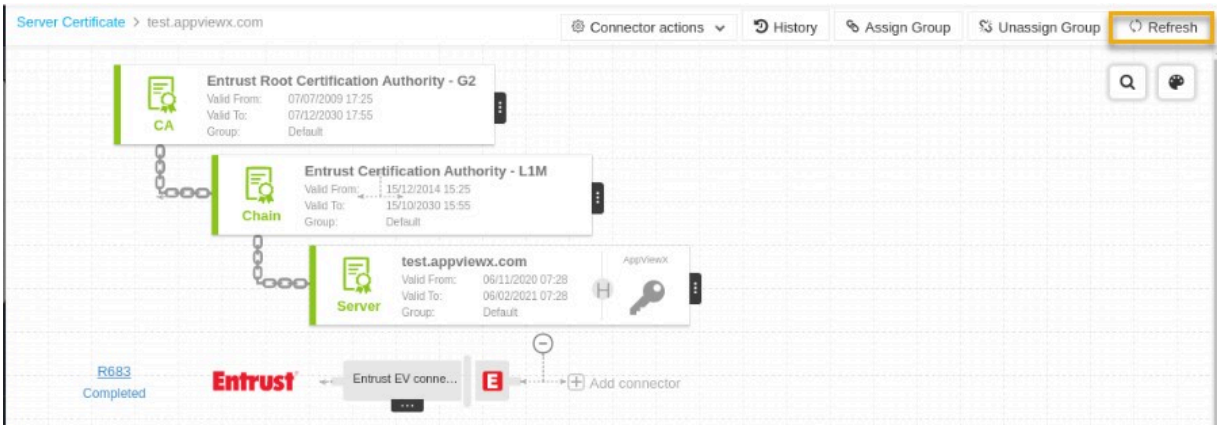
12. Click Implement proceed with renew action.

    On the Implement page that pops up:



- Click Schedule later if the workflow request has to be approved automatically in the future.
- Enter comments to approve the renewal, then click Yes.

13. Click the Refresh button on the top right until the renew status updates.



14. After the renewal action is completed, the status updates to Completed.

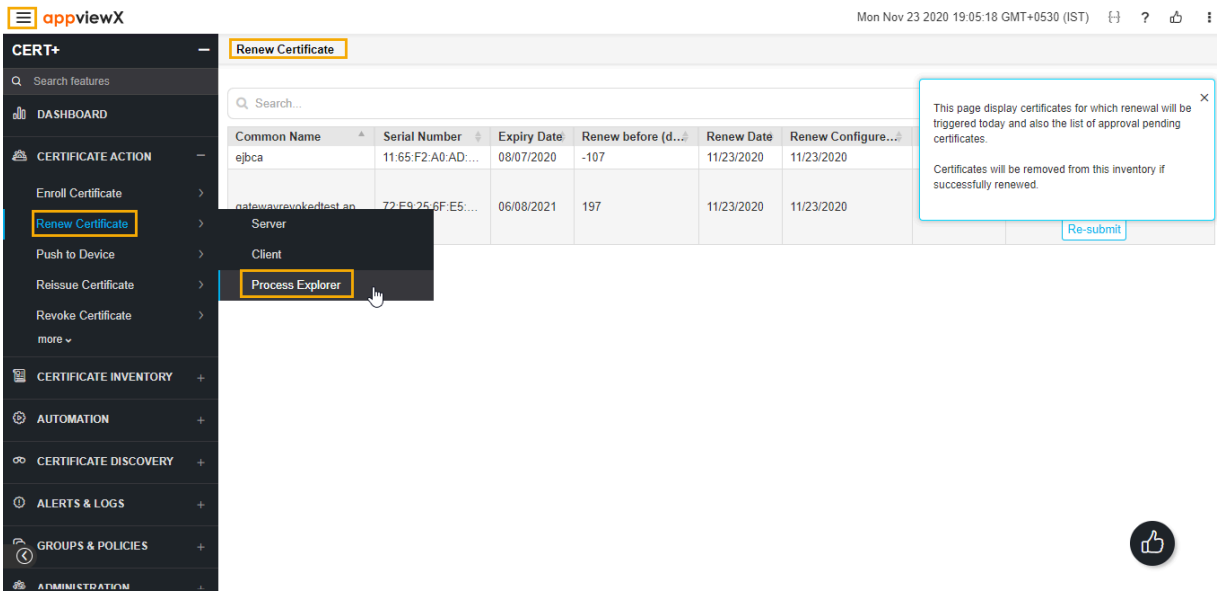
Process Explorer

Process Explorer allows users to view the list of certificates that to be triggered today and the certificates awaiting approval. Once the certificate is renewed, it will be removed from the list. This will be handy in the case of bulk operations.

Steps for the process explorer,

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 ACTION**.
5. Select **Renew Certificate**, and then **Process Explorer**.

The **Process Explorer** page appears.



Push to Device

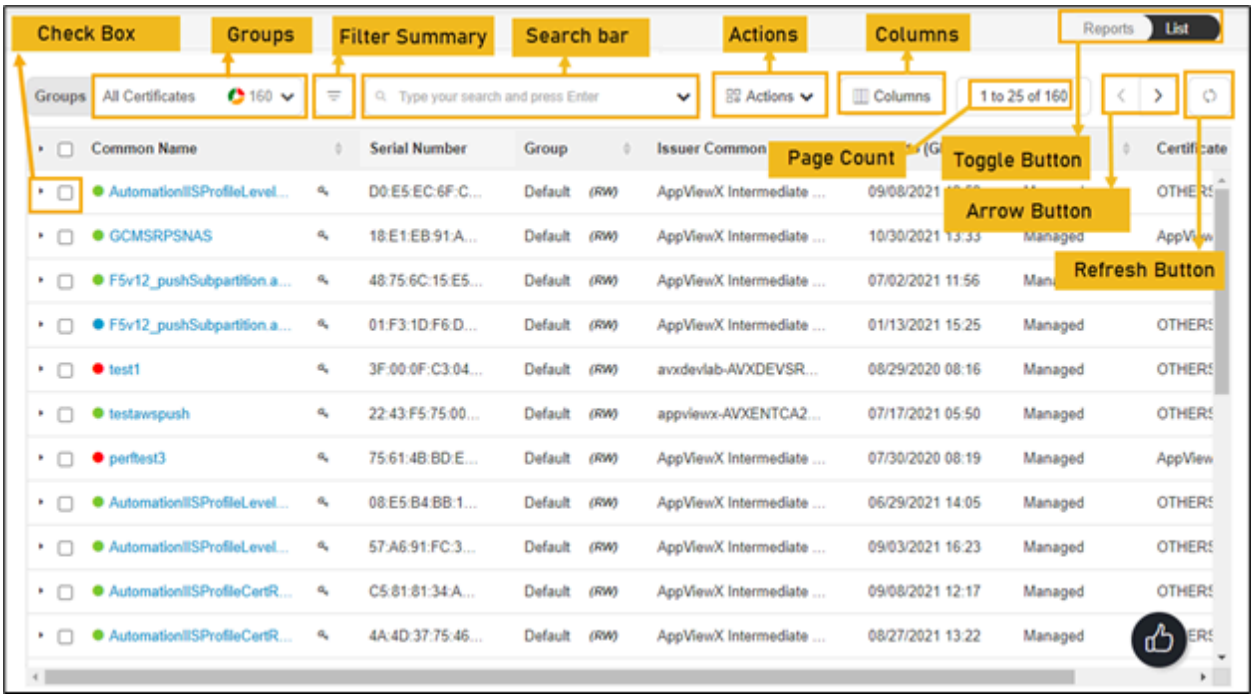
- Overview
- Add Application Connector
- Pushing Server Certificate to a Device
- Pushing Client Certificate to a Device
- Pushing Intermediate Certificate to a Device
- Pushing Root Certificate to a Device

Overview

Users can enable push automatically field is selected while adding application connecter to a certificate, then the certificate is automatically pushed to the device when it is retrieved/renewed.

Note:

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

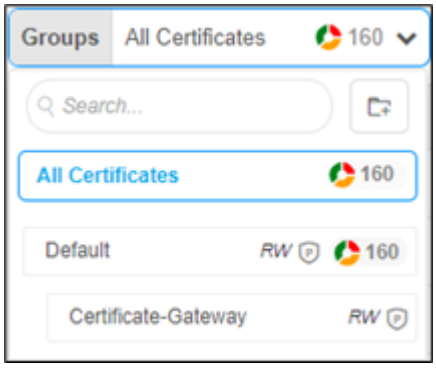


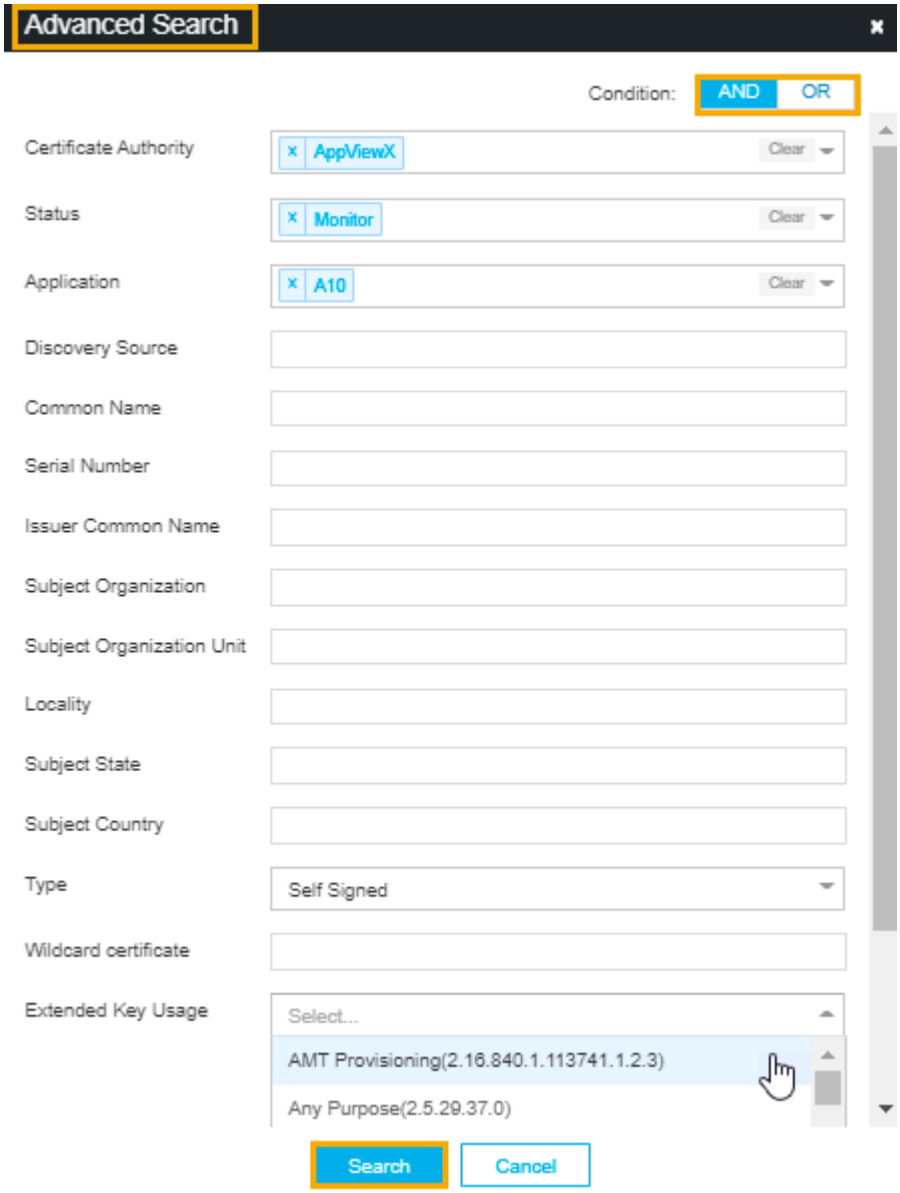
Note:

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

The following table describes the options available on the renew certificate page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected.

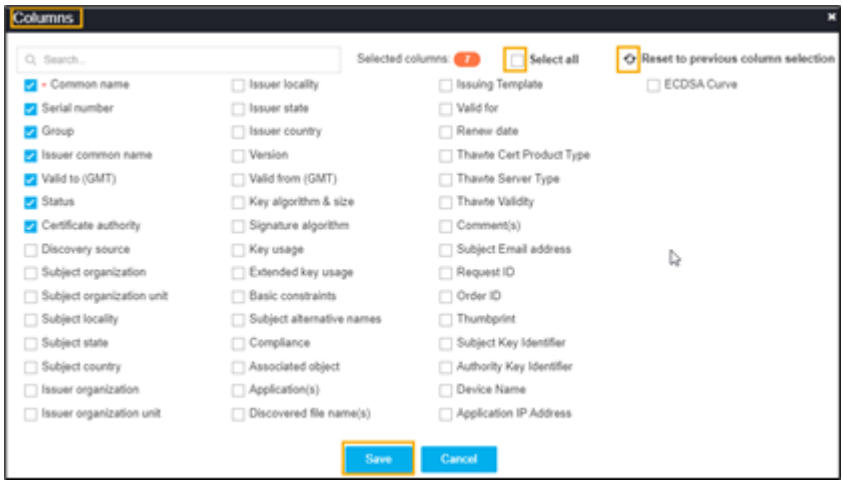
Options	Description
	
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description
	 The following table describes the options available in the Advanced Search feature: **Options** | **Description** **Condition** | Displays the type of the desired search on the page. The possible options are, • AND • OR.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Certificate Authority</td><td>Allows you to select the desired CA from the dropdown list.</td></tr>
<tr><td>Status</td><td>Allows you to select the desired status certificate. The possible options are,

• Manage
• Monitor
• New certificate.</td></tr>
<tr><td>Discovery Source</td><td>Enter the source of the discovery.</td></tr>
<tr><td>Common Name</td><td>Enter the common name of the certificate.</td></tr>
<tr><td>Serial Number</td><td>Enter the serial number of the certificate.</td></tr>
<tr><td>Issuer Common Name</td><td>Enter the name of the certificate issuer.</td></tr>
<tr><td>Subject Organization</td><td>Enter the subject of the organization.</td></tr>
<tr><td>Subject Organization Unit</td><td>Enter the subject of the organization’s unit.</td></tr>
<tr><td>Locality</td><td>Enter the specific locality.</td></tr>
<tr><td>Subject State</td><td>State Enter the state of the certificate’s subject.</td></tr>
<tr><td>Subject Country</td><td>Country of the subject.</td></tr>
<tr><td>Type</td><td>Type of the certificate.</td></tr>
<tr><td>Wildcard certificate</td><td>Enter the wildcard certificates.</td></tr>
<tr><td>Extended Key Usage</td><td>Allows you to select the EKU from the dropdown list.</td></tr>
<tr><td>Search</td><td>Click the Search button to get the results from the search.</td></tr>
</table>
</td></tr>
<tr><td>Actions</td><td>Displays the list of actions. The possible actions are,

• Export Certificates
• Import Certificates
• Delete</td></tr>
</table>

Options	Description
	• Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate. • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.

Options	Description
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Add Application Connector

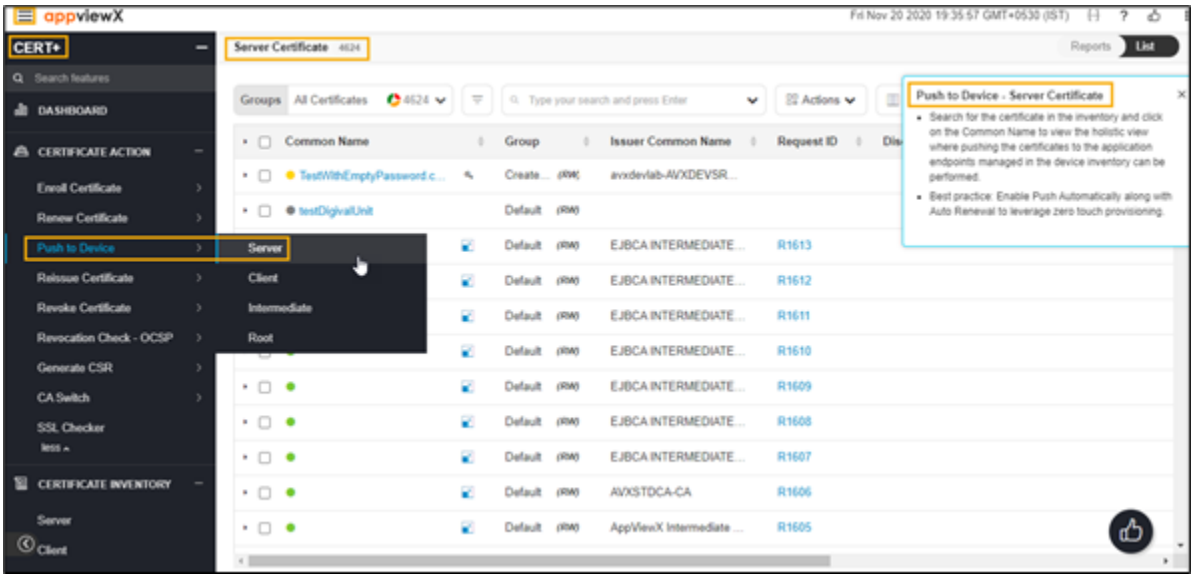
An application connector is a software application running on a server. To add the application connector the application should be managed under the AppViewX device inventory. All the supported devices in the AppViewX inventory can be provisioned with the certificate by adding the connector. The connector enables cloud-managed devices as will to provision certificates from on-premises infrastructure. To add an application connector to a server certificate,

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 ACTION**.
5. Select **Push to Device**, and then **Server**.

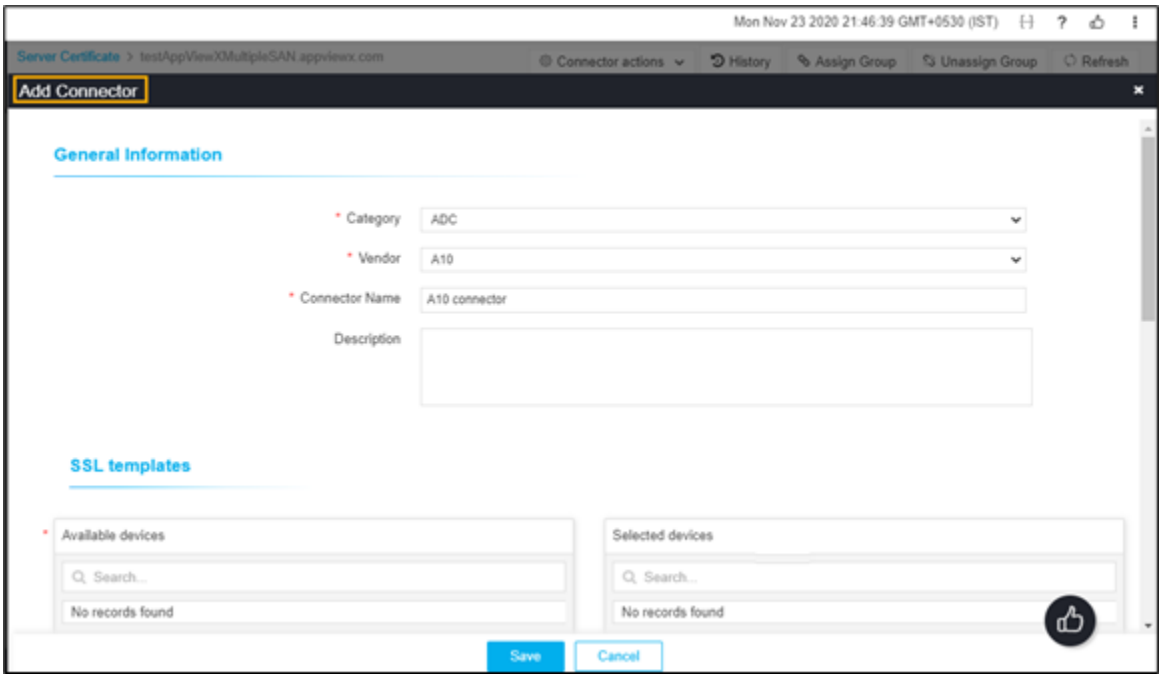
   The **Server Certificate** page appears.



6. In the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.
7. In the Certificate topology page, click

   Add Connector.

The **Add Connector** window appears.



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

The following table describes the options available in the general information section:

Field	Description
Category	Select the category from the dropdown list. The possible categories are: • ADC • Cloud • Firewall • MDM • Server • WAF.
Vendor	Select the desired vendor from the dropdown list.

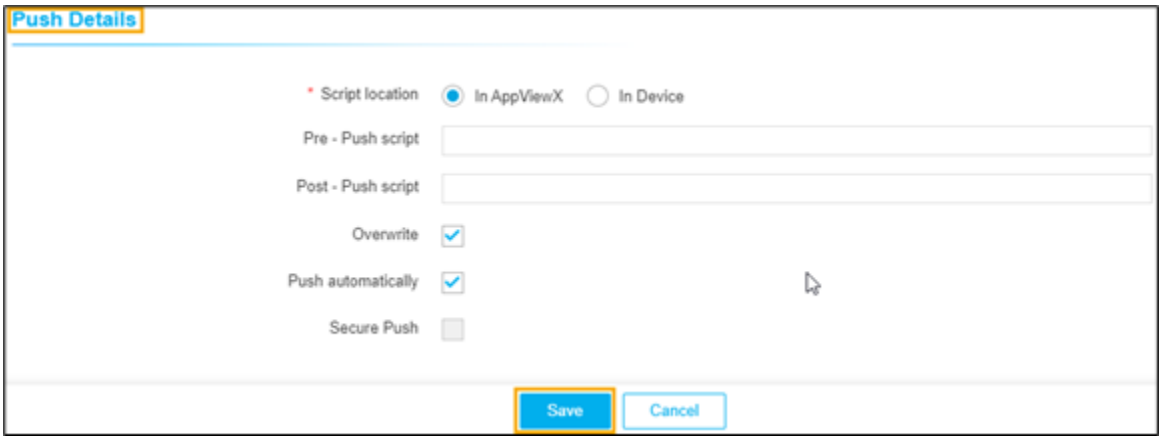
Field	Description
Connector Name	Enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
Description	Enter the description in this field.

9. (Only applicable for **Citrix** application type) The SNI-enabled virtual server option is displayed. When the checkbox is selected, the virtual servers whose SNI is enabled, will be listed. Also, you can enable SNI for the virtual server by selecting **Enable SNI push for Certificate** and **Enable SNI in Virtual Server.**
10. From the list of available application objects, click the icon beside each device you want to select.
11. Based on the certificate format and the server type the certificate details will vary. In the **Certificate Details** section, select/enter the details as follows:

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

Field	Description
Certificate Type	Select the type of certificate to be pushed from the dropdown list.
Certificate File Name	Enter the desired certificate file name.
Key File Name	Enter the desired key file name.
Push Root and Intermediate Certificates	Select the push root and intermediate certificates check box, to push the certificate into the device.
Intermediate File or Bundle Name	Enter the desired intermediate File or bundle name.

12. Push details are the optional fields that can be used based on client requirements. In the Push Details section, select/enter the details as follows:



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

Table 2.

Field	Description
Script location	Select the type of script location. The possible locations are: • In AppViewX • In Device.
Script location	If the user wants to run a certain validation script before the push operation, the path can be specified in **Pre - Push script**.
Post - Push script	If the user wants to run a certain validation script after the push operation, the path can be specified in **Post - Push script**.
Overwrite	Select the checkbox to overwrite existing certificates with the new certificate.
Push automatically	Push automatically checkbox to push certificates to the device automatically when there is an update in the certificate.
Secure Push	(applicable for F5 application type) The Secure Push checkbox is selected by default. This option encrypts the certificates while pushing them into a device. You can uncheck this option if you have permission. **Note:** For <.jks> Keystore, a valid alias needs to be entered to reference the certificate within the key store.

13. Click **Save** to add the application connector to the Certificate topology.

Pre and Post Push Script Location Details

The Push Details section lets you define the working of the push operation, for example, you can specify scripts to carry out a set of tasks before and after the certificate is pushed to a device, as explained in the field descriptions below:

Field	Description
Script Location	Location where the scripts are stored. In AppViewX • Select this if the scripts are stored in the AppViewX Cloud Connector box In Device • Select this if the scripts are stored in a device in the tenant's premises.
Pre - Push script	The pre push script defines all tasks that have to be carried out before the push option is executed. Enter the location where the pre push script is stored. For the CERT+ SaaS deployment, if the pre push certificate is stored in the AppViewX Cloud Connector Box, ensure the following: • The **.sh** file for the pre push script should be placed inside the **deps** folder in the Cloud Connector installation package. • Tenants are free to create a folder structure within the deps folder, as per requirement.

Field	Description
	• For example, you can save the **prepush.sh** file in the **deps** folder, or you can create a new folder in the **deps** folder and save the **prepush.sh** file in that new folder. • The path entered in the **Pre - Push script** field should be relative to the **deps** folder. • For example, if the prepush.sh file is stored in the deps folder, your relative path will be **/prepush.sh**. • If the **prepush.sh** file is stored in the **scripts** folder (created by the tenant) within the **deps** folder, your relative path will be **/scripts/prepush.sh**.
Post - Push script	The post push script defines all tasks that have to be carried out after the push option is executed. Enter the location where the post push script is stored. For the CERT+ SaaS deployment, if the post push certificate is stored in the AppViewX Cloud Connector Box, ensure the following: • The .sh file for the post push script should be placed inside the deps folder in the Cloud Connector installation package. • Tenants are free to create a folder structure within the deps folder, as per requirement. • For example, you can save the postpush.sh file in the deps folder, or you can create a new folder in the deps folder and save the postpush.sh file in that new folder. • The path entered in the Post - Push script field should be relative to the deps folder.

Field	Description
	• For example, if the postpush.sh file is stored in the deps folder, your relative path will be /postpush.sh. • If the postpush.sh file is stored in the scripts folder (created by the tenant) within the deps folder, your relative path will be /scripts/postpush.sh.

Note: If a tenant deploys multiple Cloud Connector instances, it is mandatory that the pre and post push scripts should be available on all instances. In this situation, the folder structure within the deps folder should also be the same across all Cloud Connectors.

Pushing Server Certificate to a Device

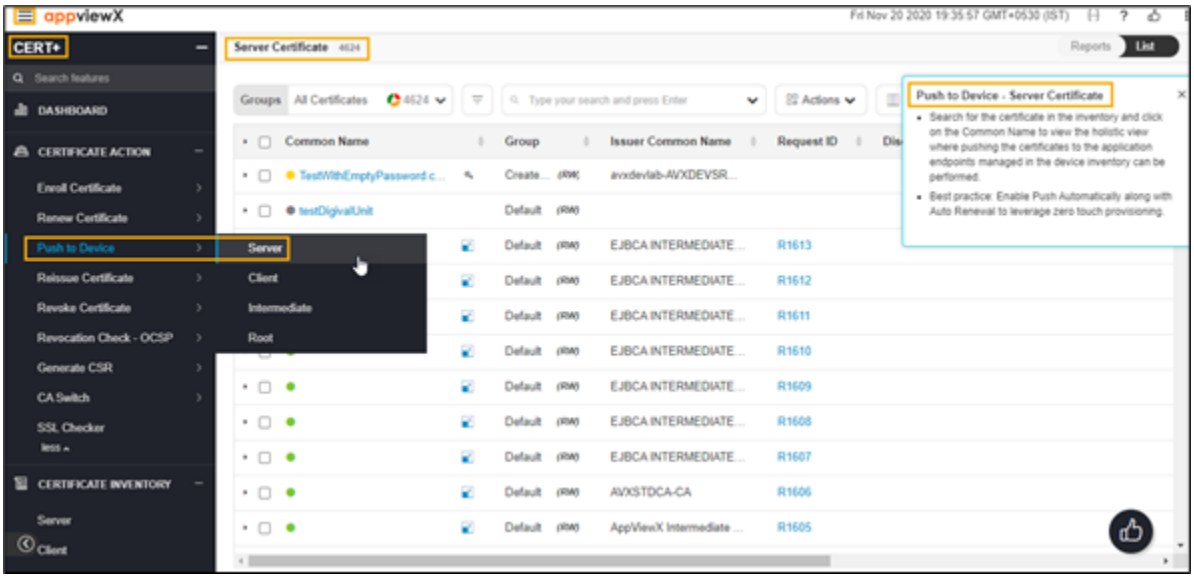
To push a certificate to a device,

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 ACTION**.
5. Select **Push to Device**, and then **Server**.

   The **Server Certificate** page appears.



6. In the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.
7. On the certificate topology page, click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.
8. On the **Confirmation** pop-up window, enter the comments if required. Upon confirmation based on policy, the approval process takes place. The current flow is based on the default policy of two-level approvals.
9. Click **OK**.

   A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.

10. Click **Approve** to approve the push request.
11. On the Confirmation screen that pop-up window:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert push to occur.
    c. Enter comments and click **Yes**.
12. The work order status displayed beside the connector updates to **Push-Review In Progress**.
13. Click **Implement** to implement the push request.
14. On the Confirmation screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert implementation to occur.
    c. Enter comments and click **Yes**.
15. Click the refresh icon on the top of the page until the topology updates.
16. After the push action is completed, the status updates to **Completed**.

Colour Codes Status

Colour

The topological view follows a colour codes scheme to identify certificate status.

Colour	Description
Green	The certificate is available and valid.
Red	.The certificate has expired
Gray	Certificate push action failed.
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

Pushing Client Certificate to a Device

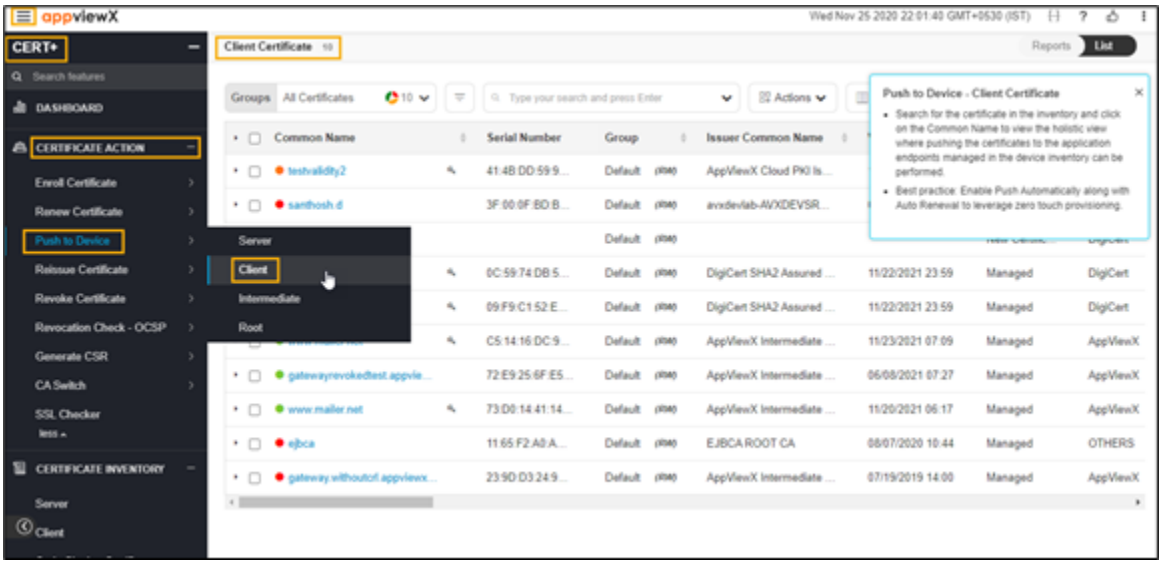
To push a certificate to a device,

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 ACTION**.
5. Select **Push to Device**, and then **Server**.

   The **Client Certificate** page appears.



6. In the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.
7. On the certificate topology page, click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.
8. On the **Confirmation** pop-up window, enter the comments if required. Upon confirmation based on policy, the approval process takes place. The current flow is based on the default policy of two-level approvals.
9. Click **OK**.

   A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.

10. Click **Approve** to approve the push request.
11. On the Confirmation screen that pop-up window:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert push to occur.
    c. Enter comments and click **Yes**.
12. The work order status displayed beside the connector updates to **Push-Review In Progress**.
13. Click **Implement** to implement the push request.
14. On the Confirmation screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert implementation to occur.
    c. Enter comments and click **Yes**.
15. Click the refresh icon on the top of the page until the topology updates.
16. After the push action is completed, the status updates to **Completed**.

Colour Codes Status

Colour

The topological view follows a colour codes scheme to identify certificate status.

Colour	Description
Green	The certificate is available and valid.
Red	.The certificate has expired
Gray	Certificate push action failed.
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

Pushing Intermediate Certificate to a Device

In the case of intermediate CA certificates or trust certificate renewal, the same should be pushed to the device in order to update the trust chain for the SSL communication. Otherwise, the SSL handshake will fail.

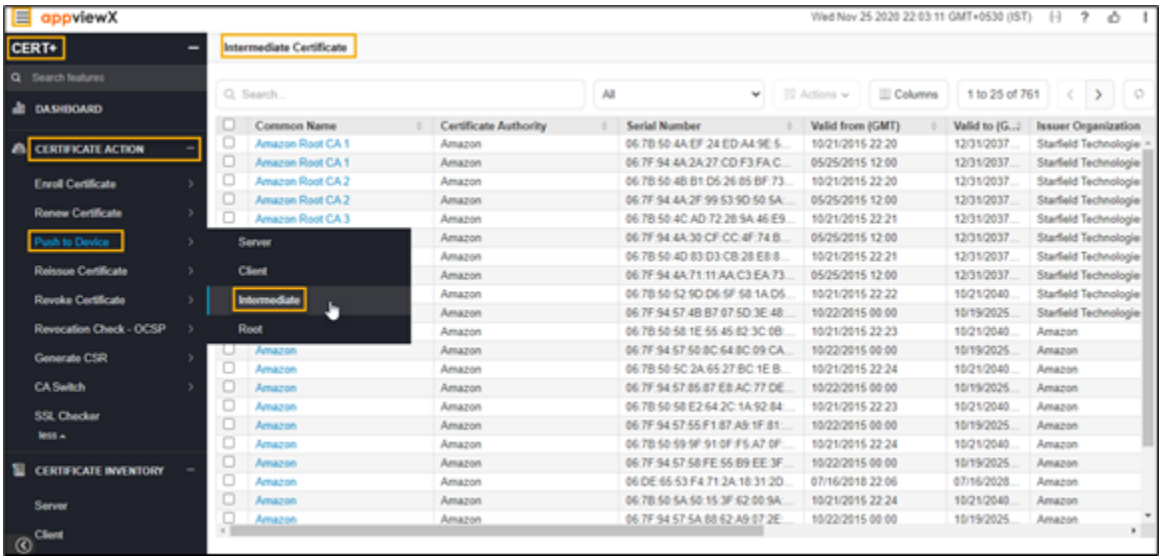
To push an intermediate certificate,

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+**.

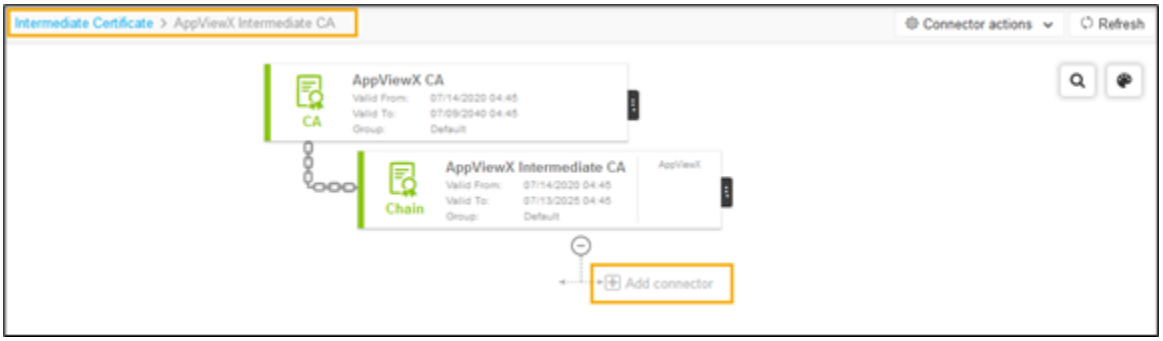
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Push to Device**, and then **Intermediate**.

The **Intermediate Certificate** page appears.



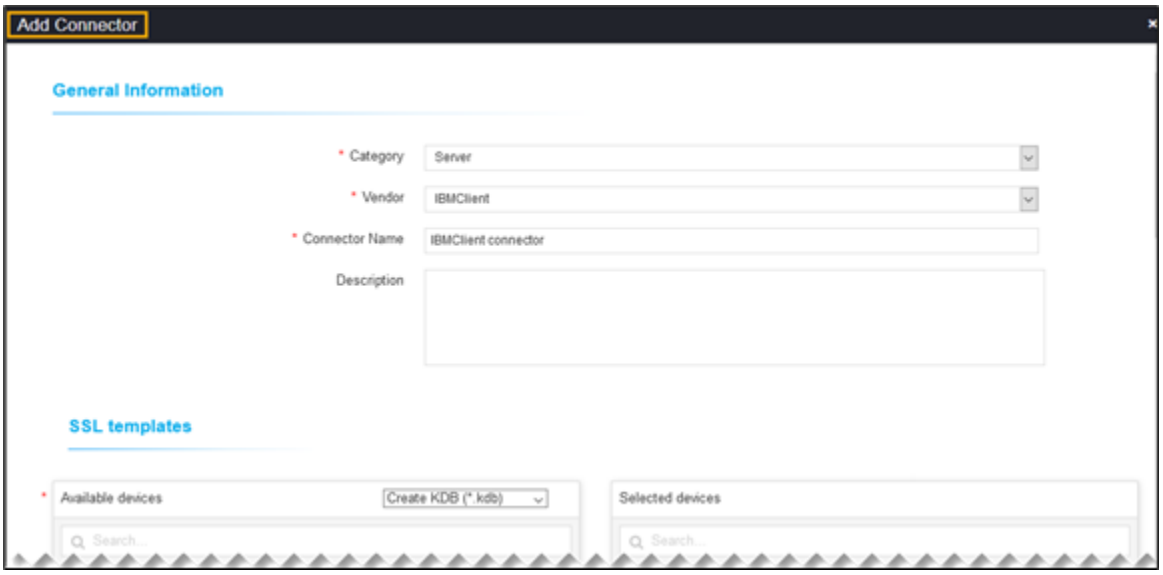
6. In the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.

   The holistic view appears.

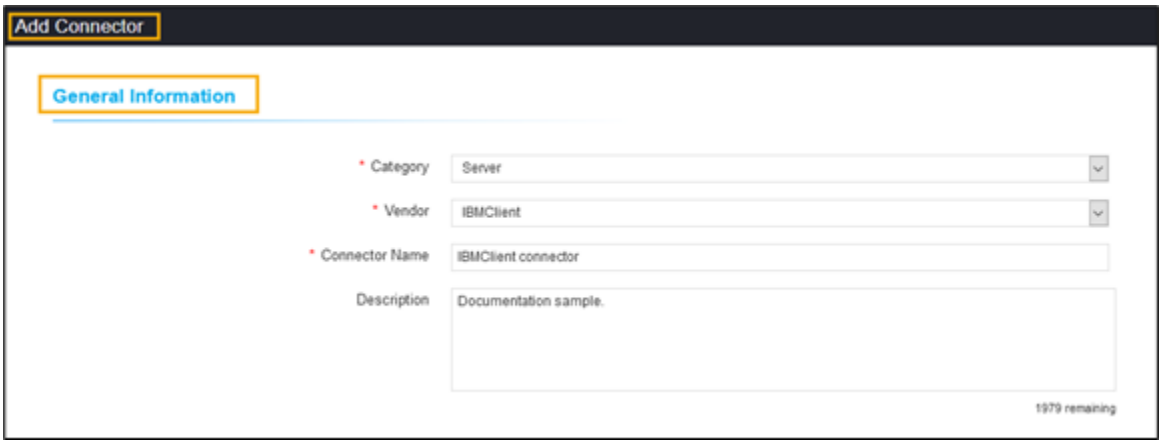


7. Click Add Connector in the holistic view page.

   The **Add Connector** page appears.



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

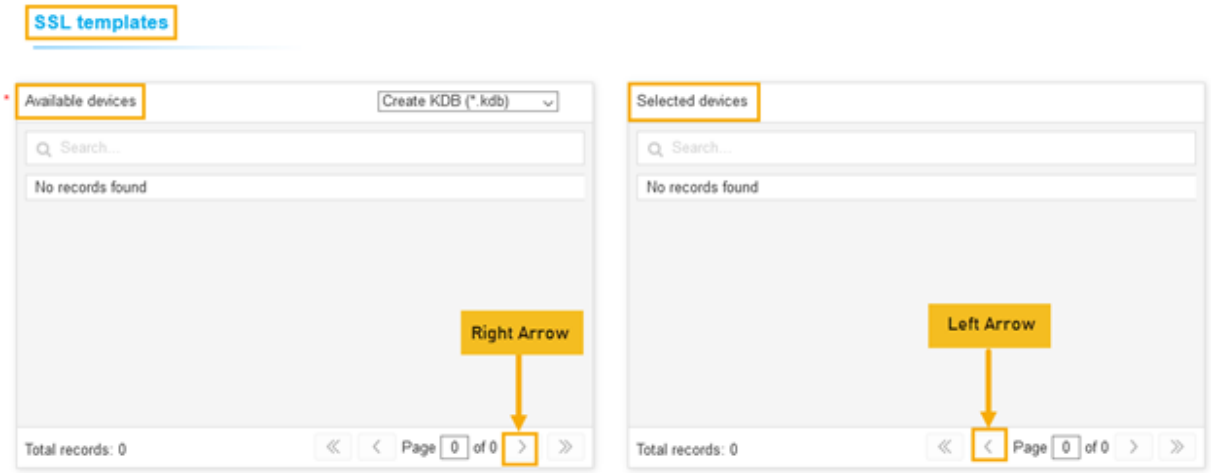


The following table describes the options available in the general information section:

Fields	Description
Category	Select the category from the dropdown list.
Connector Name	Enter the desired connector name.
Vendor	Select the vendor from the dropdown list.
Description	Enter a description in this field.

Fields	Description
	Note: You can enter a maximum of 2000 words in the field.

9. In the **SSL Template** section, select a device from the **Available devices** and click the right arrow mark to move the device to the **Selected devices** list.



Pushing Root Certificate to a Device

There can be renewal or change of root certificate in the trust store. In such occurrences, the user can push the root certificate to the desired endpoints to avoid the SSL handshake failure.

Steps to push a root certificate,

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

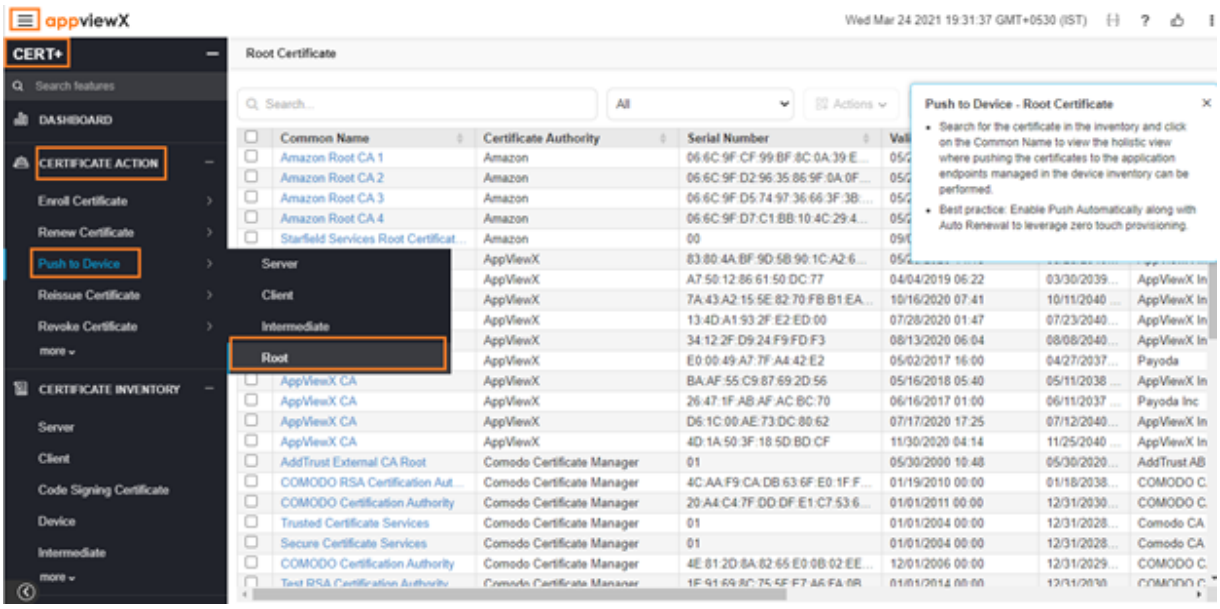
   The left navigation pane appears.

3. Click **CERT+**.

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

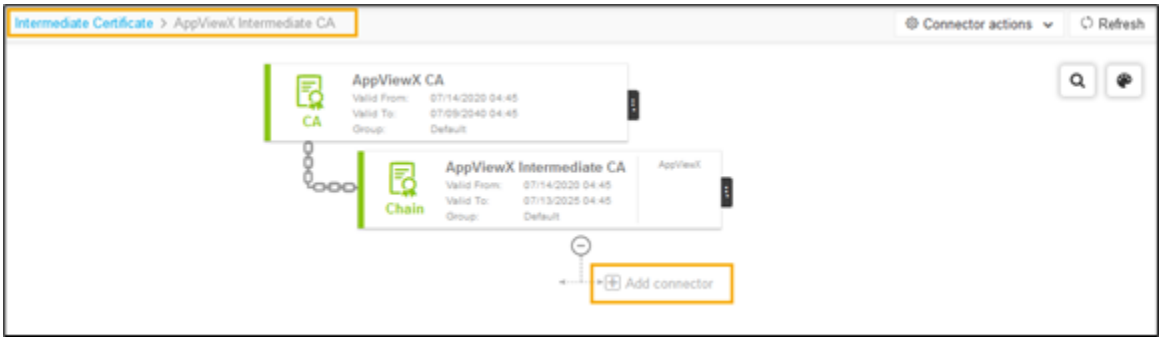
4. Expand **CERTIFICATE ACTION**.
5. Select **Push to Device**, and then **Intermediate**.

   The **Root Certificate** page appears.



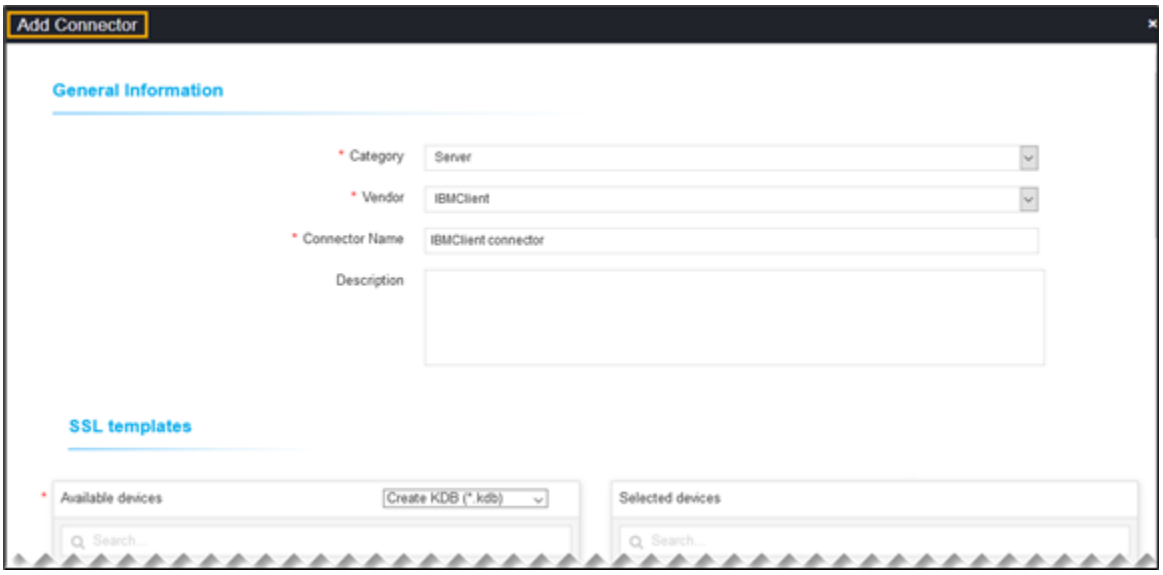
6. In the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.

   The holistic view appears.

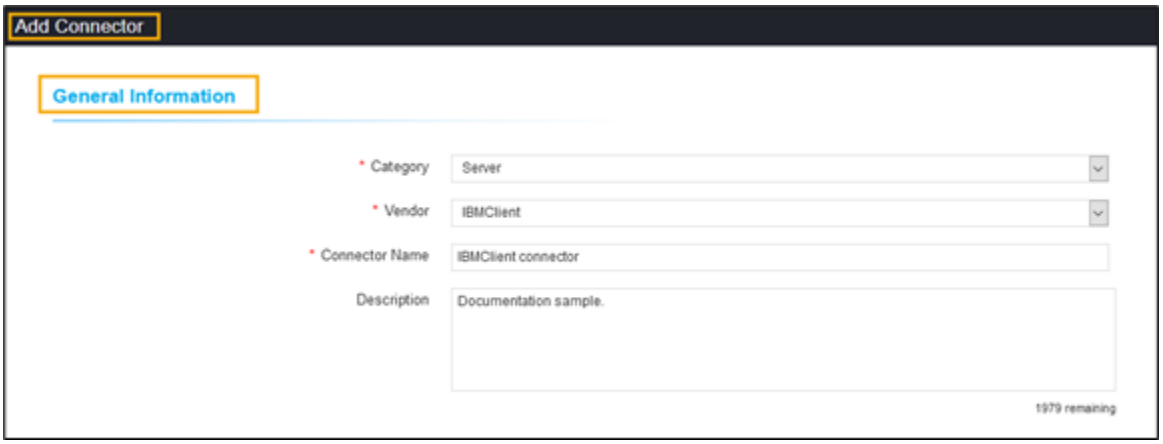


7. Click Add Connector in the holistic view page.

   The **Add Connector** page appears.



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

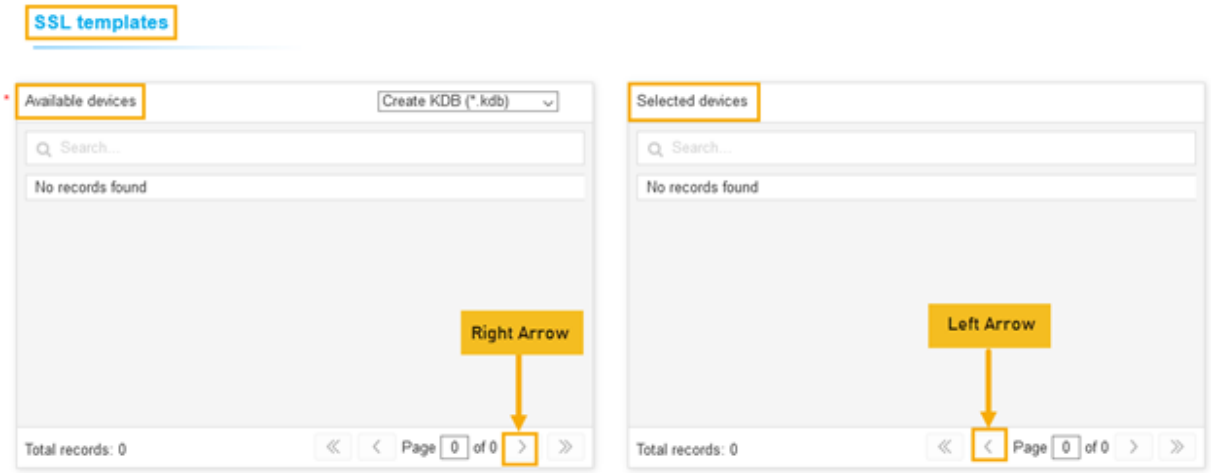


The following table describes the options available in the general information section:

Fields	Description
Category	Select the category from the dropdown list.
Connector Name	Enter the desired connector name.
Vendor	Select the vendor from the dropdown list.
Description	Enter a description in this field.

Fields	Description
	Note: You can enter a maximum of 2000 words in the field.

9. In the **SSL Template** section, select a device from the **Available devices** and click the right arrow mark to move the device to the **Selected devices** list.



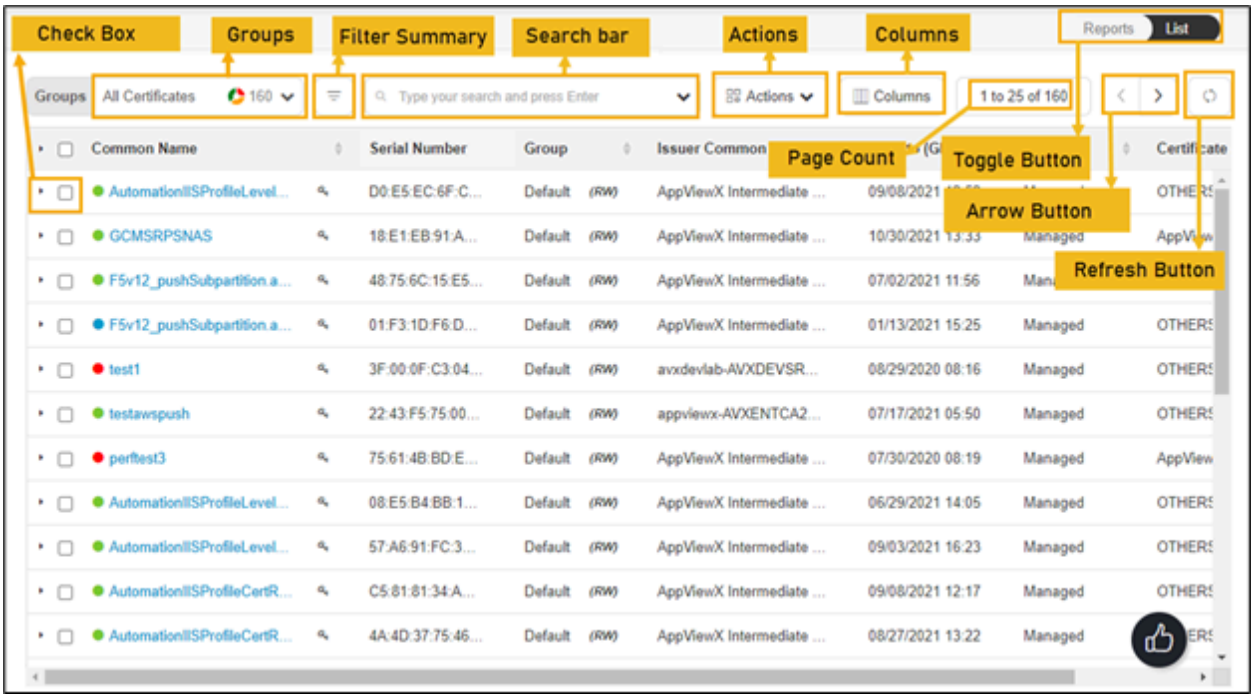
Reissuing Certificate

- Overview
- Reissuing Server Certificate
- Reissuing Client Certificate

Overview

To update or modify the certificate parameters, it can be reissued by the same certificate authority who issued it. A common use case will be an addition of SAN names. Reissuing certificates will not be considered as a new order to the CA.

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

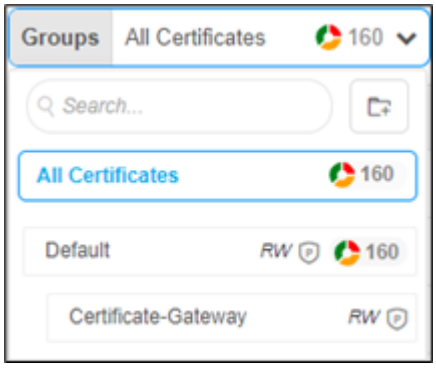


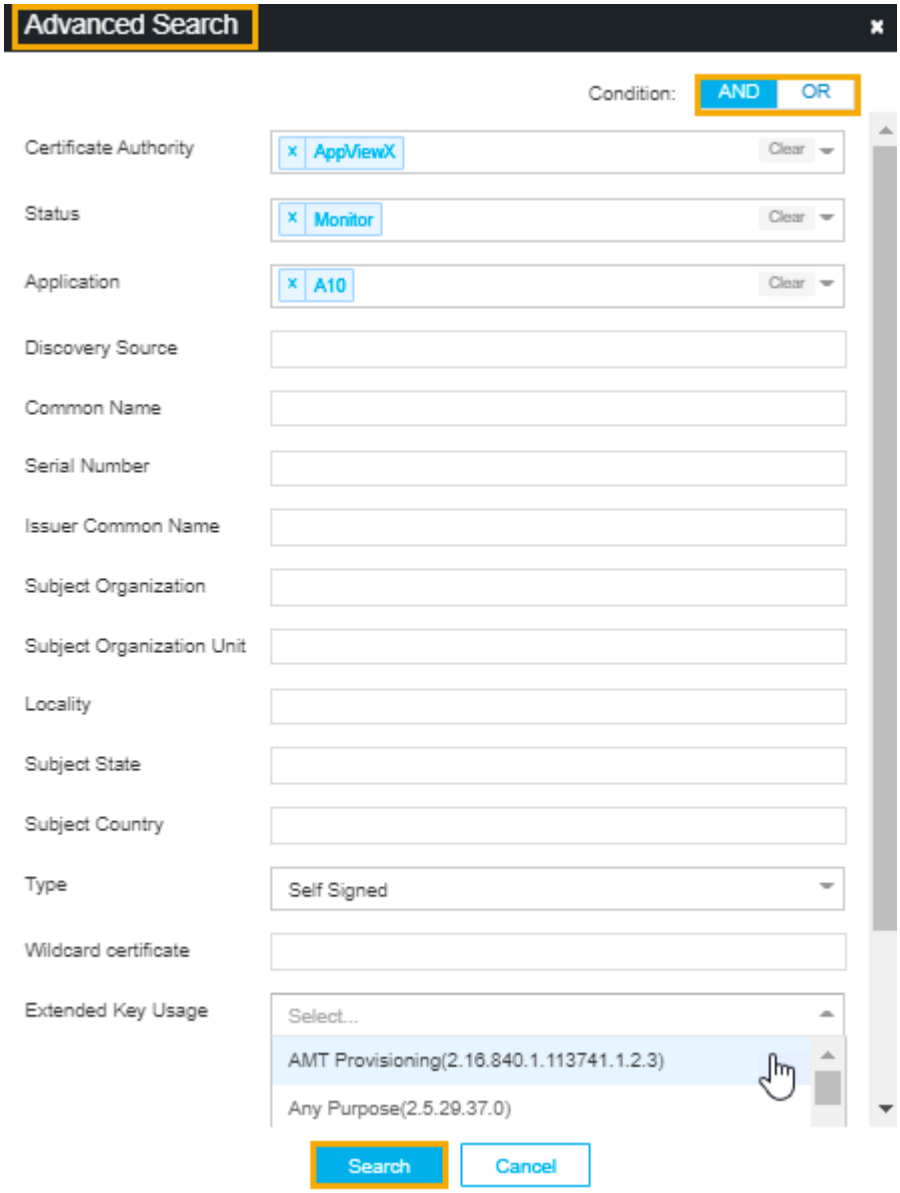
Note:

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

The following table describes the options available on the reissue certificate page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected.

Options	Description
	
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description
	

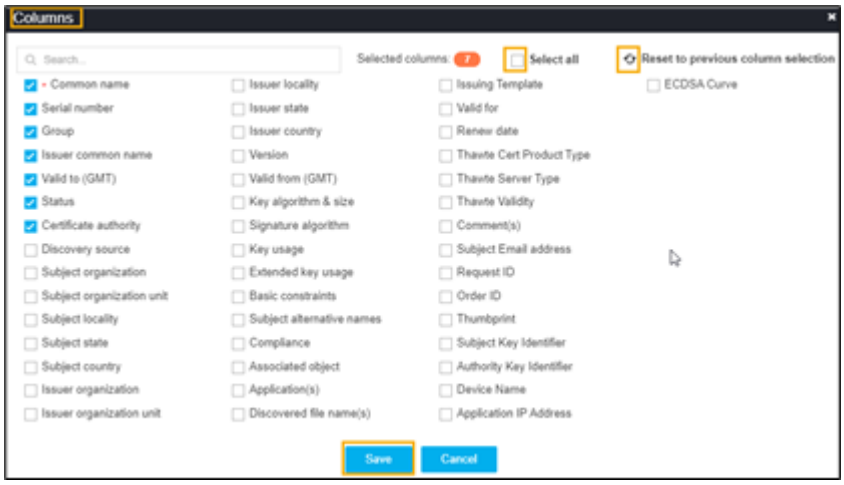
The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Certificate Authority</td><td>Allows you to select the desired CA from the dropdown list.</td></tr>
<tr><td>Status</td><td>Allows you to select the desired status certificate. The possible options are,

• Manage
• Monitor
• New certificate.</td></tr>
<tr><td>Discovery Source</td><td>Enter the source of the discovery.</td></tr>
<tr><td>Common Name</td><td>Enter the common name of the certificate.</td></tr>
<tr><td>Serial Number</td><td>Enter the serial number of the certificate.</td></tr>
<tr><td>Issuer Common Name</td><td>Enter the name of the certificate issuer.</td></tr>
<tr><td>Subject Organization</td><td>Enter the subject of the organization.</td></tr>
<tr><td>Subject Organization Unit</td><td>Enter the subject of the organization’s unit.</td></tr>
<tr><td>Locality</td><td>Enter the specific locality.</td></tr>
<tr><td>Subject State</td><td>State Enter the state of the certificate’s subject.</td></tr>
<tr><td>Subject Country</td><td>Country of the subject.</td></tr>
<tr><td>Type</td><td>Type of the certificate.</td></tr>
<tr><td>Wildcard certificate</td><td>Enter the wildcard certificates.</td></tr>
<tr><td>Extended Key Usage</td><td>Allows you to select the EKU from the dropdown list.</td></tr>
<tr><td>Search</td><td>Click the Search button to get the results from the search.</td></tr>
</table>
</td></tr>
<tr><td>Actions</td><td>Displays the list of actions. The possible actions are,

• Export Certificates
• Import Certificates</td></tr>
</table>

Options	Description
	• Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are,

Options	Description
	• Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Reissuing Server Certificate

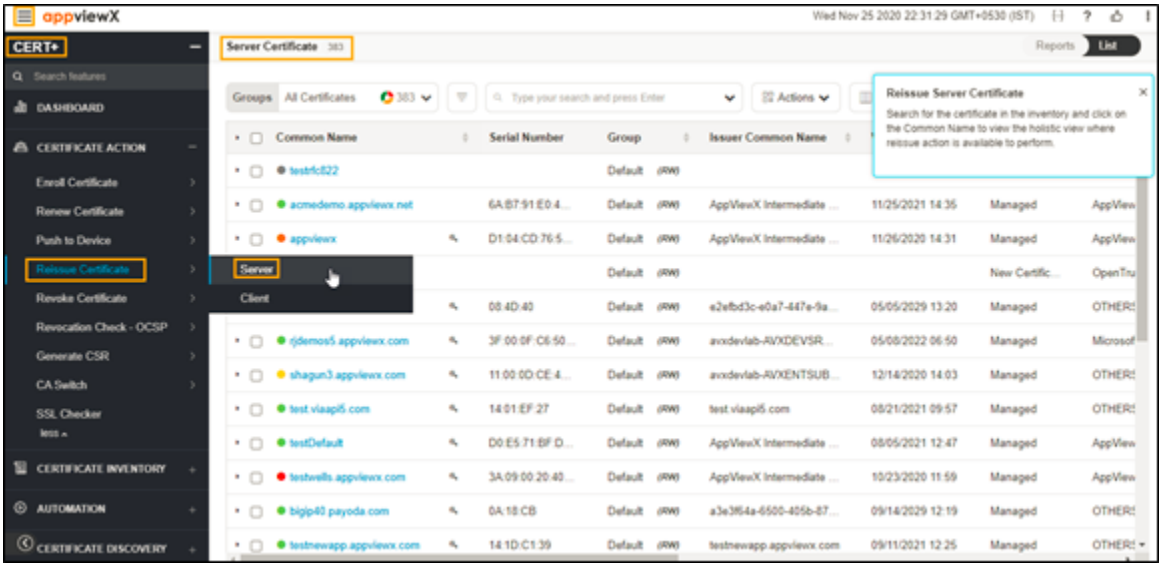
To reissue a server certificate,

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

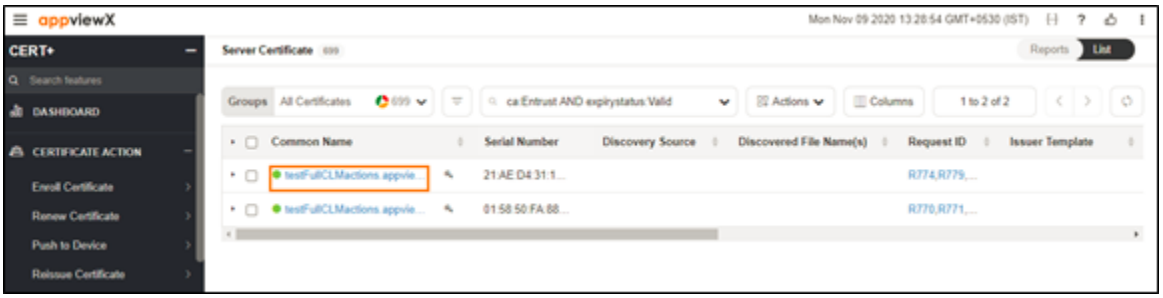
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Reissue Certificate**, and then **Server**.

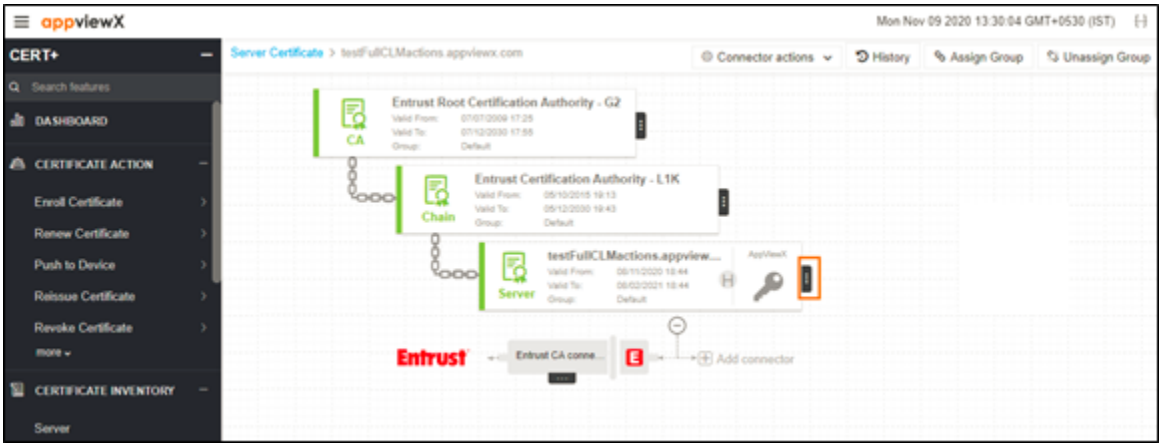
   The **Server Certificate** page appears.



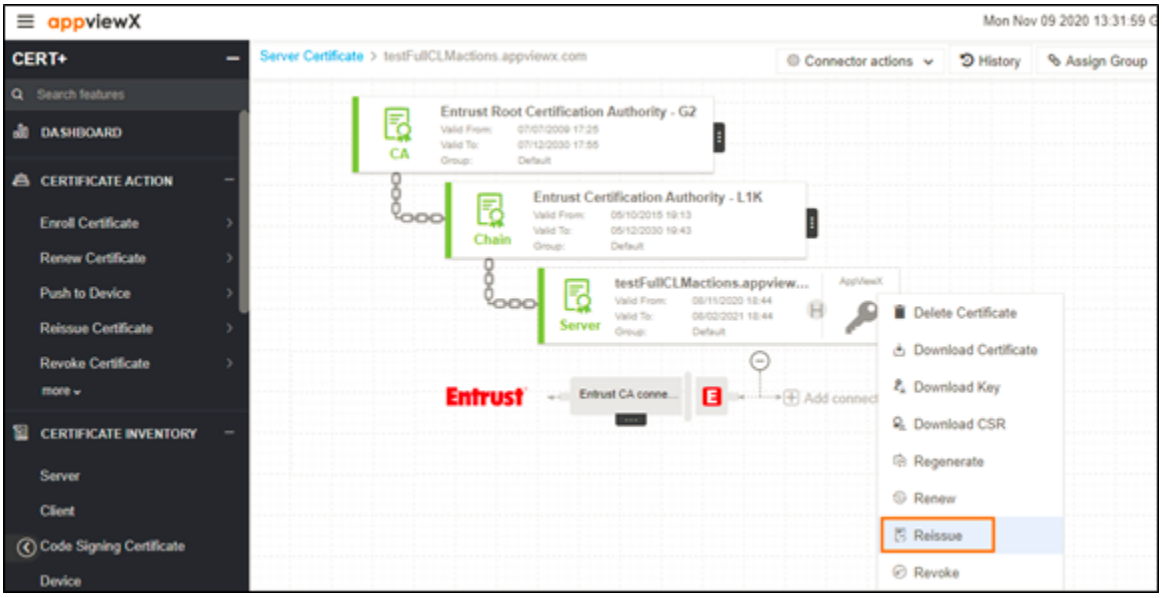
6. Click the **Common Name** of the certificate to navigate into the holistic view.



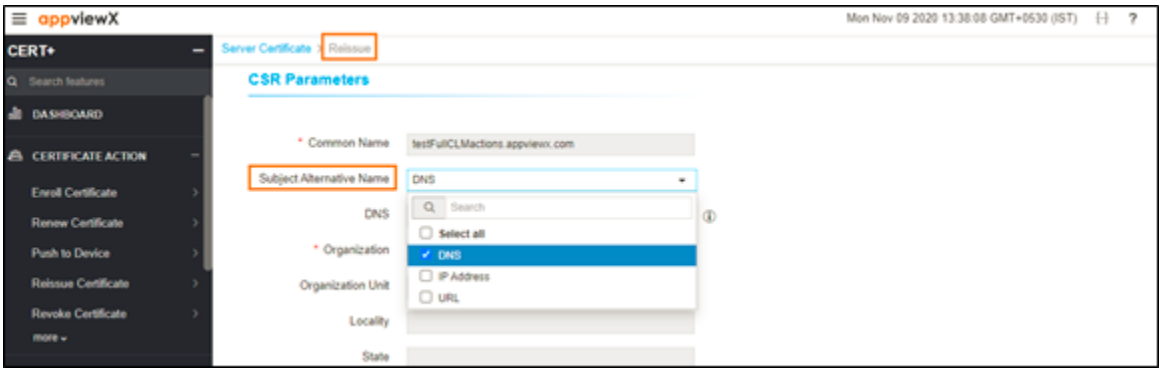
7. Hover over the vertical eclipse icon on the certificate.



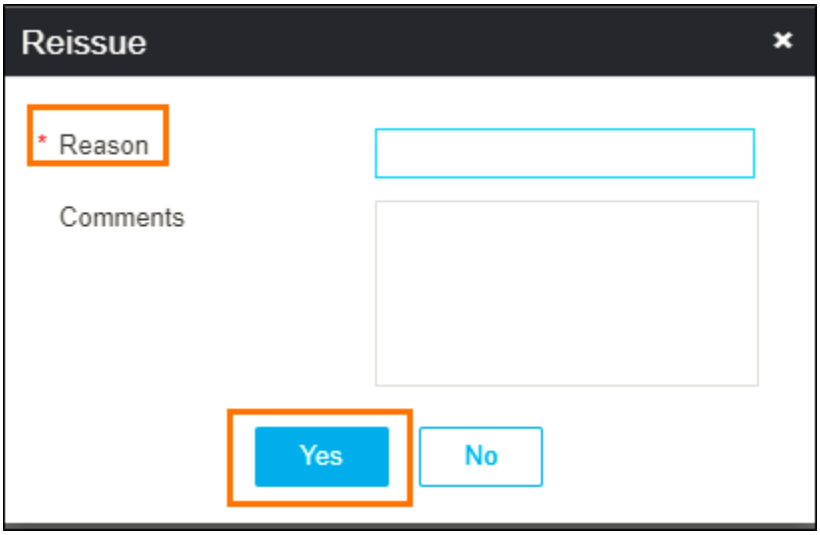
8. Click **Reissue** from the drop-down list.



9. In the **Server Certificate** > **Reissue** page, if required, user can edit the **Subject Alternate Names**. Also, the **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can be modified.

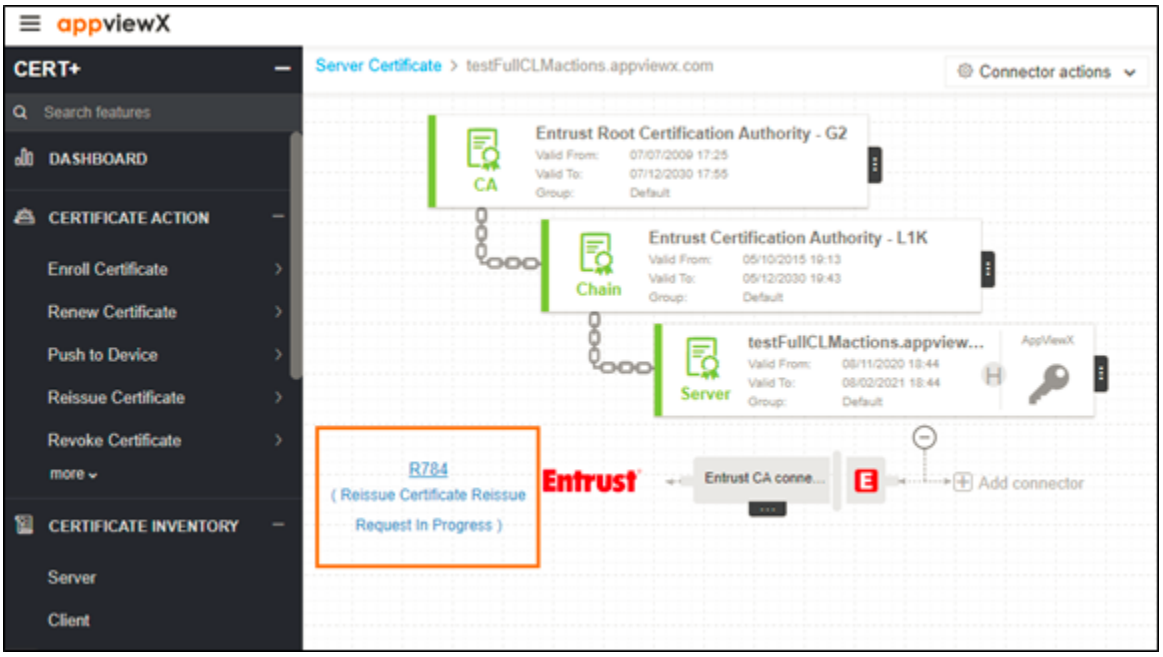


10. Click **Reissue**.
11. In the Reissue pop up window, provide the **Reason** and **Comments.**



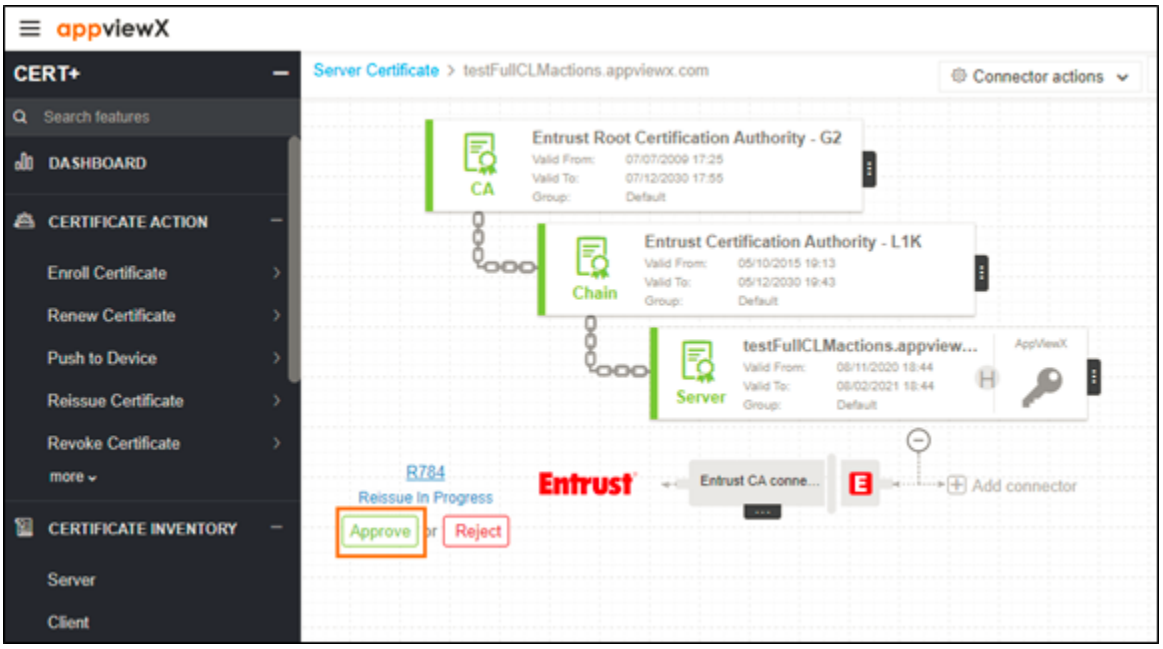
12. Click **Yes**.

    The reissue process is initiated.

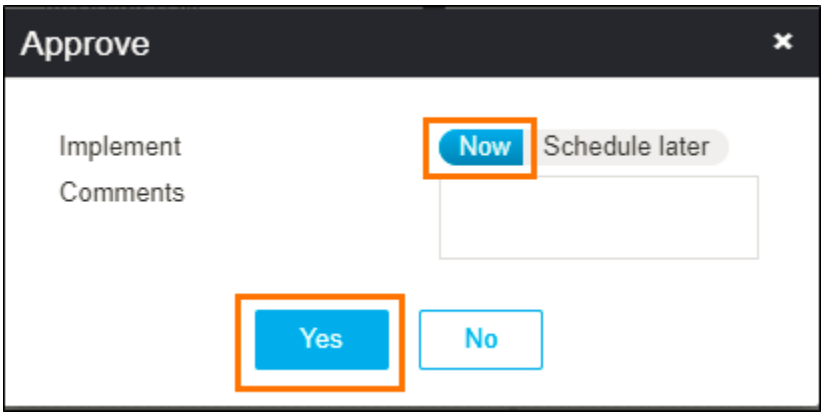


13. **Note:** If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

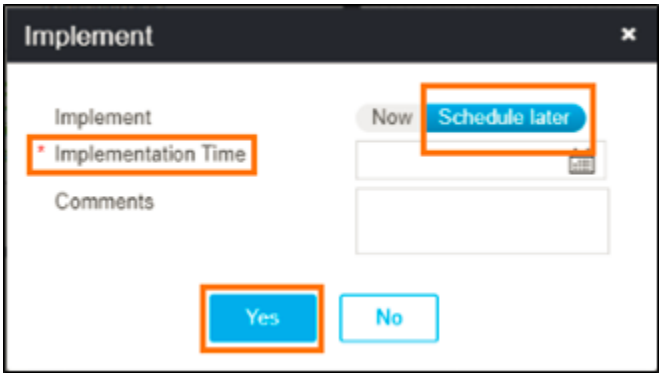
Click **Approve** button to proceed.



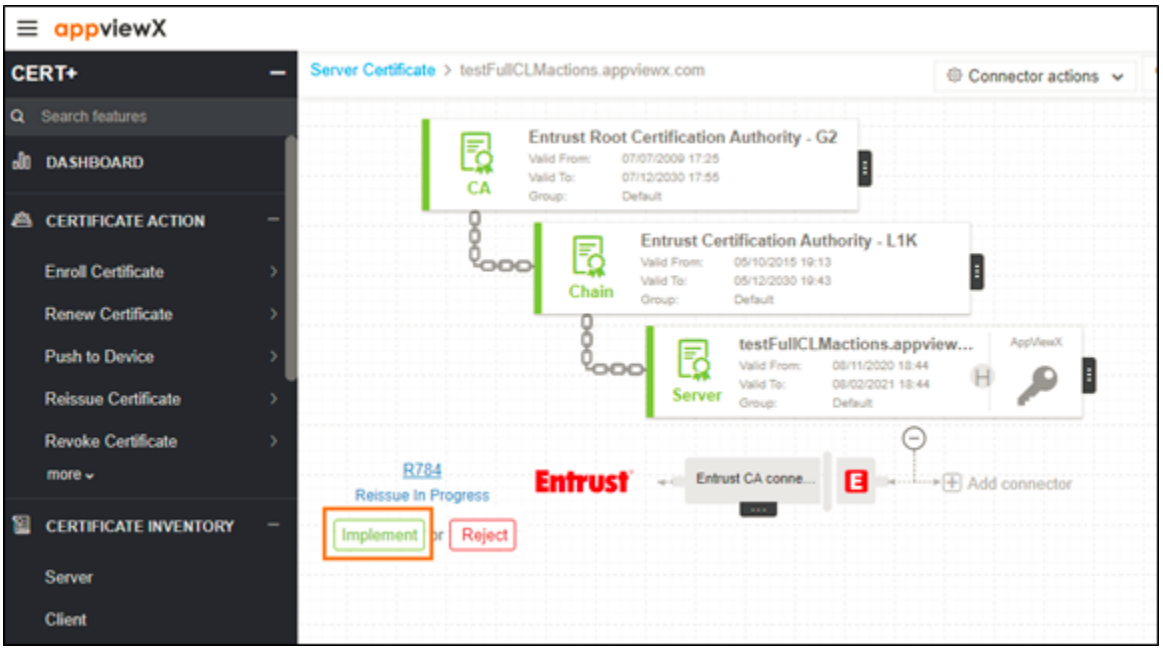
14. In the **Approve** pop-up window, provide the **Comments**.



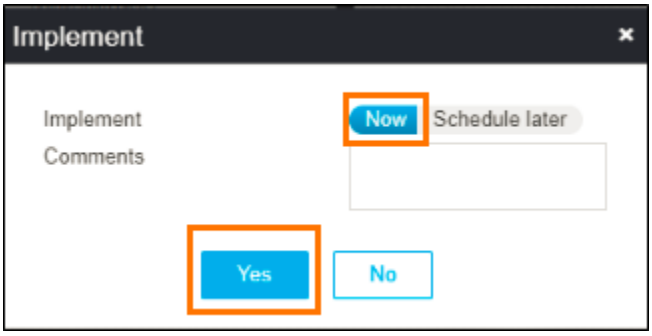
15. Click **Yes**.
16. Click **Schedule later** if the workflow request has to be approved automatically in the future.



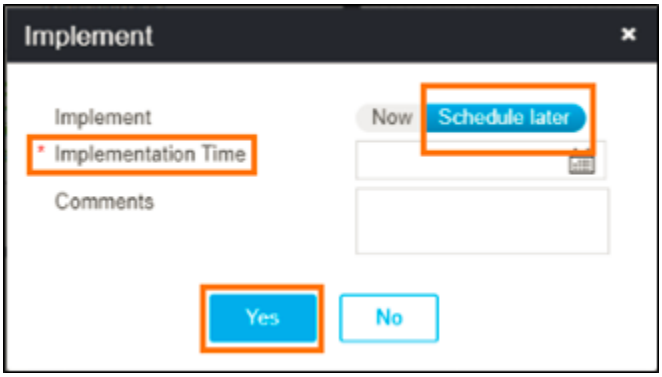
17. Click **Implement**.



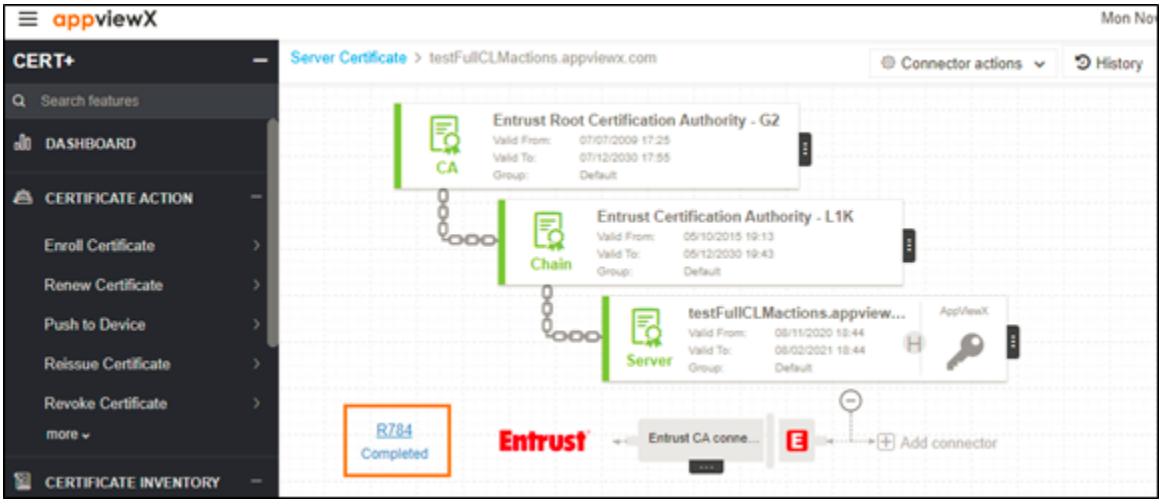
18. In the **Implement** pop-up window, provide the **Comments.**



19. Click **Yes**.
20. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



21. After the reissue action is completed, the status updates to **Completed**.



Reissuing Client Certificate

To reissue a client certificate,

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

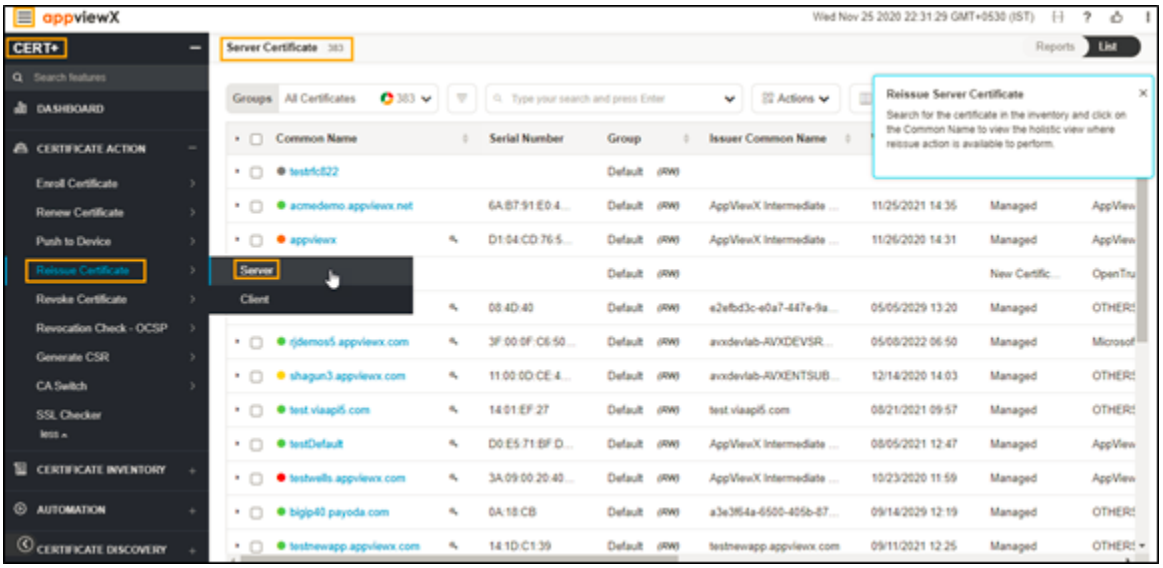
   The left navigation pane appears.

3. Click **CERT+**.

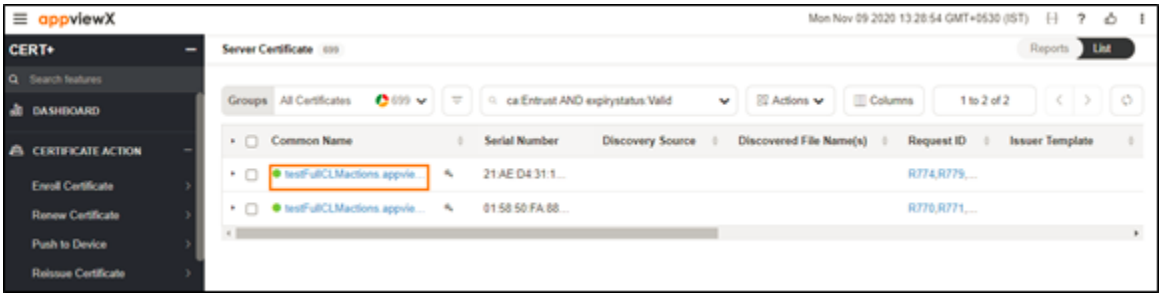
   The **CERT+** left navigation pane appears.

4. Expand **CERTIFICATE ACTION**.
5. Select **Reissue Certificate**, and then **Client**.

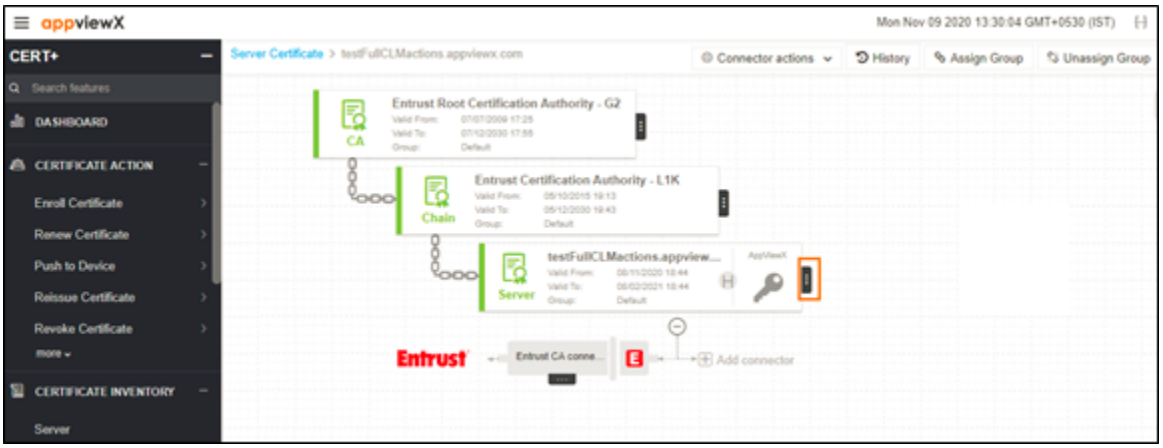
   The **Client Certificate** page appears.



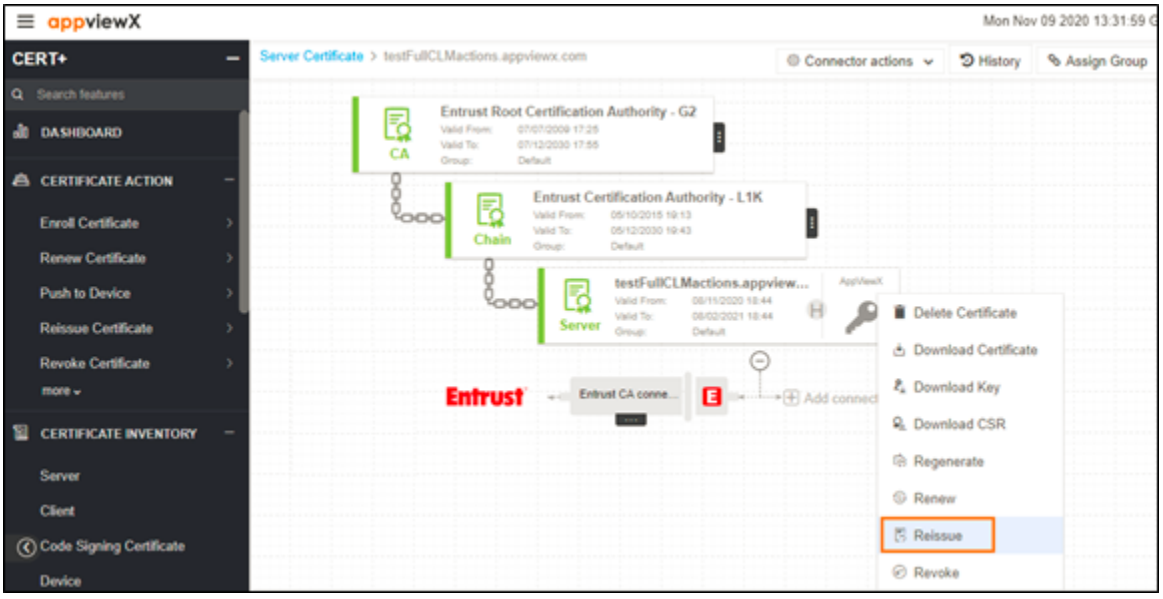
6. Click the **Common Name** of the certificate to navigate into the holistic view.



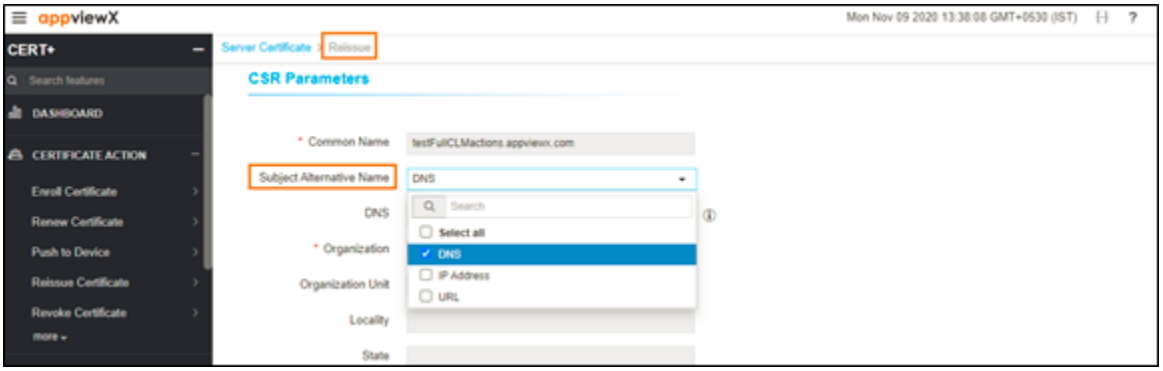
7. Hover over the vertical eclipse icon on the certificate.



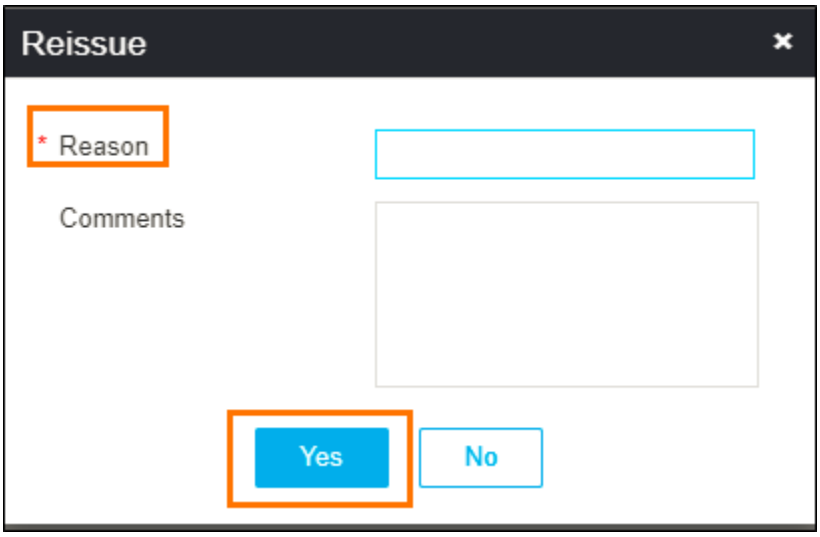
8. Click **Reissue** from the drop-down list.



9. In the **Client Certificate** > **Reissue** page, if required, user can edit the **Subject Alternate Names**. Also, the **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can be modified.

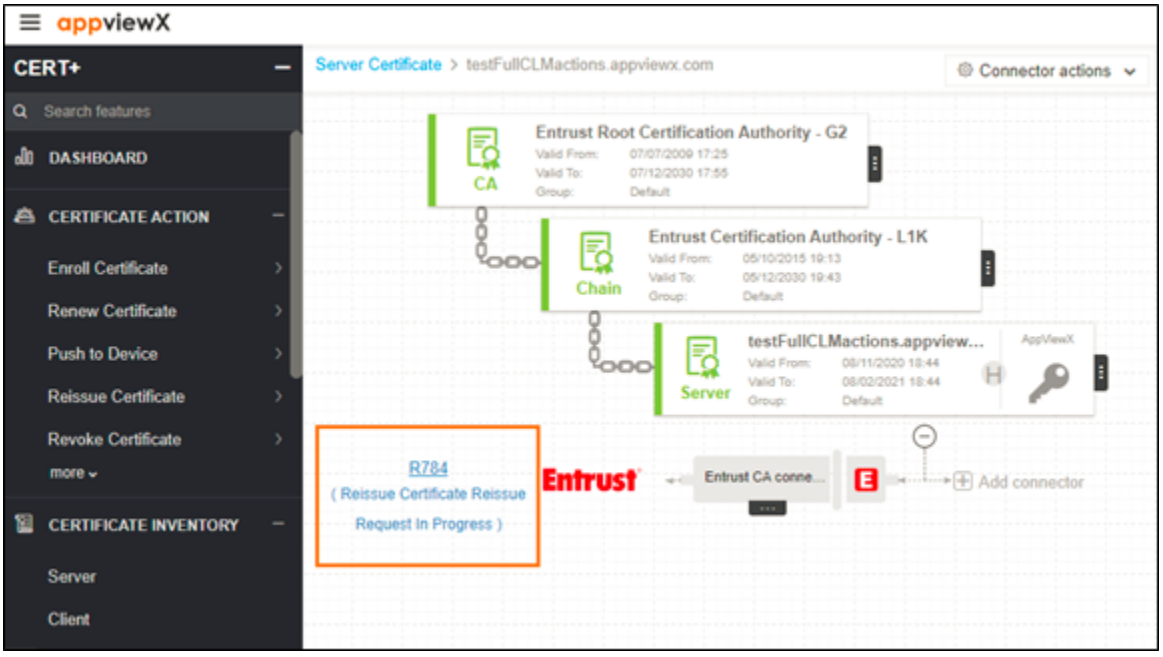


10. Click **Reissue**.
11. In the Reissue pop up window, provide the **Reason** and **Comments.**

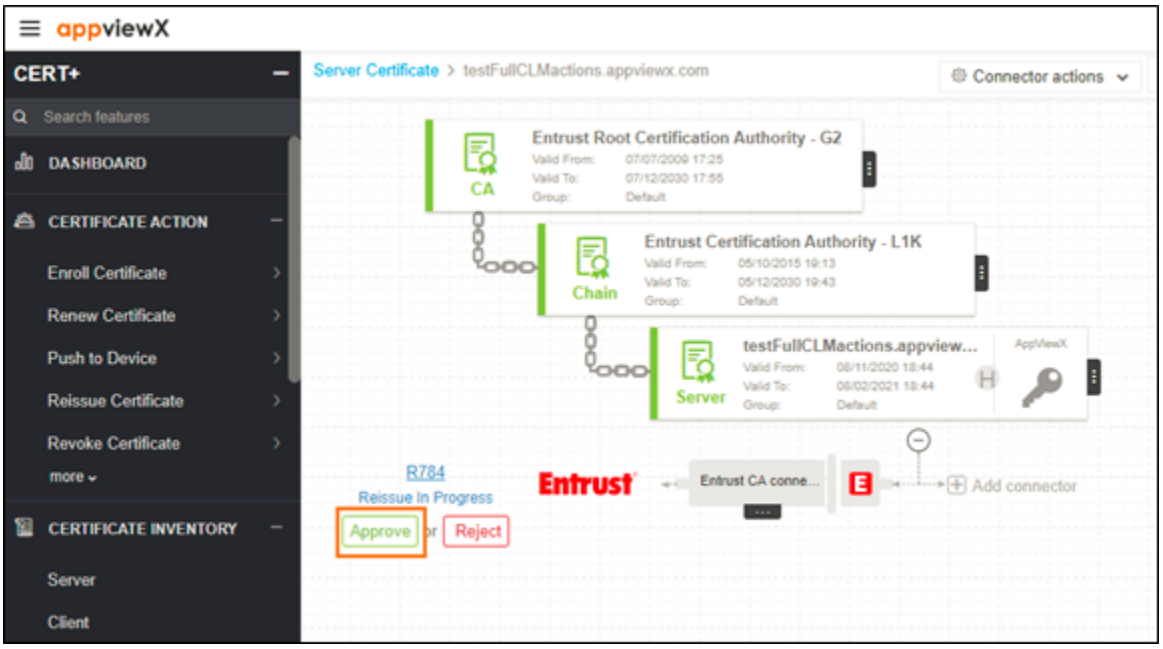


12. Click **Yes**.

    The reissue process is initiated.

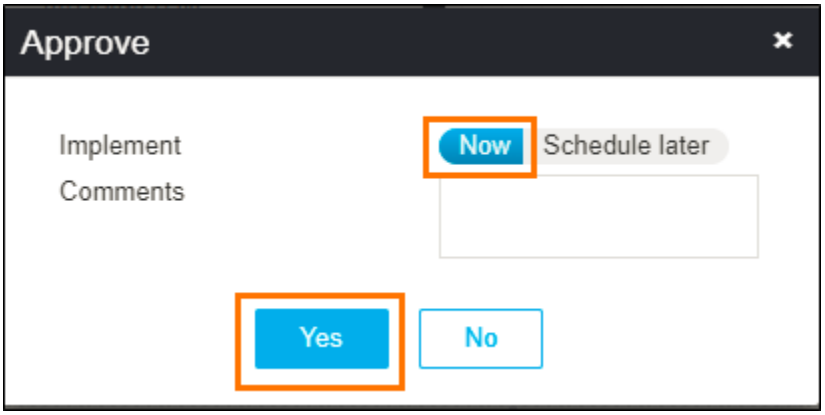


13. Click **Approve** button to proceed.

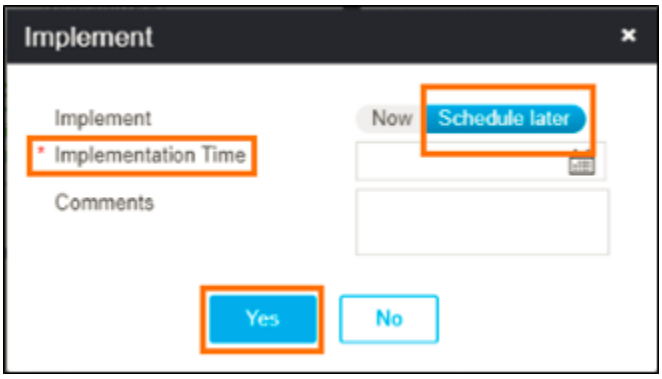


Note: If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

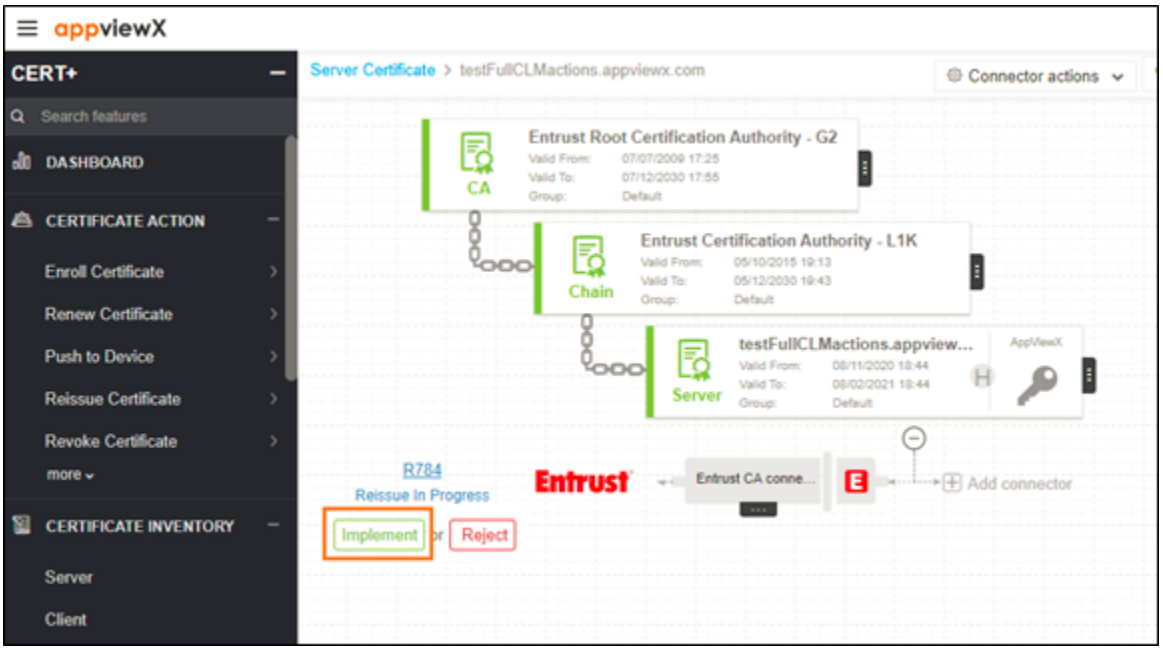
14. In the **Approve** pop-up window, provide the **Comments**.



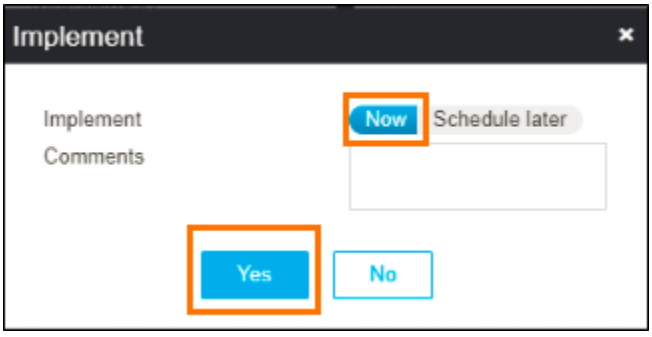
15. Click **Yes**.
16. Click **Schedule later** if the workflow request has to be approved automatically in the future.



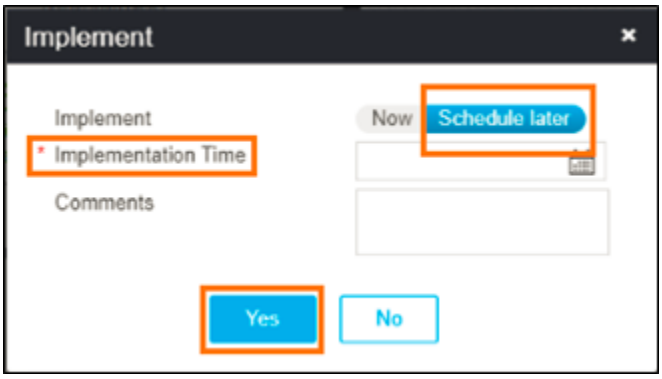
17. Click **Implement**.



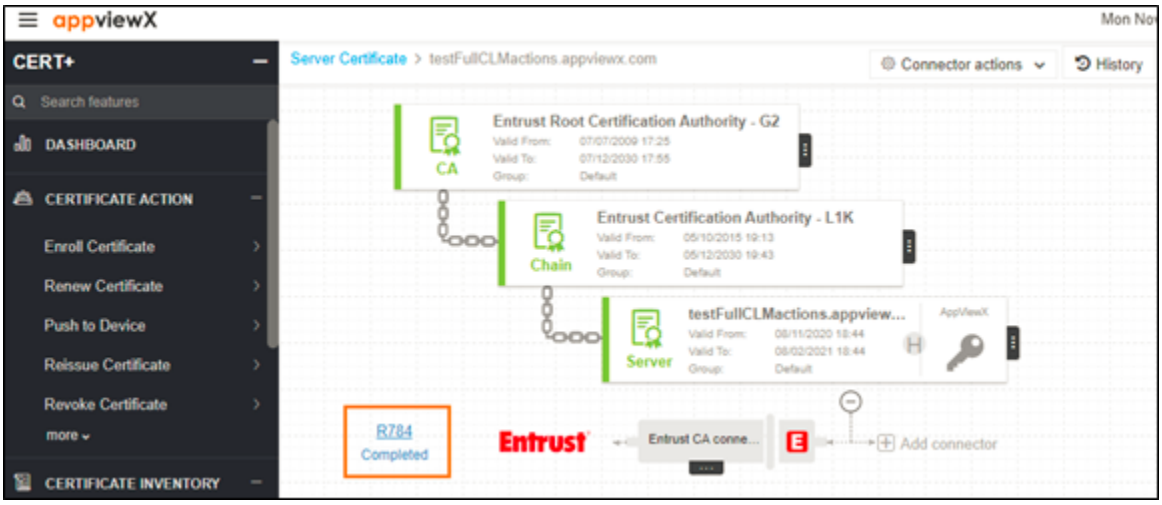
18. In the **Implement** pop-up window, provide the **Comments.**



19. Click **Yes**.
20. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



21. After the reissue action is completed, the status updates to **Completed**.



Revoking Certificate

- Overview
- Revoking Server Certificate
- Revoking Client Certificate
- Revoking Device Certificate
- Revoking Code Signing Certificate

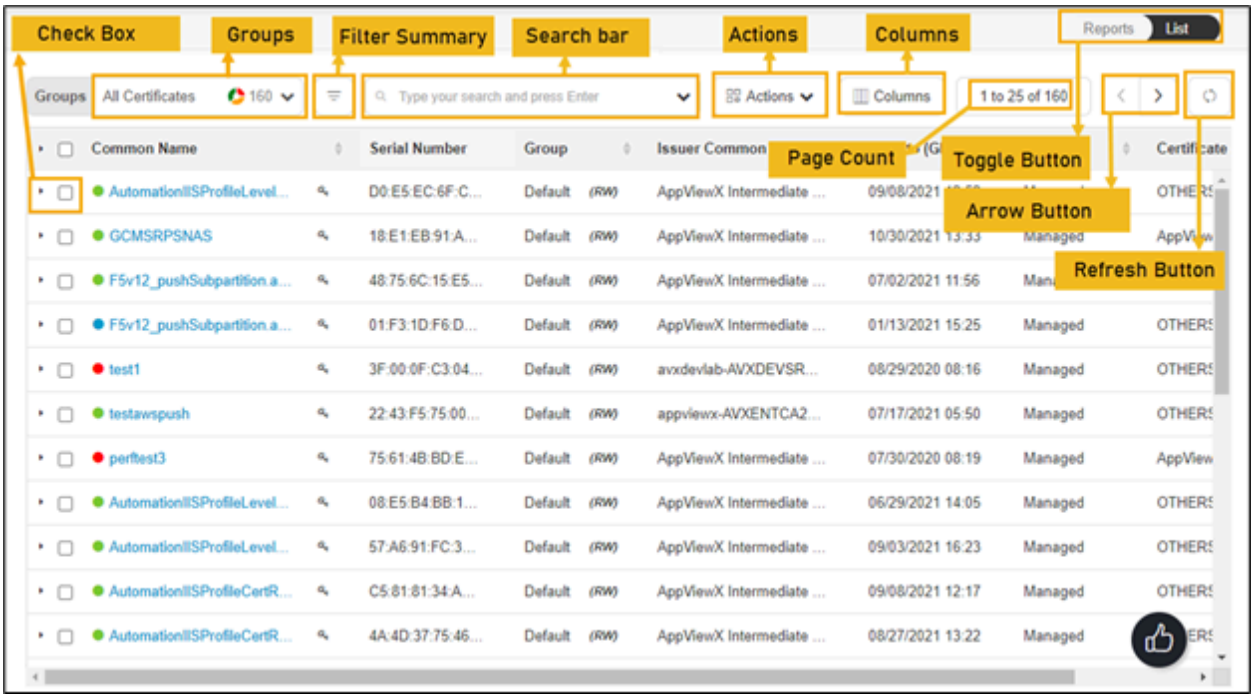
Overview

Revocation is the process of making a certificate invalid. For example, you might need to revoke a certificate if the certificate is no longer required (or) certificate's private key is compromised. Make sure that you have permission to revoke a certificate and submit a request to the certificate authority. As soon

as the certificate is revoked, it is not considered to be a trusted certificate. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.

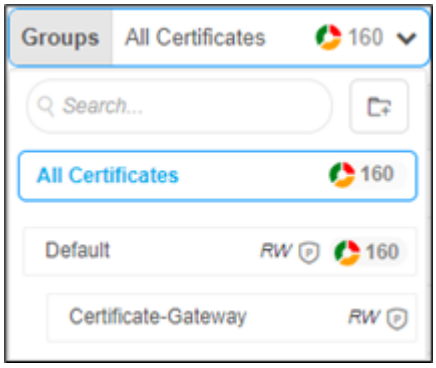
Note:

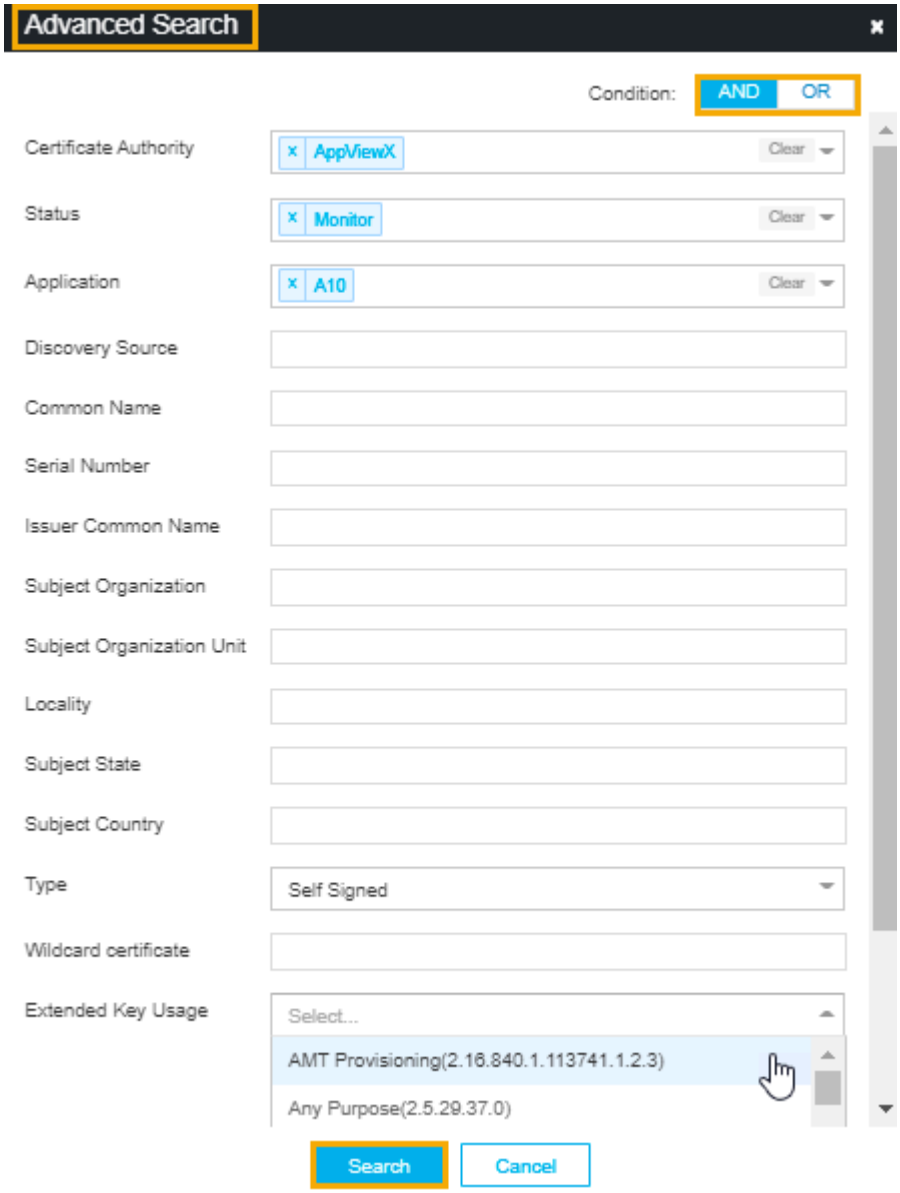
You can revoke the certificates via the Certificate Inventory section also.



The following table describes the options available on the revoke certificate page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected.

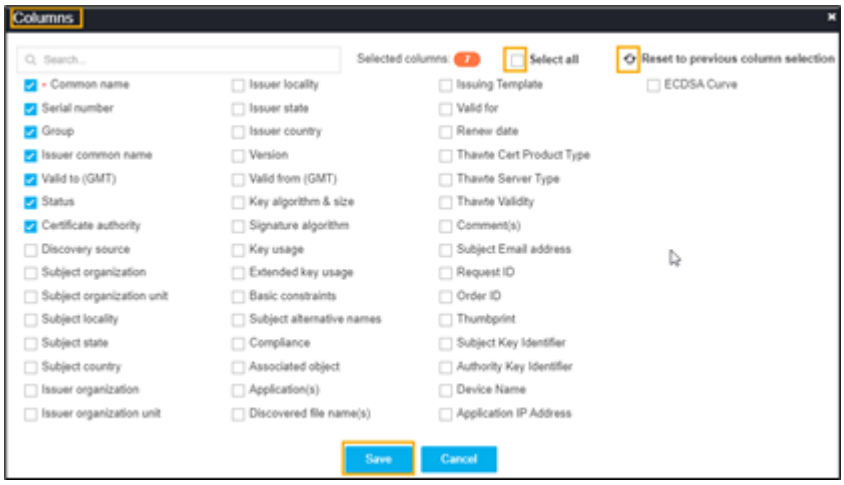
Options	Description
	
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description
	 The following table describes the options available in the Advanced Search feature: **Options** | **Description** **Condition** | Displays the type of the desired search on the page. The possible options are, • AND • OR.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Certificate Authority</td><td>Allows you to select the desired CA from the dropdown list.</td></tr>
<tr><td>Status</td><td>Allows you to select the desired status certificate. The possible options are,

• Manage
• Monitor
• New certificate.</td></tr>
<tr><td>Discovery Source</td><td>Enter the source of the discovery.</td></tr>
<tr><td>Common Name</td><td>Enter the common name of the certificate.</td></tr>
<tr><td>Serial Number</td><td>Enter the serial number of the certificate.</td></tr>
<tr><td>Issuer Common Name</td><td>Enter the name of the certificate issuer.</td></tr>
<tr><td>Subject Organization</td><td>Enter the subject of the organization.</td></tr>
<tr><td>Subject Organization Unit</td><td>Enter the subject of the organization’s unit.</td></tr>
<tr><td>Locality</td><td>Enter the specific locality.</td></tr>
<tr><td>Subject State</td><td>State Enter the state of the certificate’s subject.</td></tr>
<tr><td>Subject Country</td><td>Country of the subject.</td></tr>
<tr><td>Type</td><td>Type of the certificate.</td></tr>
<tr><td>Wildcard certificate</td><td>Enter the wildcard certificates.</td></tr>
<tr><td>Extended Key Usage</td><td>Allows you to select the EKU from the dropdown list.</td></tr>
<tr><td>Search</td><td>Click the Search button to get the results from the search.</td></tr>
</table>
</td></tr>
<tr><td>Actions</td><td>Displays the list of actions. The possible actions are,

• Export Certificates
• Import Certificates</td></tr>
</table>

Options	Description
	• Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are,

Options	Description
	• Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Revoking Server Certificate

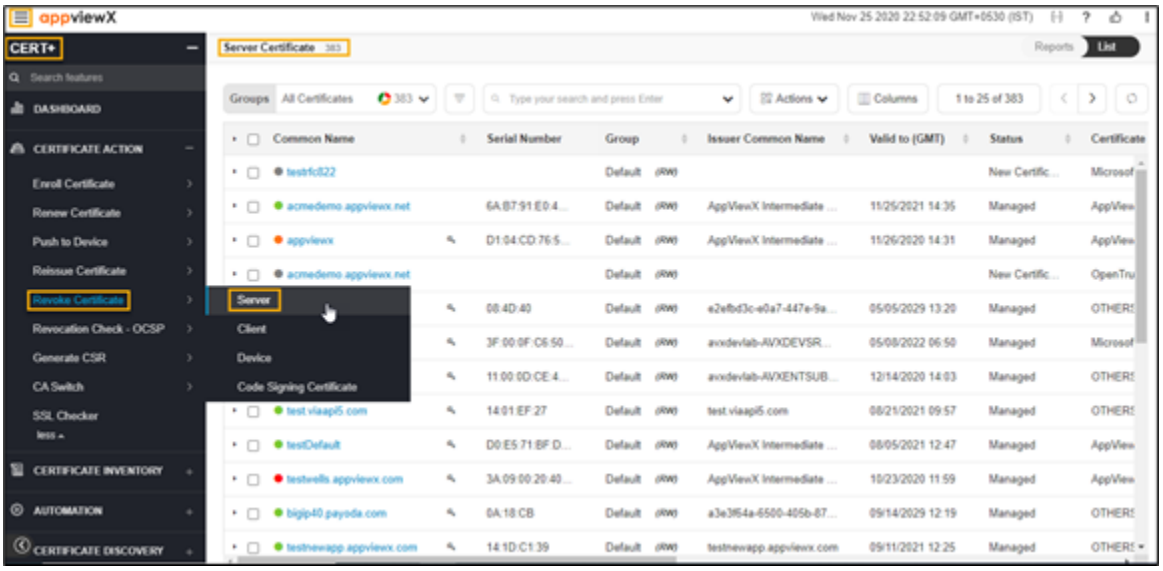
Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

To revoke a server certificate:

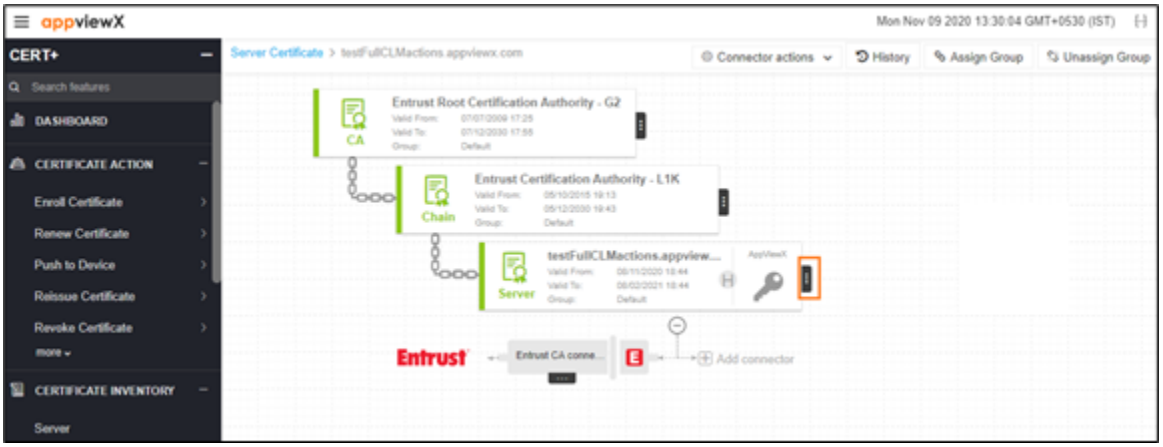
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Revoke Certificate**, and then **Server**.

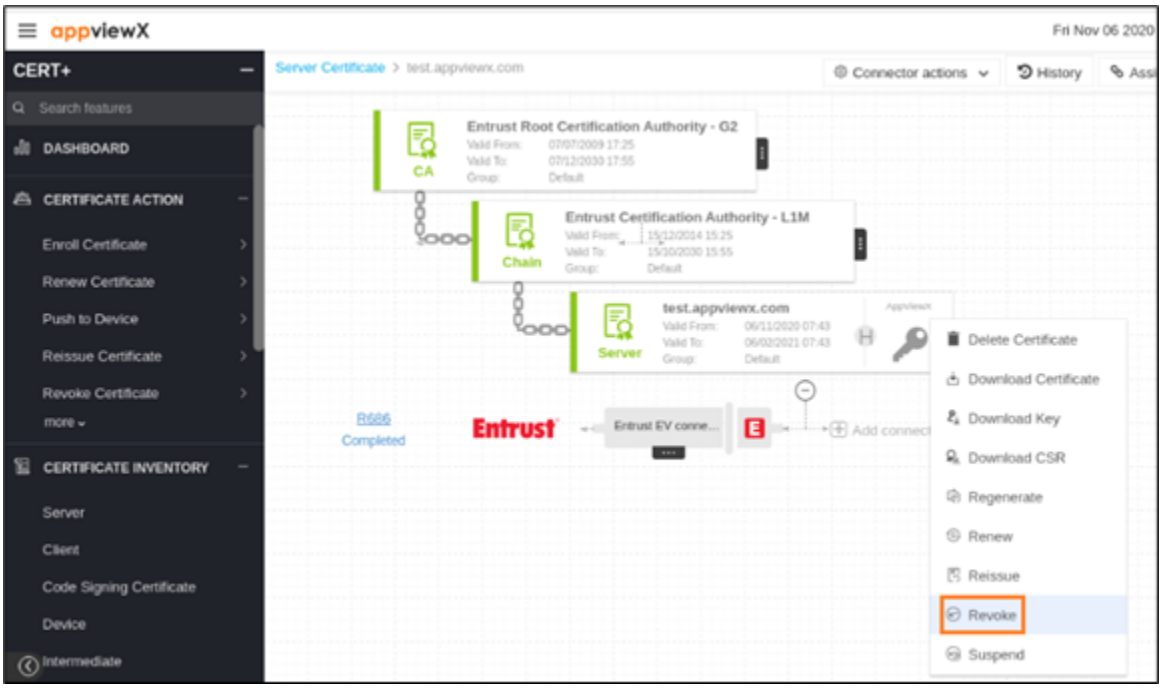
   The **Server Certificate** page appears.



6. Click the **Common Name** of the certificate to navigate into the holistic view.
7. Hover over the vertical eclipse icon on the certificate.

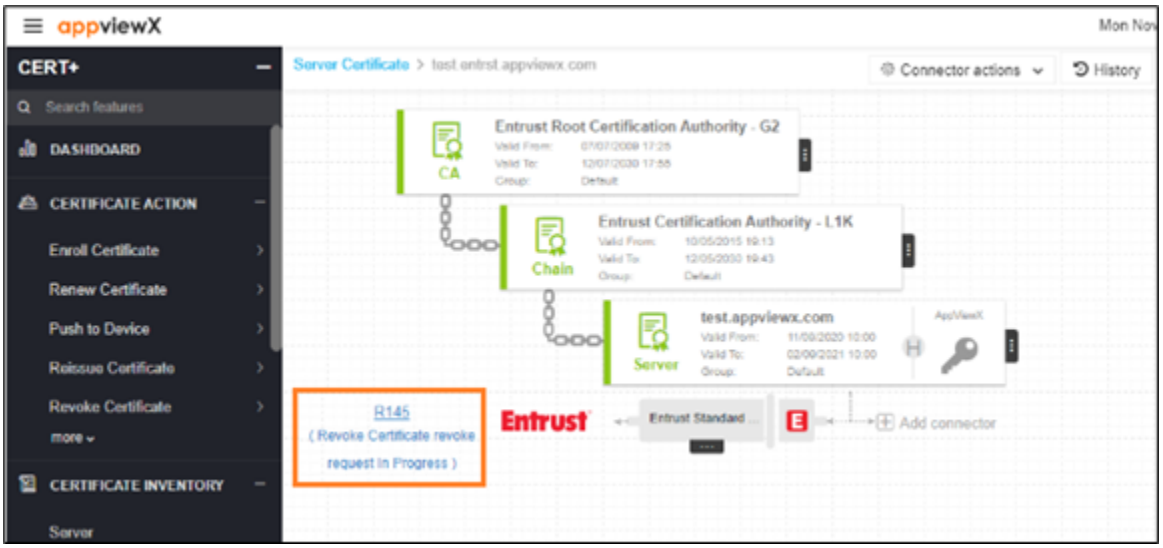


8. Click **Revoke** from the drop-down list.



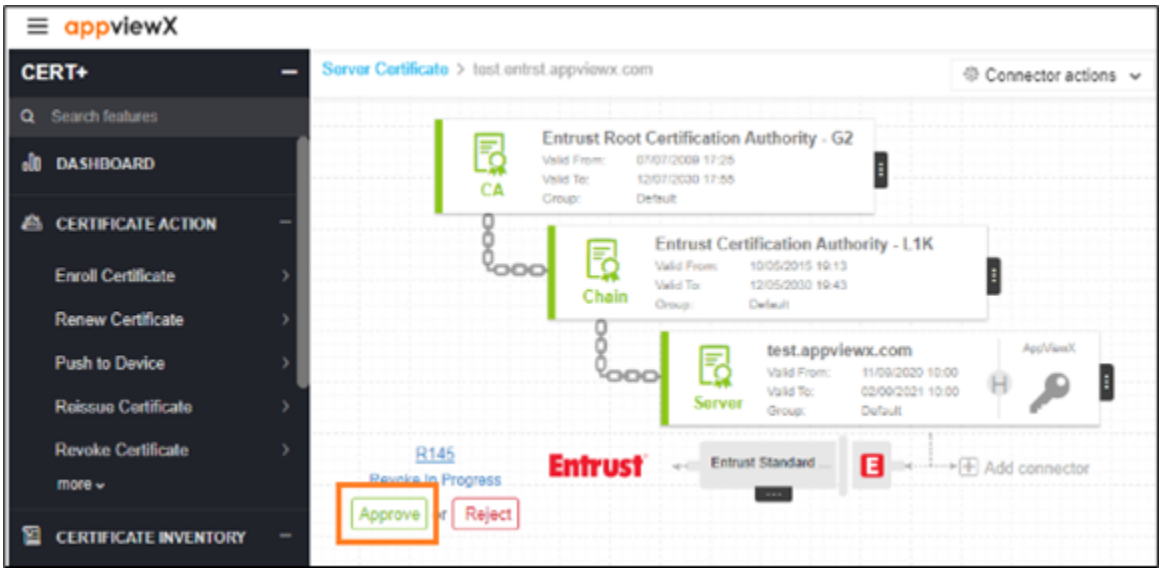
9. In the **Revoke** pop-up window, select **Reason** from the drop-down list and click **Yes** to proceed.

10. Revoke process is initiated.

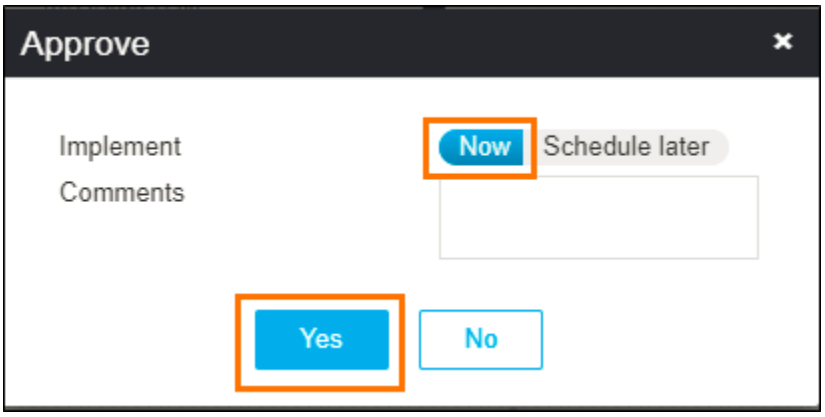


Note: If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

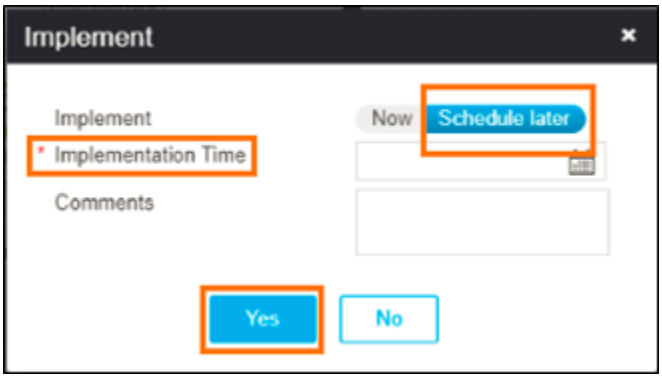
11. Click **Approve** button to proceed.



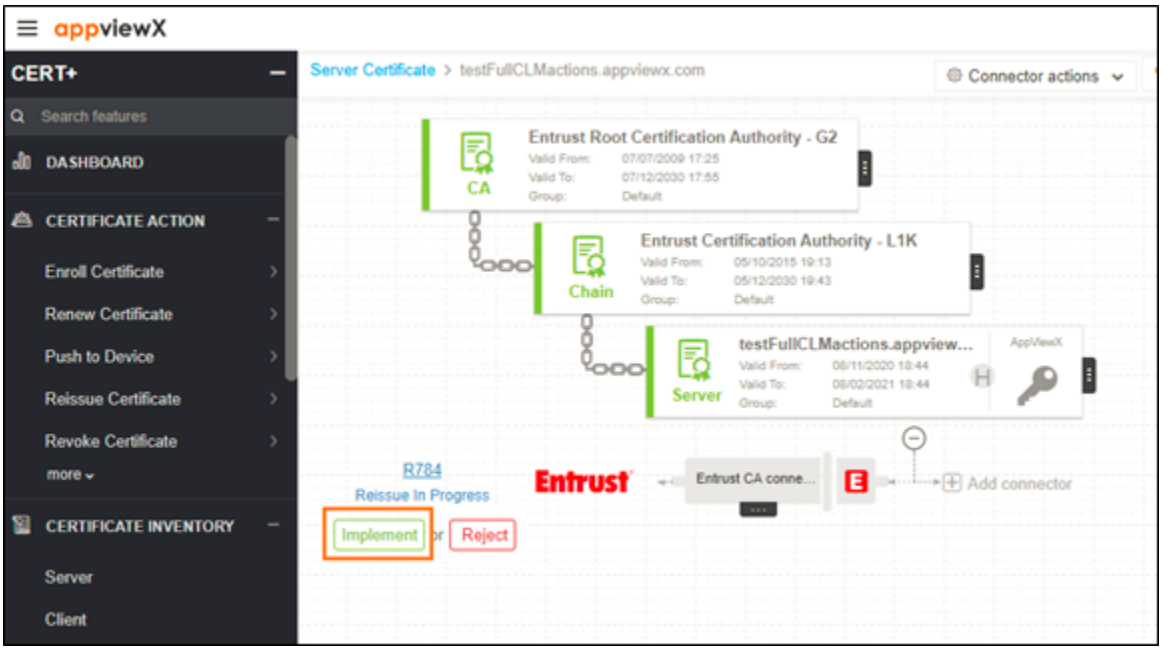
12. Click **Yes**.
13. In the **Approve** pop-up window, provide the **Comments.**



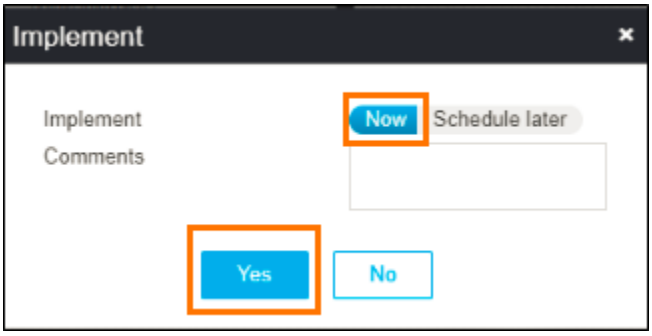
14. Click **Schedule later** if the workflow request has to be approved automatically in the future.



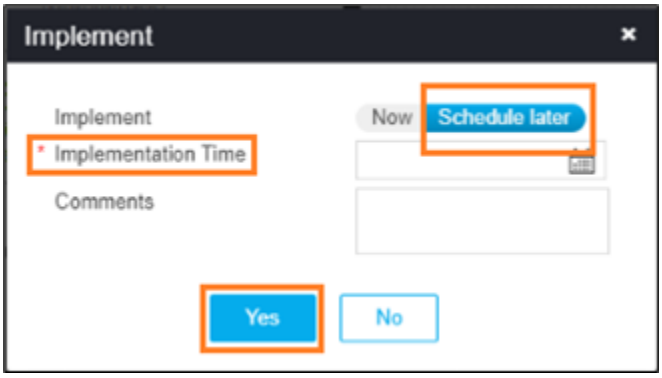
15. Click **Yes**.
16. Click the **Implement** button to proceed.



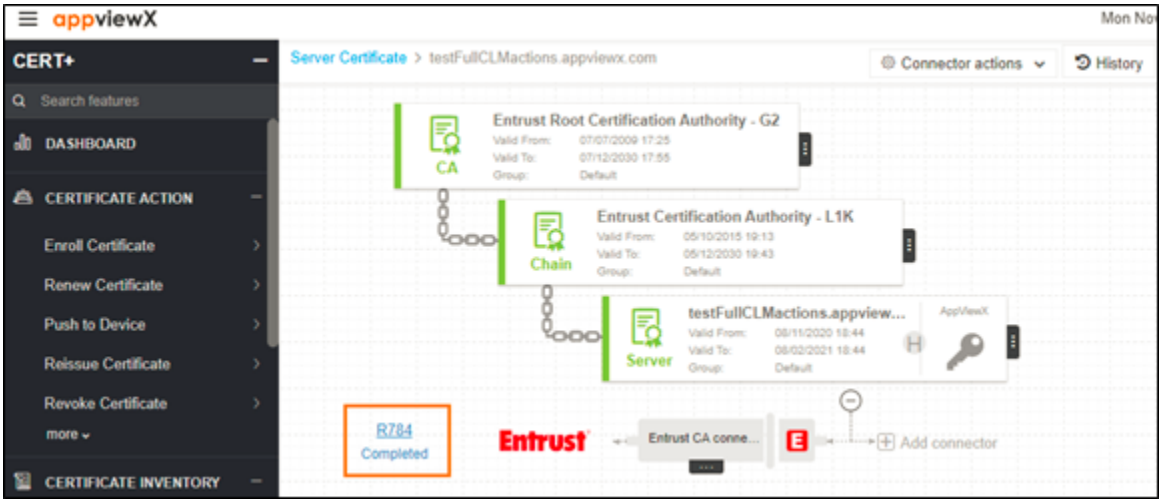
17. On the **Implement** pop-up, provide the **Comments.**



18. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



19. Click **Yes.**
20. After the revoke action is completed, the status updates to **Completed**.



Revoking Client Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

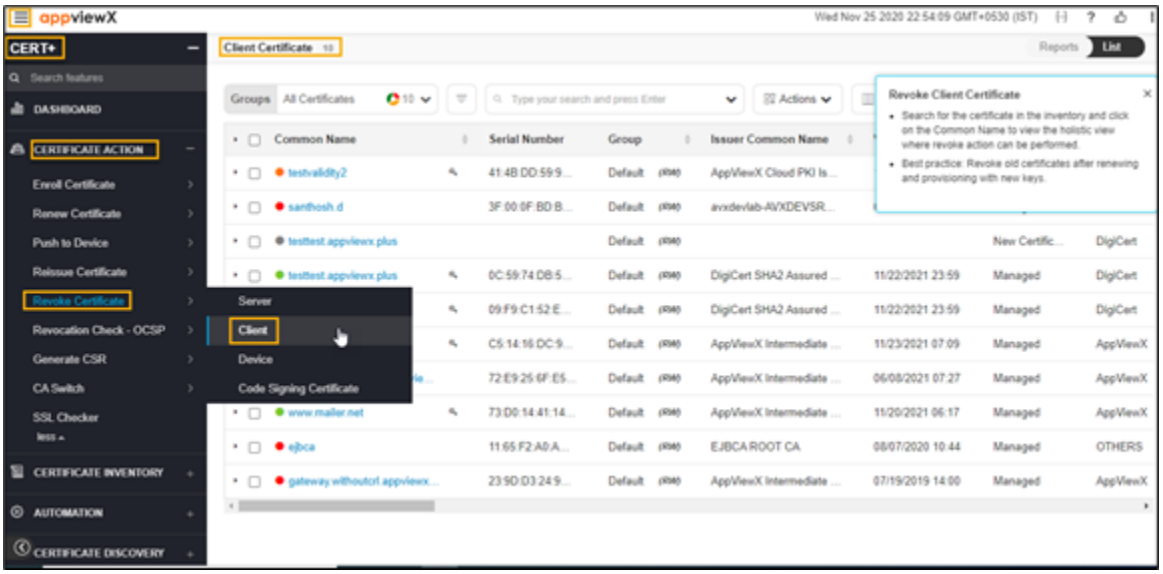
To revoke a client certificate:

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

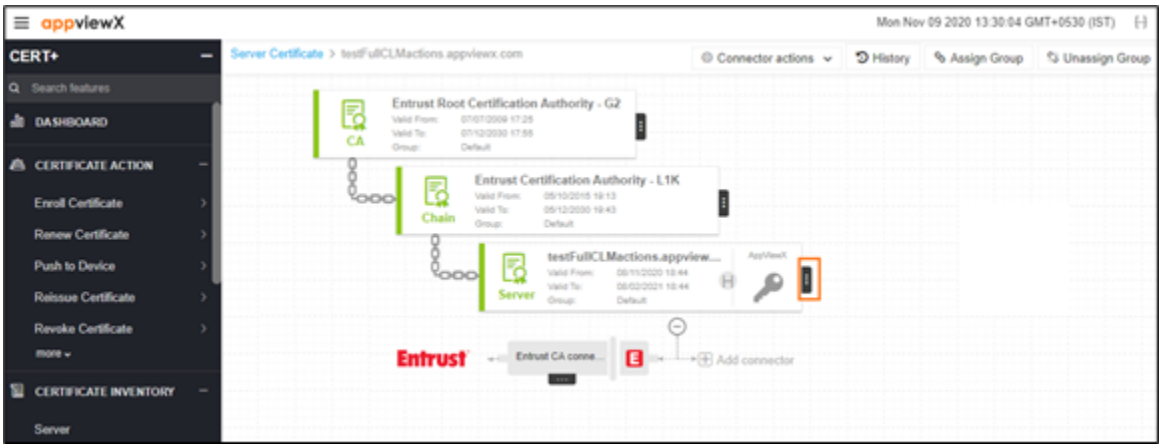
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Revoke Certificate**, and then **Client**.

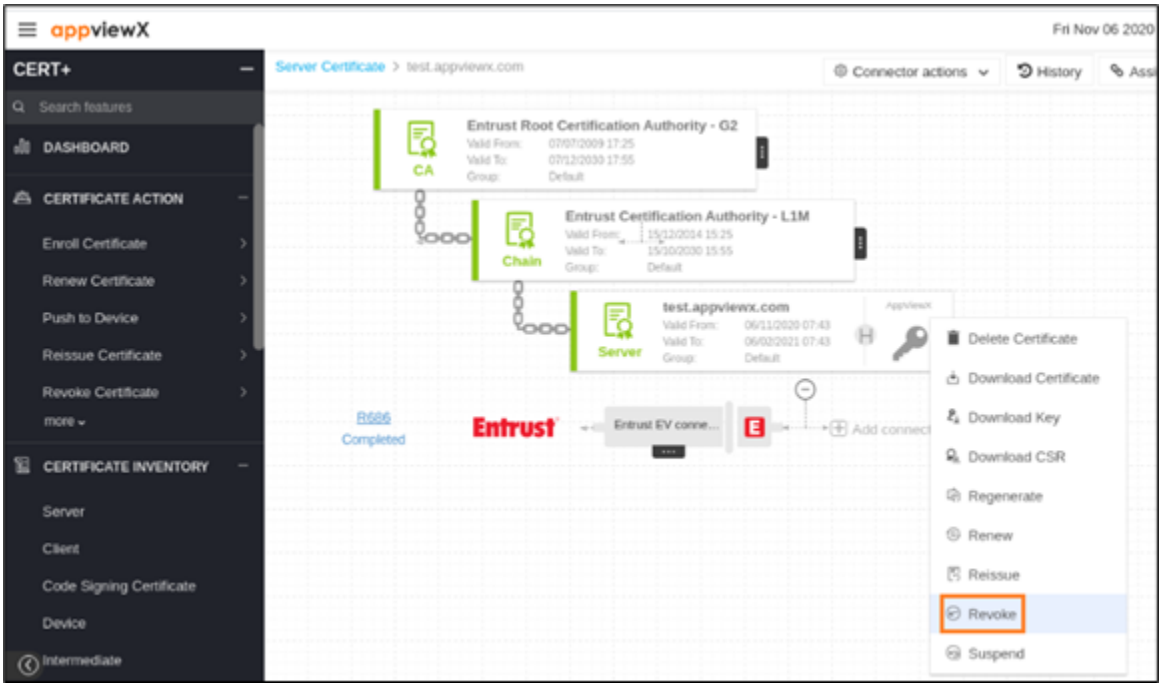
   The **Client Certificate** page appears.



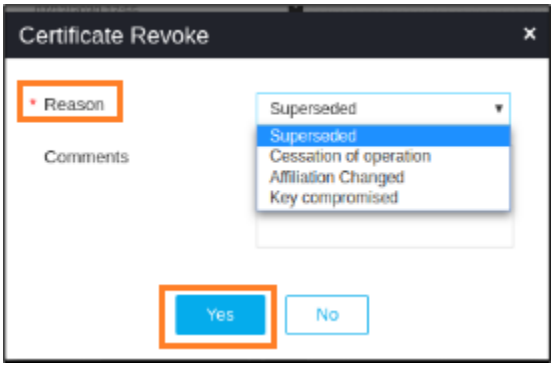
6. Click the **Common Name** of the certificate to navigate into the holistic view.
7. Hover over the vertical eclipse icon on the certificate.



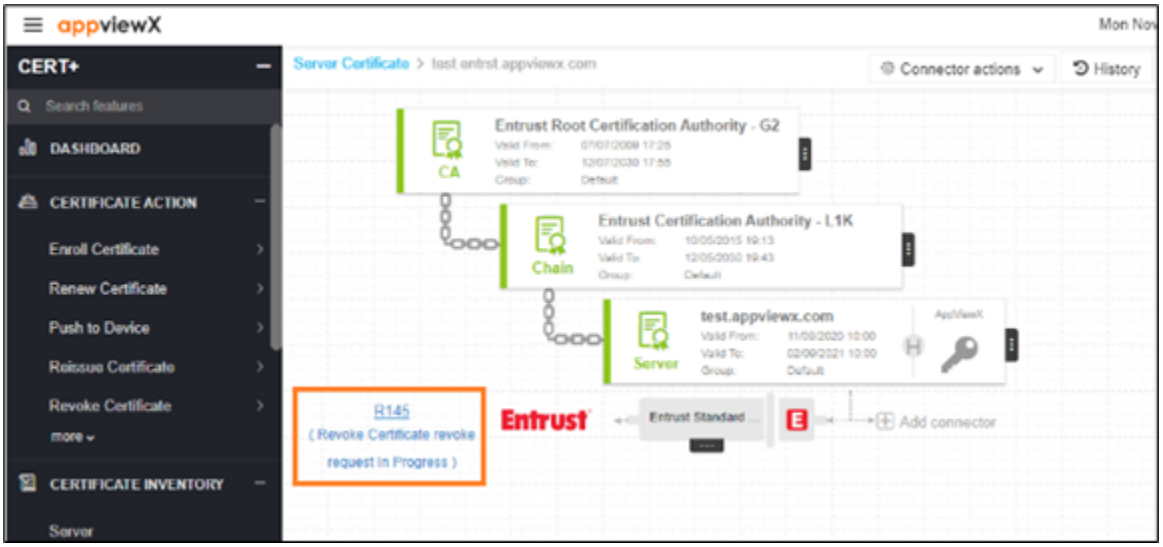
8. Click **Revoke** from the drop-down list.



9. In the **Revoke** pop-up window, select **Reason** from the drop-down list and click **Yes** to proceed.

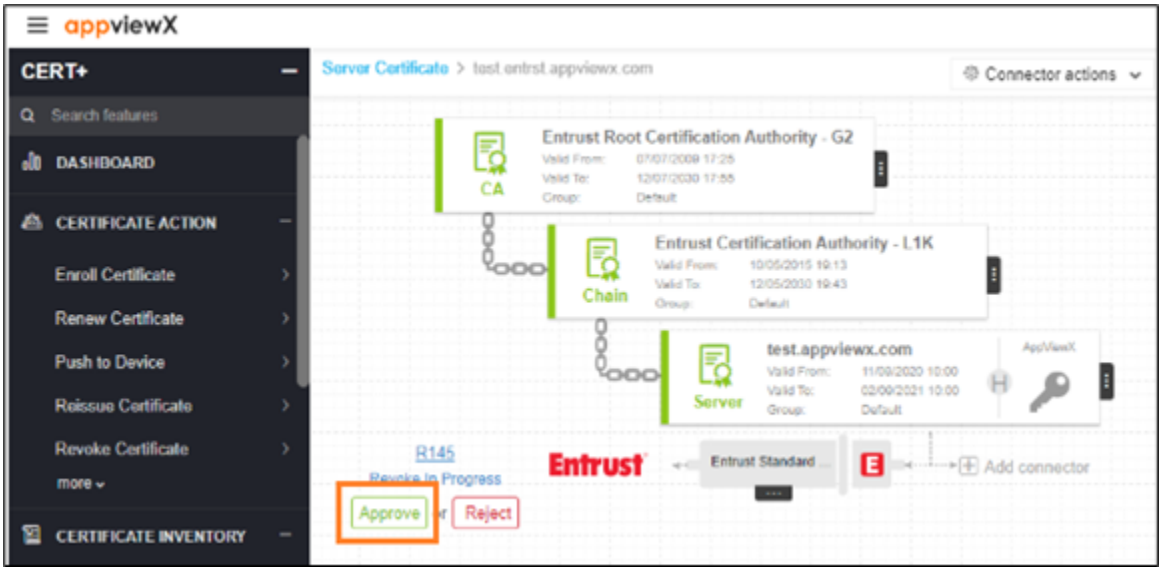


10. Revoke process is initiated.

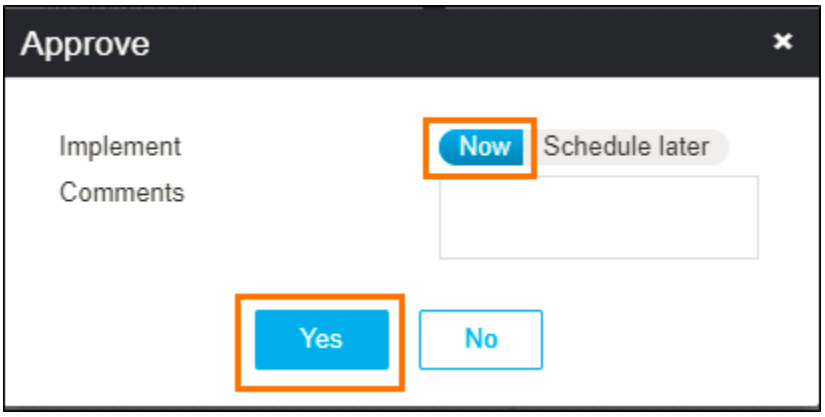


Note: If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

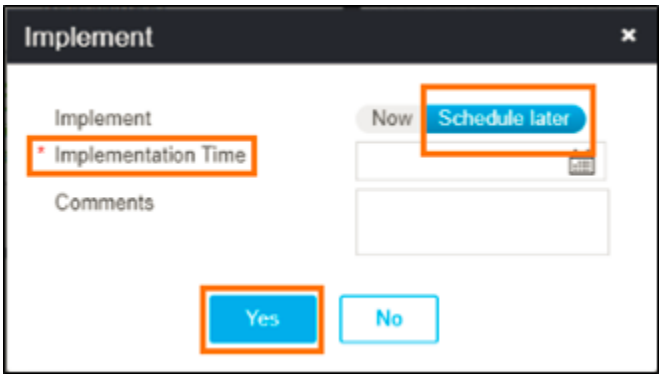
11. Click **Approve** button to proceed.



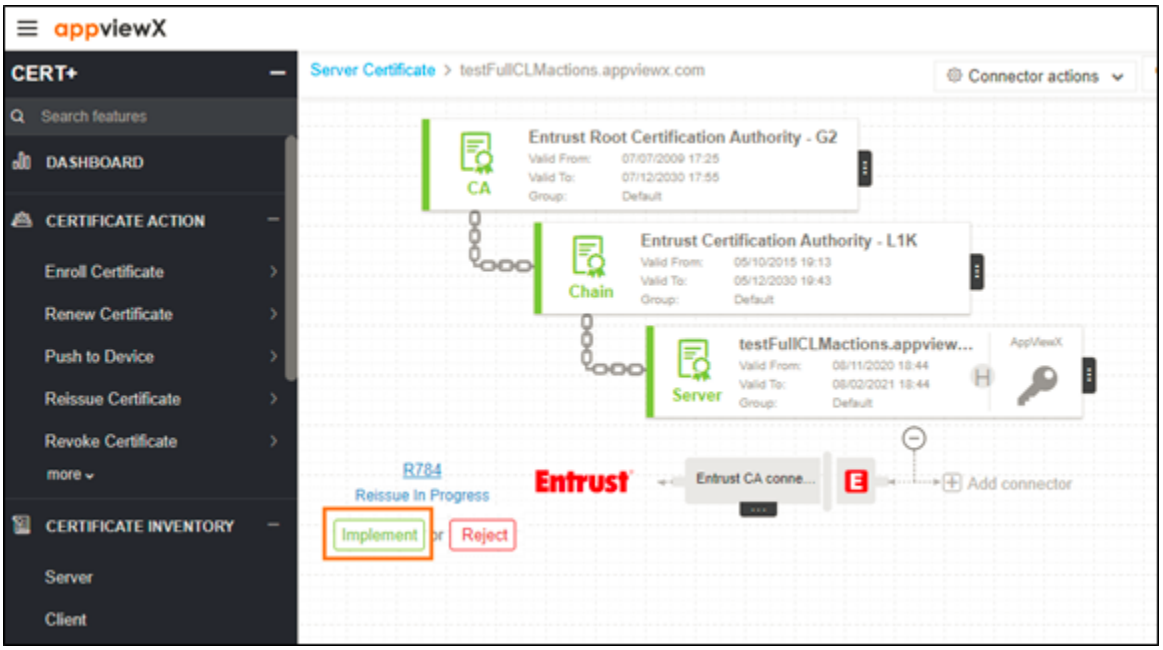
12. Click **Yes**.
13. In the **Approve** pop-up window, provide the **Comments.**



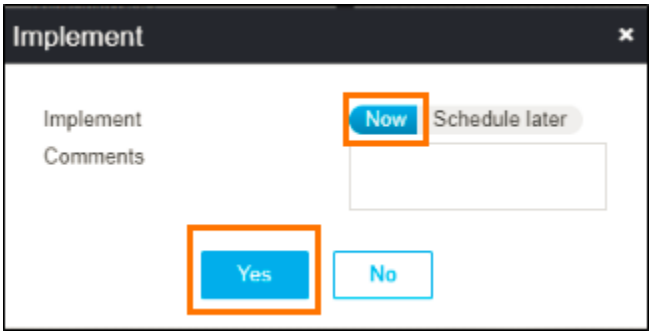
14. Click **Schedule later** if the workflow request has to be approved automatically in the future.



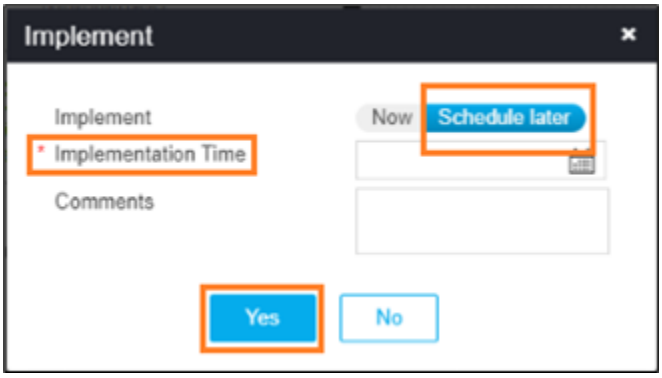
15. Click **Yes**.
16. Click the **Implement** button to proceed.



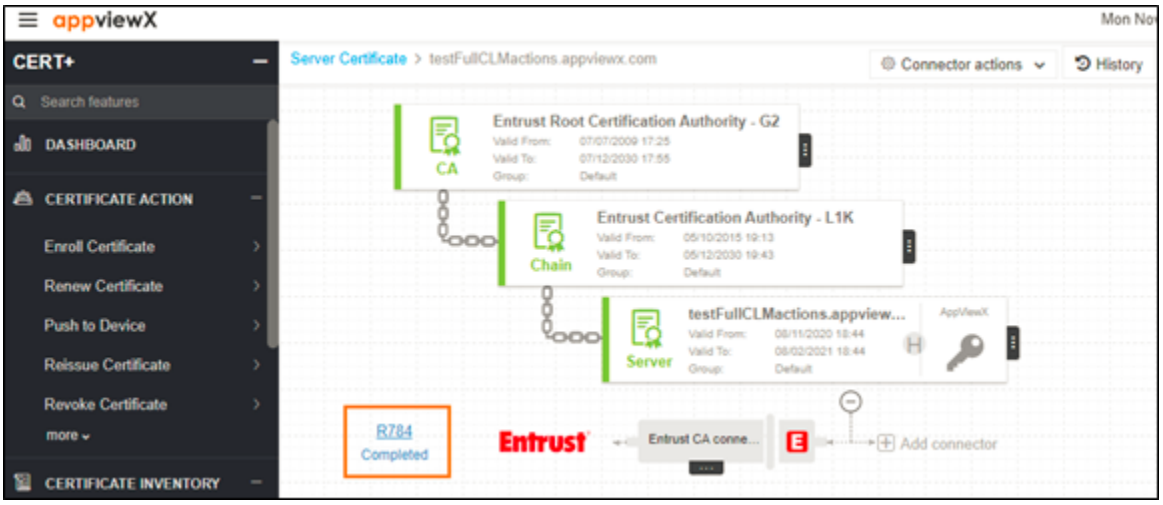
17. On the **Implement** pop-up, provide the **Comments.**



18. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



19. Click **Yes.**
20. After the revoke action is completed, the status updates to **Completed**.



Revoking Device Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

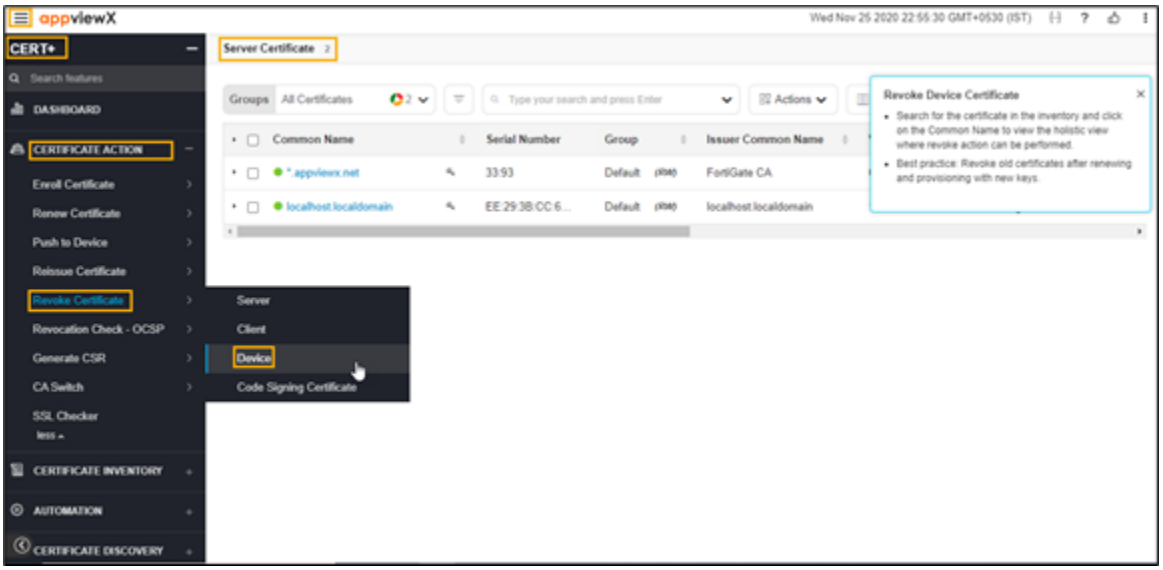
To revoke a device certificate,

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

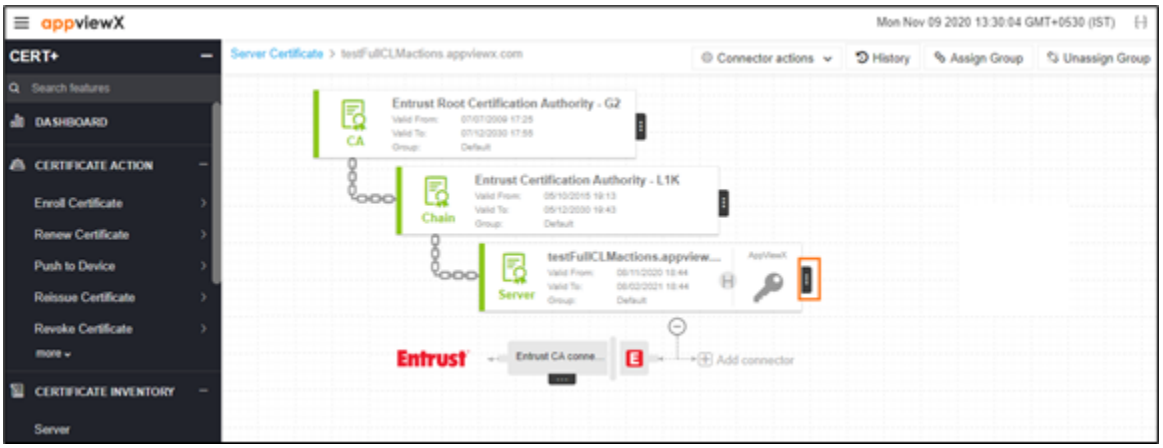
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Revoke Certificate**, and then **Device**.

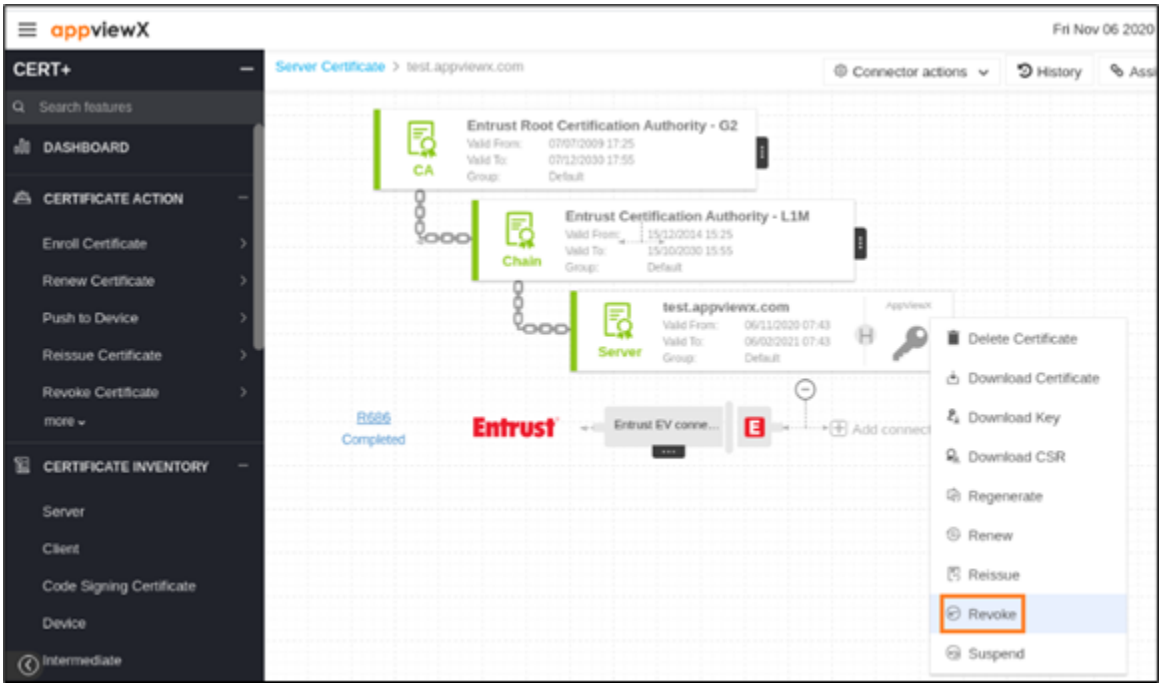
   The **Device Certificate** page appears.



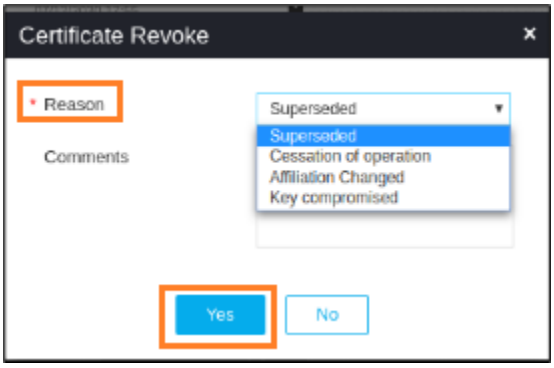
6. Click the **Common Name** of the certificate to navigate into the holistic view.
7. Hover over the vertical eclipse icon on the certificate.



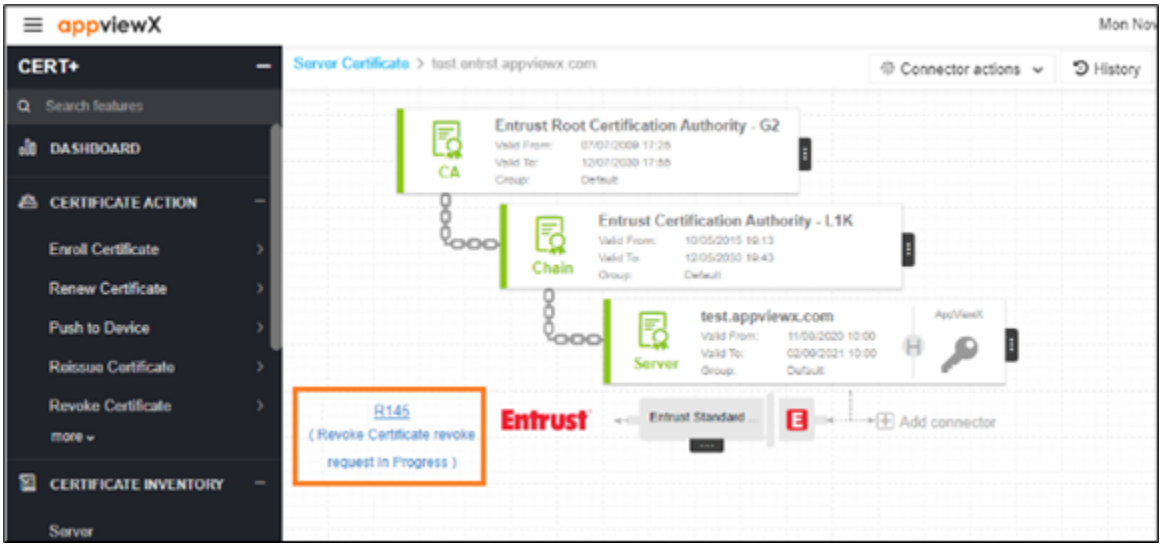
8. Click **Revoke** from the drop-down list.



9. In the **Revoke** pop-up window, select **Reason** from the drop-down list and click **Yes** to proceed.

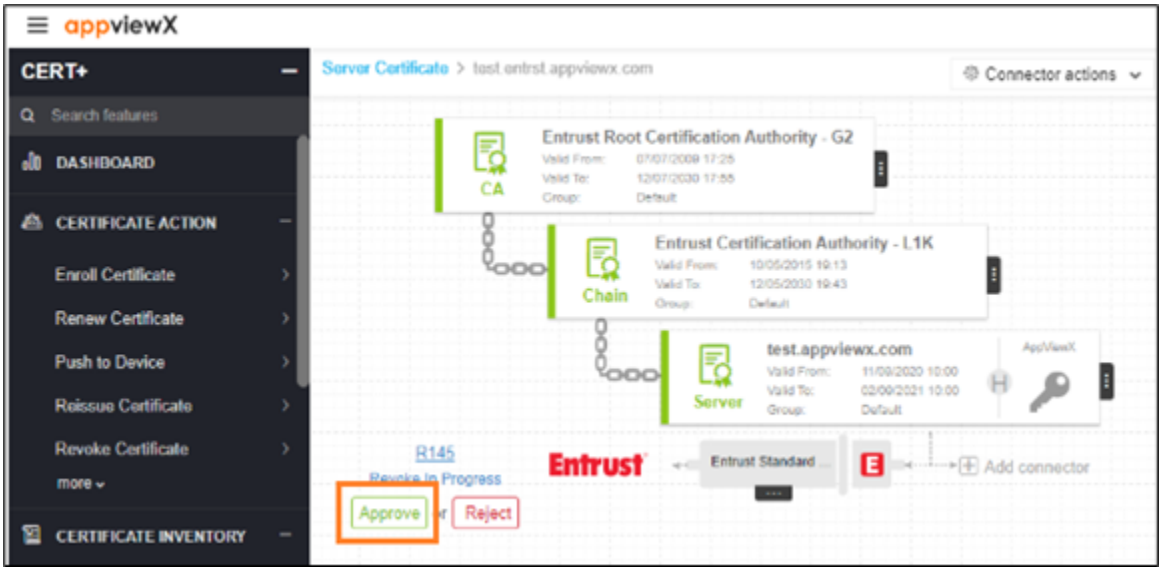


10. Revoke process is initiated.

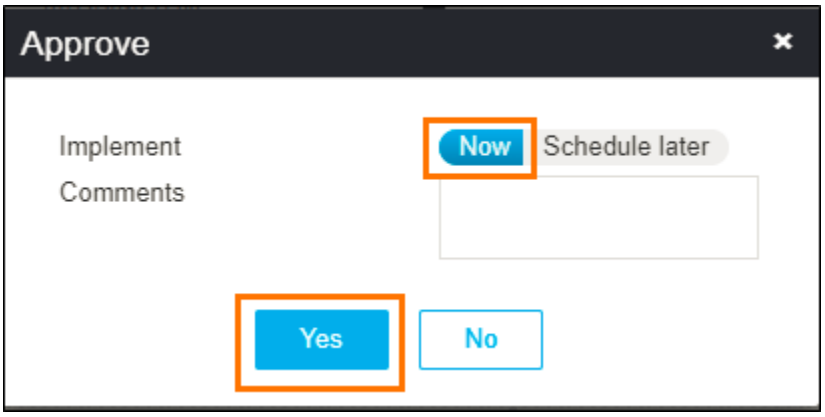


Note: If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

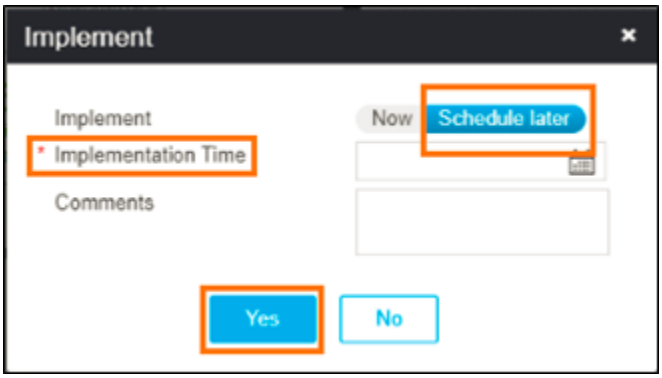
11. Click **Approve** button to proceed.



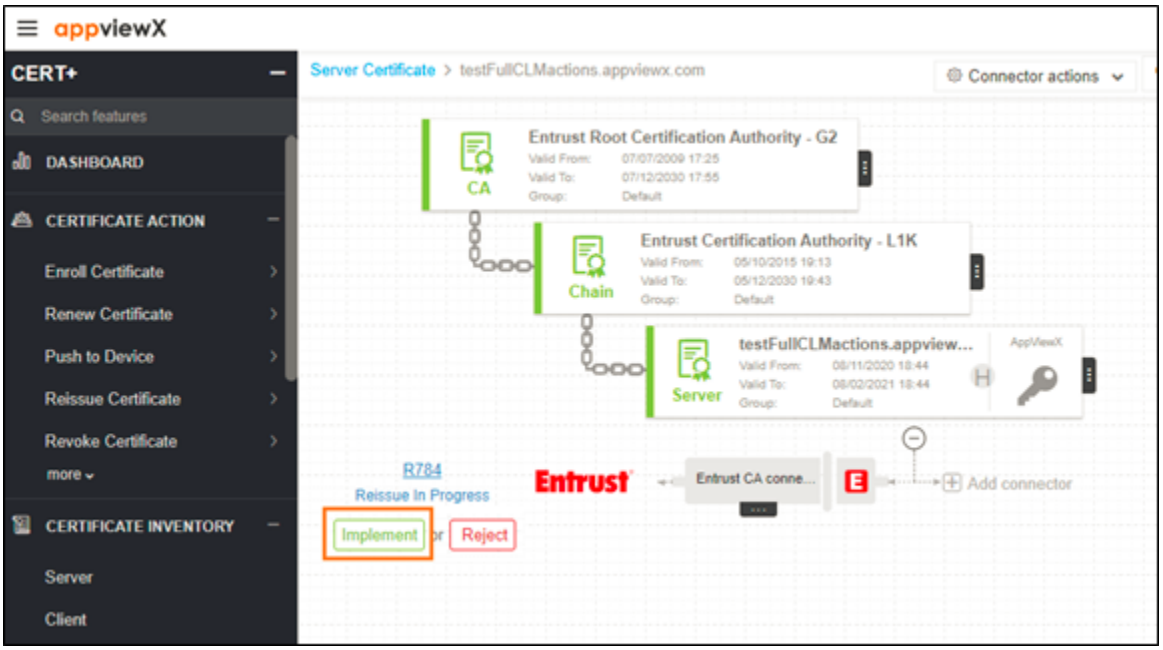
12. Click **Yes**.
13. In the **Approve** pop-up window, provide the **Comments.**



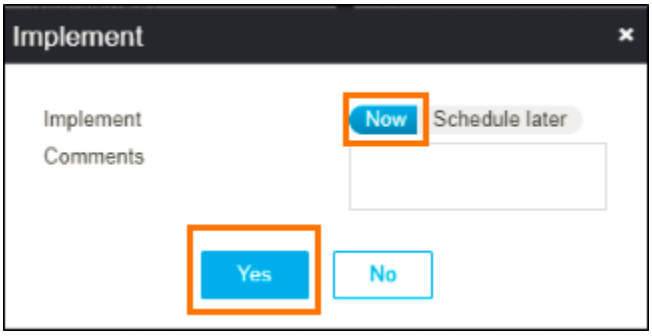
14. Click **Schedule later** if the workflow request has to be approved automatically in the future.



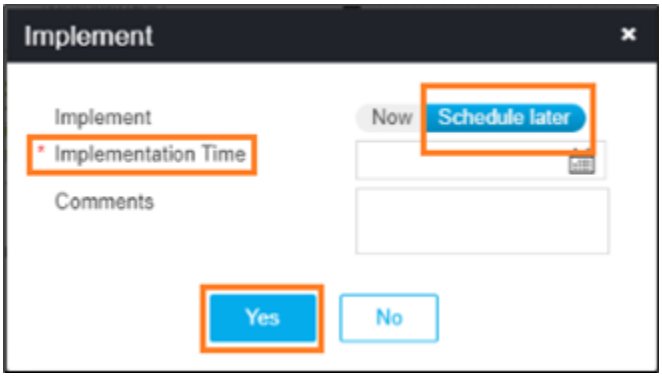
15. Click **Yes**.
16. Click the **Implement** button to proceed.



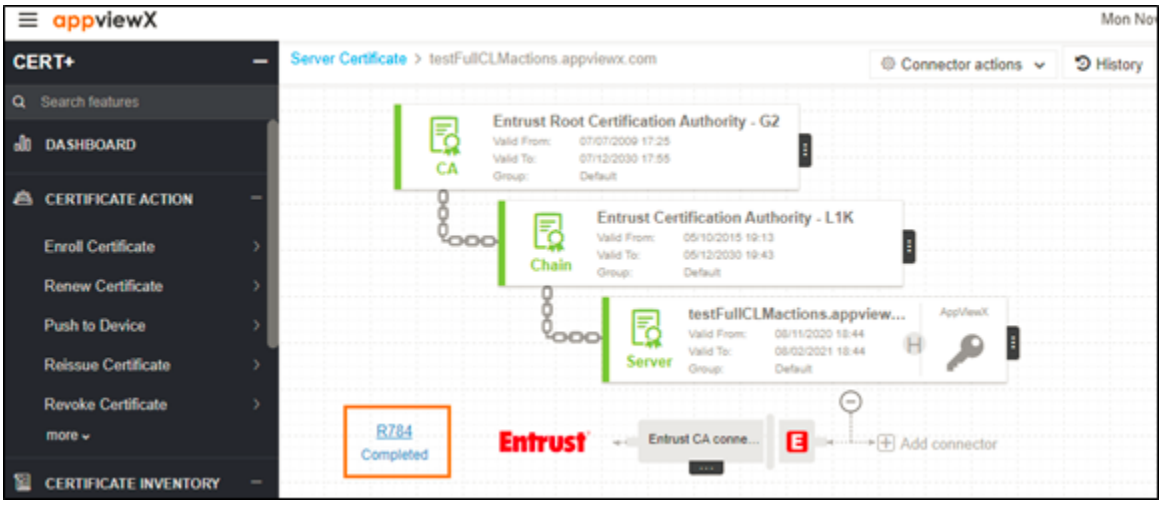
17. On the **Implement** pop-up, provide the **Comments.**



18. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



19. Click **Yes.**
20. After the revoke action is completed, the status updates to **Completed**.



Revoking Code Signing Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

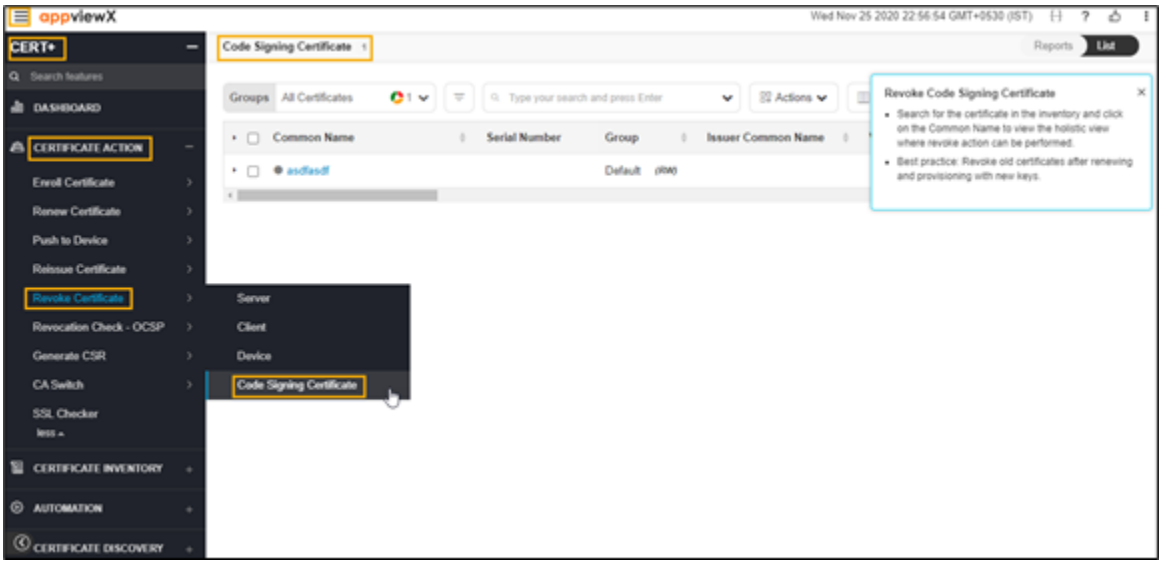
To revoke a code signing certificate:

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

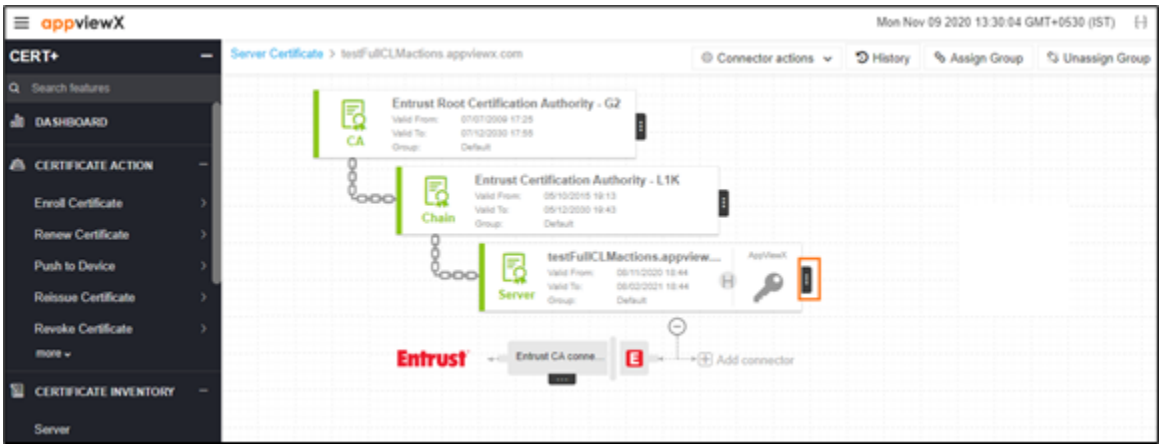
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Revoke Certificate**, and then **Code Signing Certificate**.

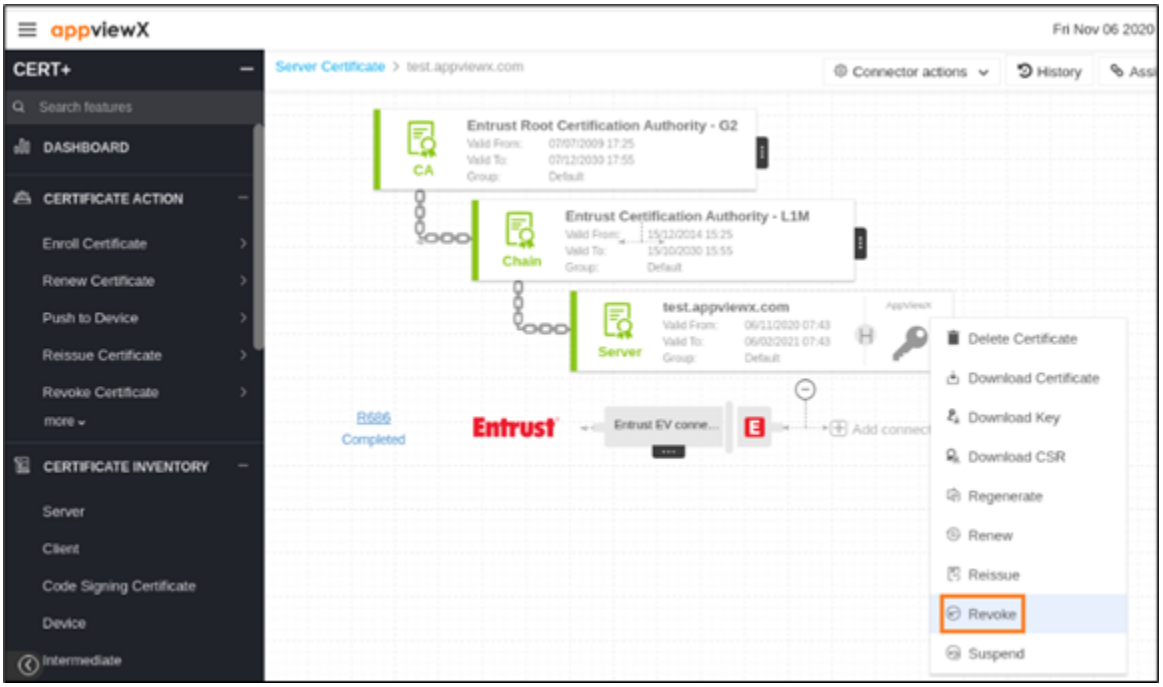
   The **Code Signing Certificate** page appears.



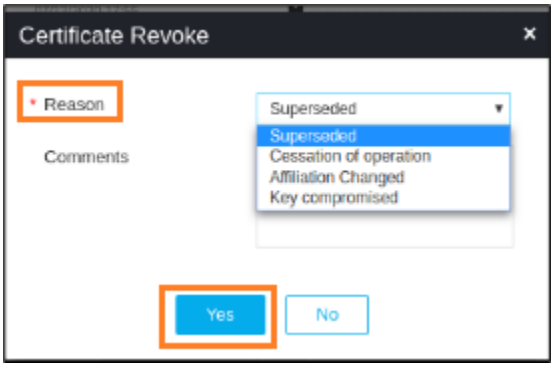
6. Click the **Common Name** of the certificate to navigate into the holistic view.
7. Hover over the vertical eclipse icon on the certificate.



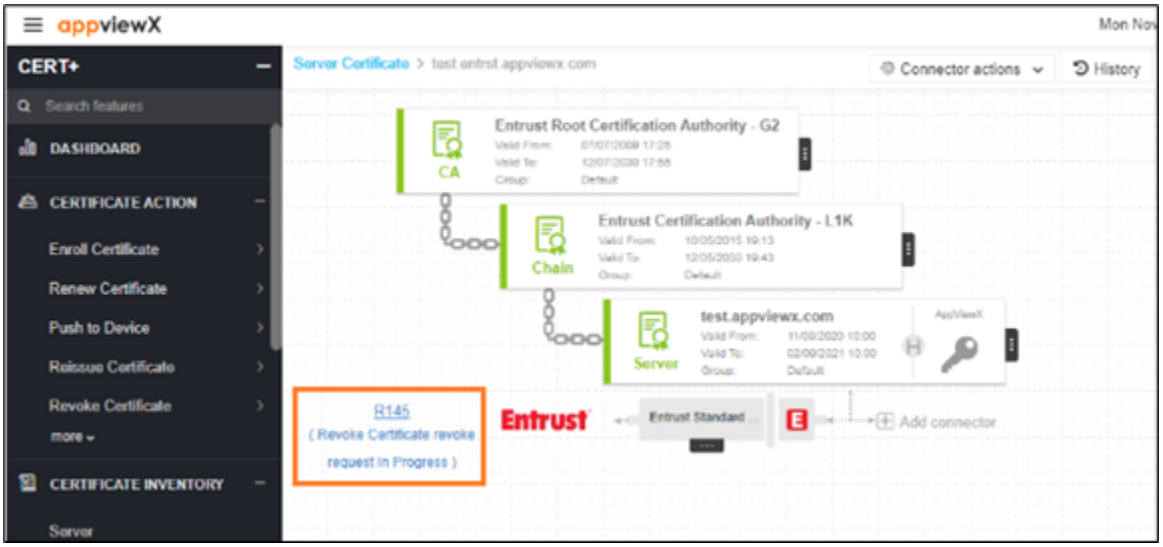
8. Click **Revoke** from the drop-down list.



9. In the **Revoke** pop-up window, select **Reason** from the drop-down list and click **Yes** to proceed.

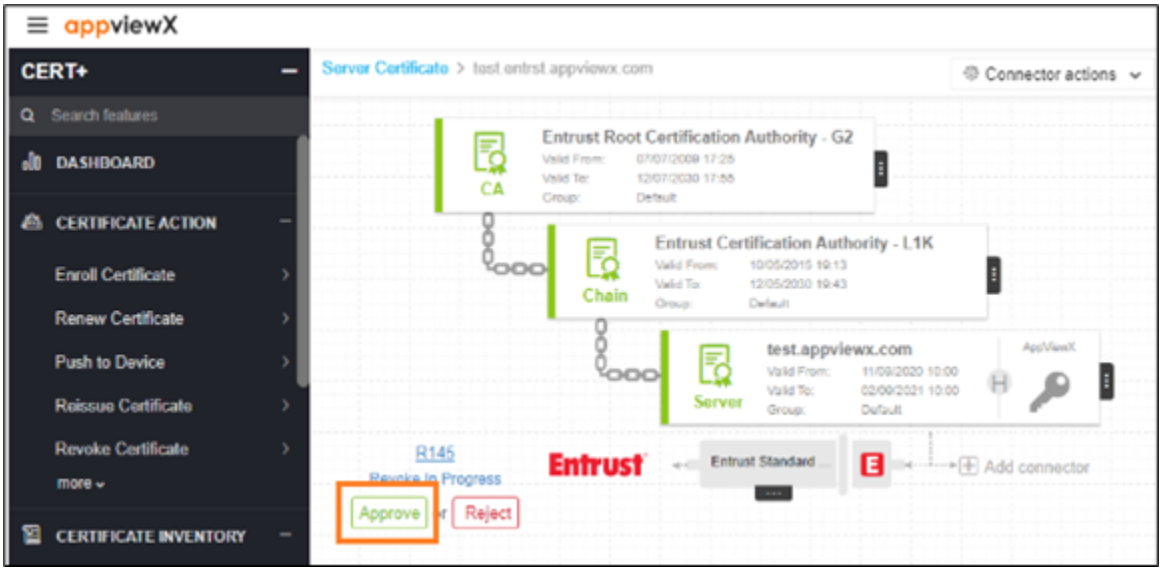


10. Revoke process is initiated.

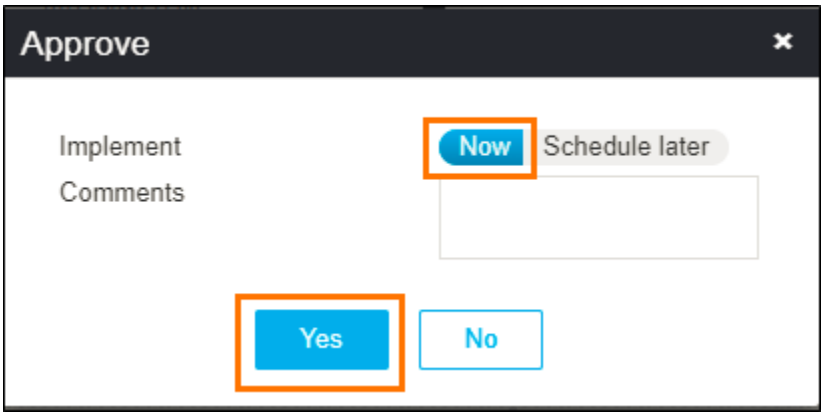


Note: If an Approval Required checkbox is enabled on the Certificate Policy page, the request goes to Approve and Implementation stages.

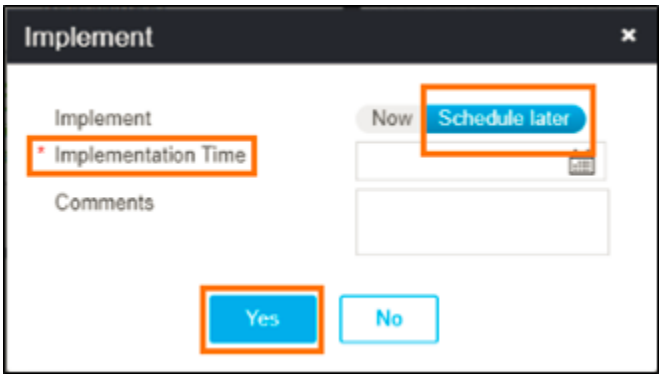
11. Click **Approve** button to proceed.



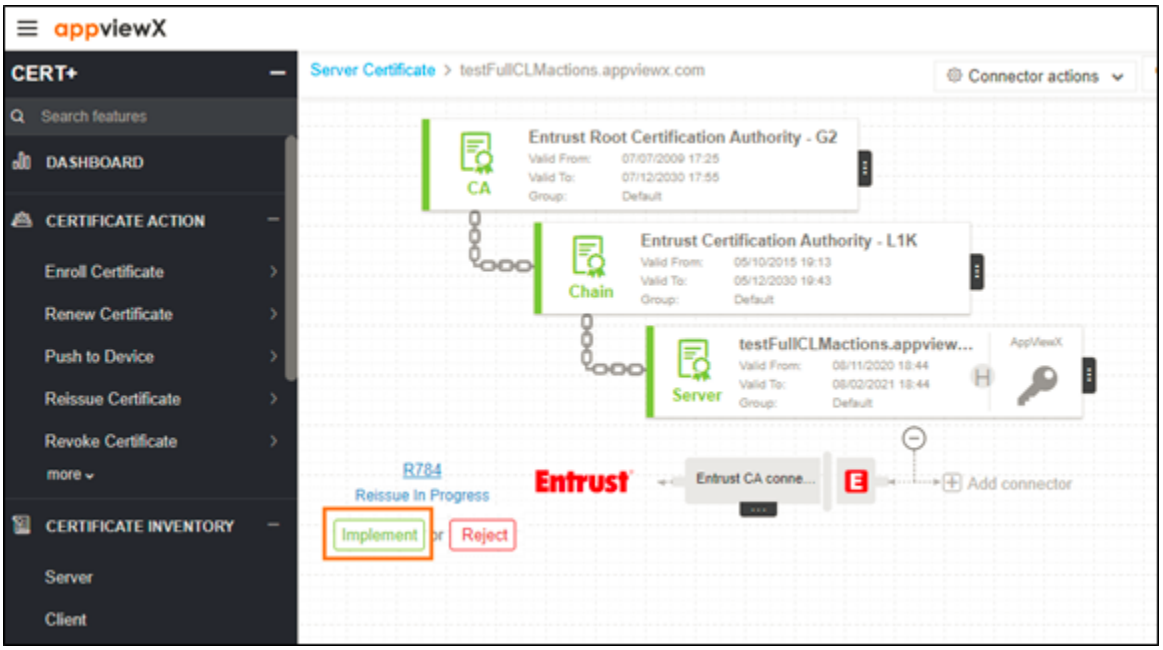
12. Click **Yes**.
13. In the **Approve** pop-up window, provide the **Comments.**



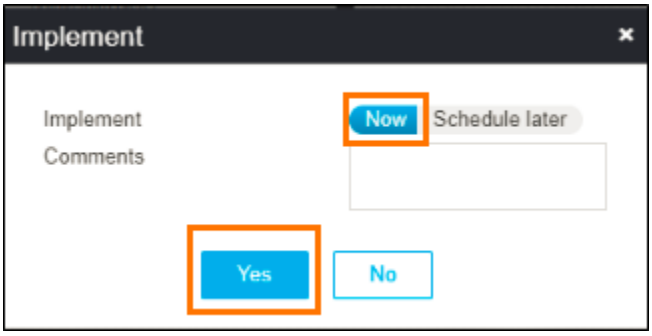
14. Click **Schedule later** if the workflow request has to be approved automatically in the future.



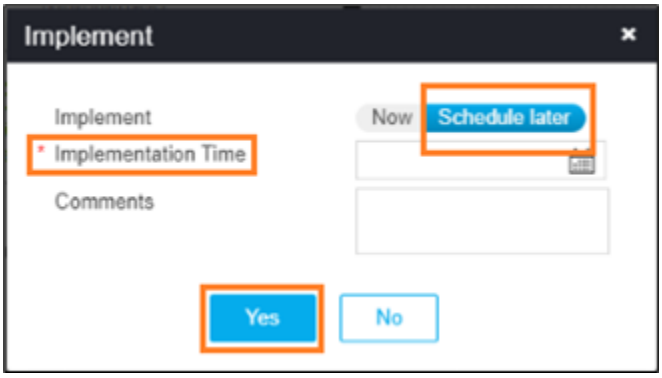
15. Click **Yes**.
16. Click the **Implement** button to proceed.



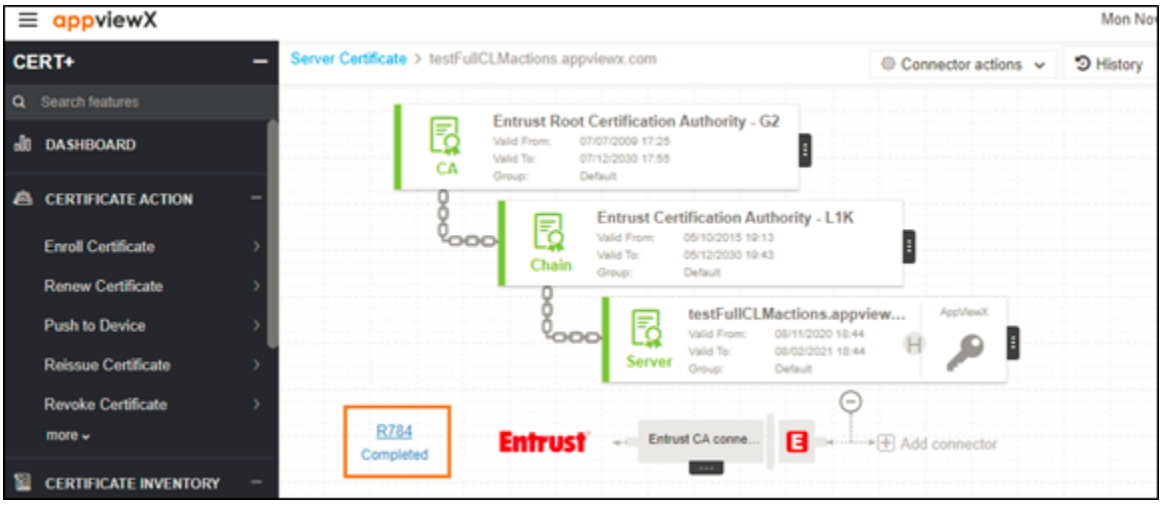
17. On the **Implement** pop-up, provide the **Comments.**



18. Click **Schedule later** if the workflow request has to be implemented automatically in the future.



19. Click **Yes.**
20. After the revoke action is completed, the status updates to **Completed**.



Regenerating Certificate

Overview

The regenerate allows you to create a new certificate with the same parameters as an existing certificate. Regenerate will be a new order to the Certificate authority. This will come in handy if the user wants to switch the CA for the respective certificate.

Regenerating Server Certificate

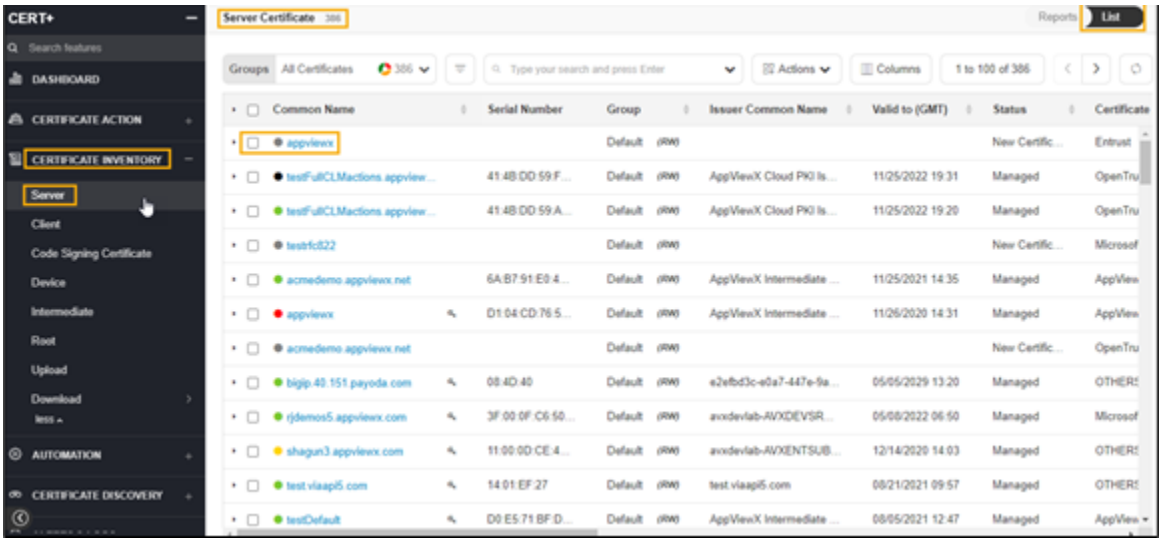
To regenerate a server certificate,

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. Click **Server**.

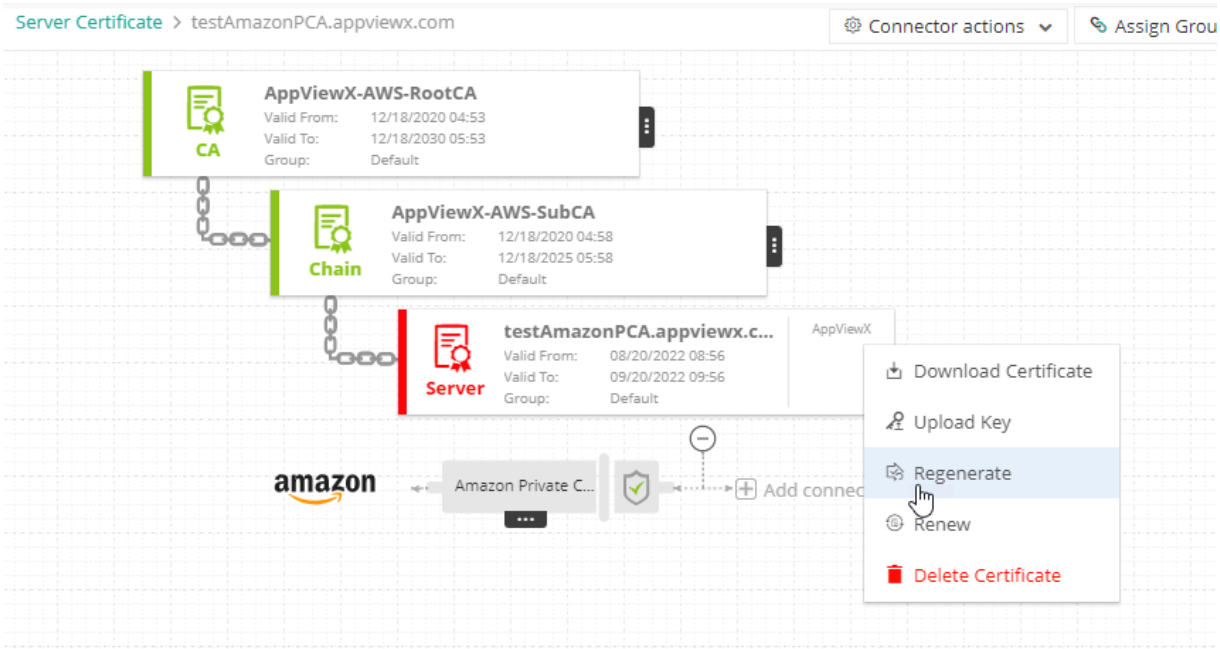
   The **Server Certificate** page appears.



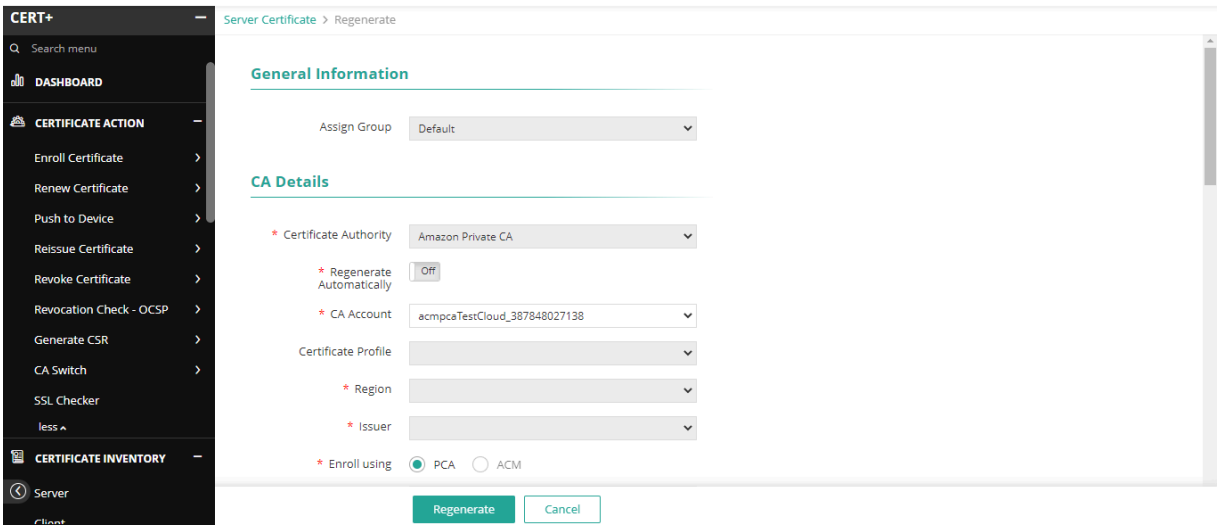
6. In the **Common Name** column certificate list, select the desired certificate that you want to regenerate a certificate.

   The holistic view page appears.

7. Click the vertical eclipsis icon, and then select **Regenerate** from the list.



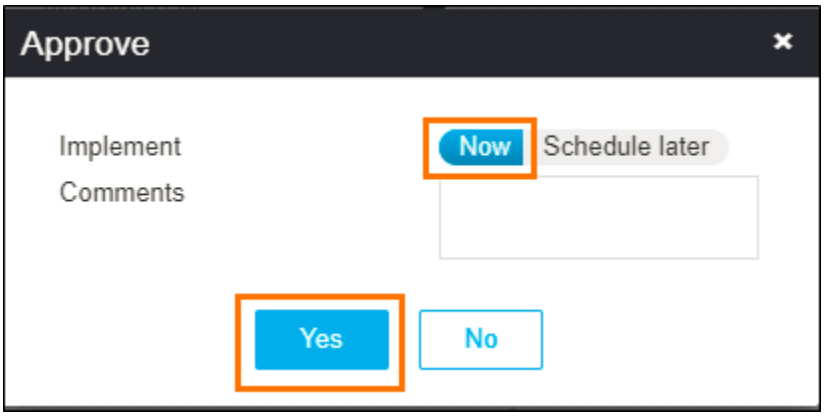
The **Server Certificate > Regenerate** page is displayed.



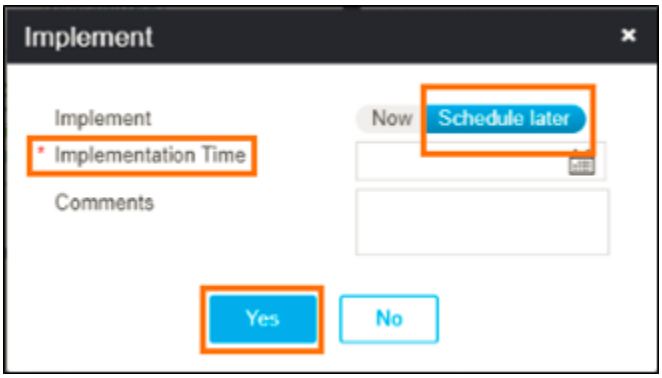
8. On the **Server Certificate > Regenerate** page, modify the required details under the **General Information, CA Details, CSR Parameters, Attachments, Generic Fields, Vendor-Specific Details,** and **Custom Attributes** sections, as explained in the **Enrolling a Server Cetrificate** section.
9. Click **Regenerate**.

   The regenerate process is initiated and you will be navigated back to the holistic view.
10. Click **Approve** to proceed.

    The **Approve** pop-up window appears.

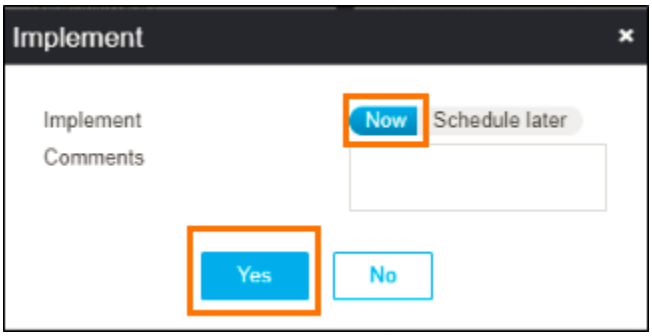


11. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.

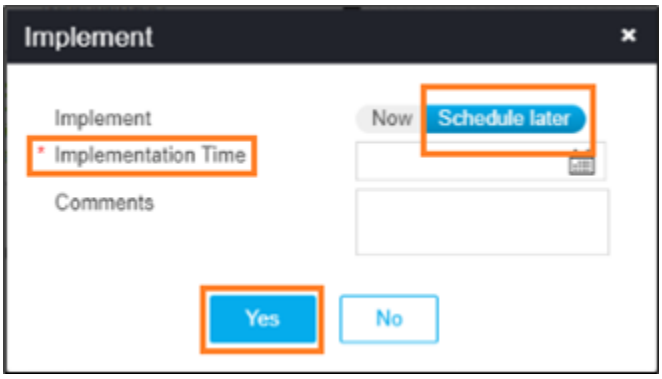


12. Select the **Implementation Time** from the calendar field.
13. Enter the comments in the field.
14. Click **Yes**.
15. The approval process is initiated and you are redirected to the holistic view.
16. Click **Implement**.

    The **Implement** pop-up window appears.



17. Click the **Schedule later** button if the workflow request has to be implemented automatically in future.



18. Select the **Implementation Time** from the calendar field.
19. Enter the comments in the field.
20. Click **Yes**.
21. After the regenerate action is completed, the status updates to **Completed**.

Regenerating Client Certificate

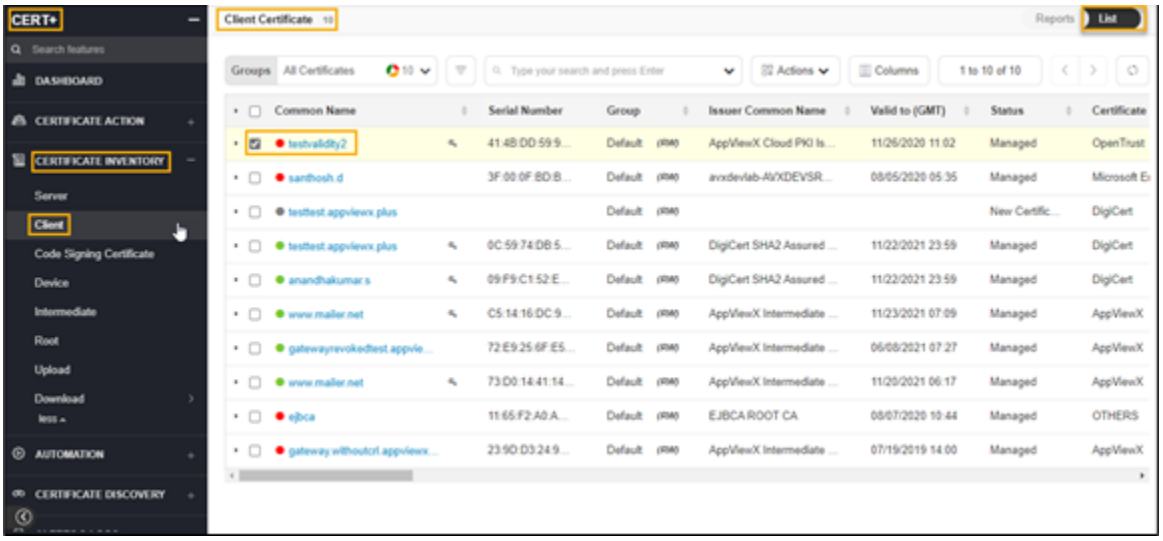
To regenerate a client certificate,

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. Click **Client**.

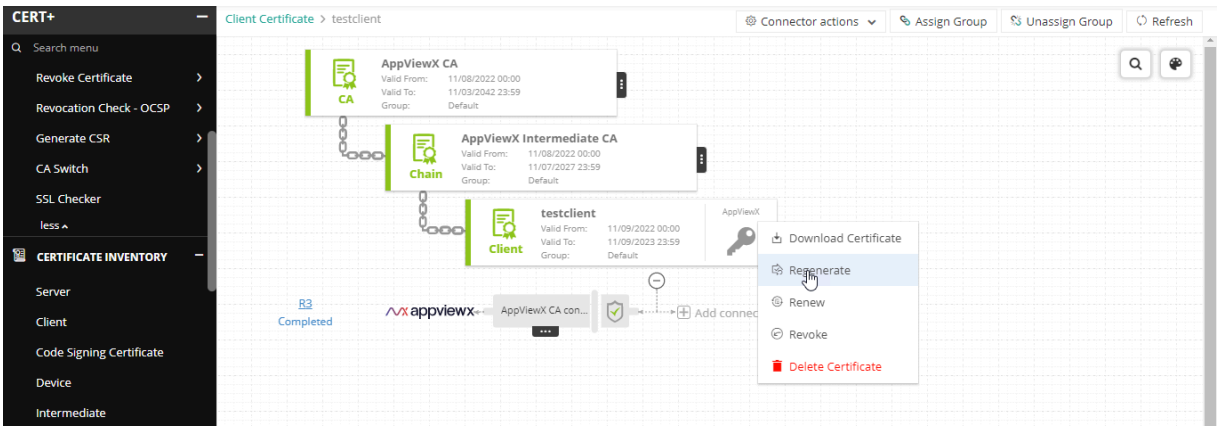
   The **Client Certificate** page appears.



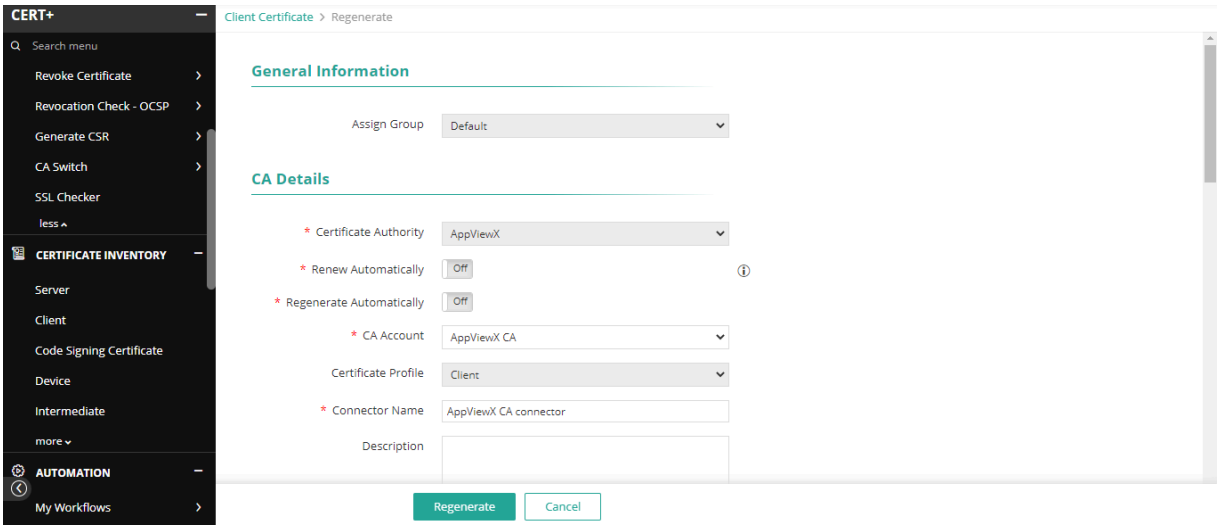
6. In the **Common Name** column certificate list, select the desired certificate that you want to regenerate a certificate.

   The holistic view page appears.

7. Click the vertical eclipsis icon, and then select **Regenerate** from the list.



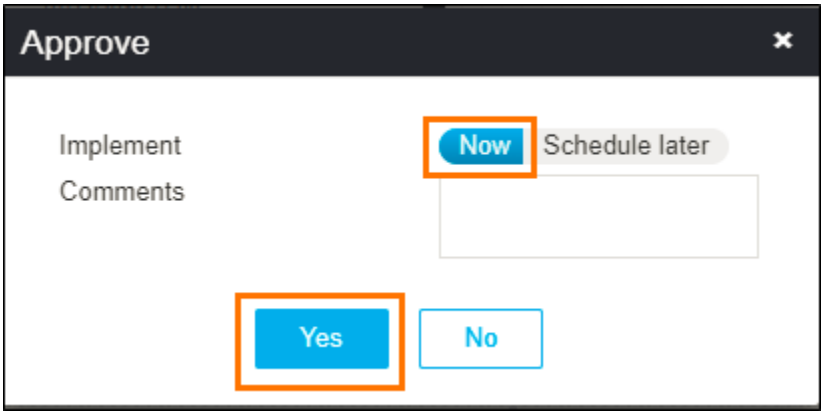
   The **Client Certificate > Regenerate** page is displayed.



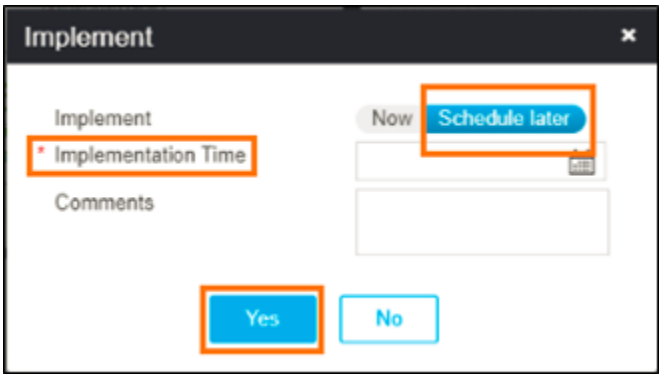
8. On the **Server Certificate > Regenerate** page, modify the required details under the **General Information, CA Details, CSR Parameters, Attachments, Generic Fields, Vendor-Specific Details,** and **Custom Attributes** sections, as explained in the **Enrolling a Client Certificate** section.
9. Click **Regenerate**.

   The regenerate process is initiated and you are redirected to the holistic view.
10. Click **Approve** to proceed.

    The **Approve** pop-up window appears.



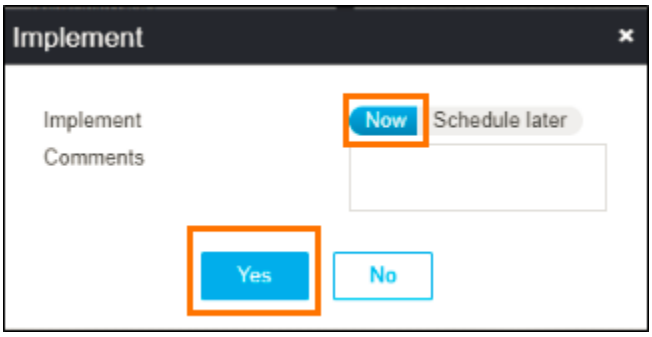
11. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.



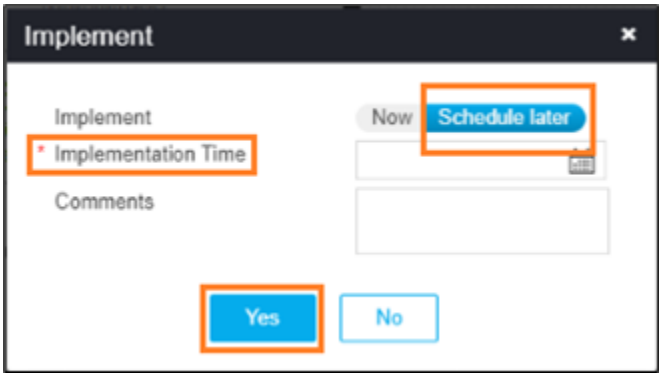
12. Select the **Implementation Time** from the calendar field.
13. Enter the comments in the field.
14. Click **Yes**.

    The approval process is initiated and you are redirected to the holistic view.
15. Click **Implement**.

    The **Implement** pop-up window appears.



16. Click the **Schedule later** button if the workflow request has to be implemented automatically in future.



17. Select the **Implementation Time** from the calendar field.
18. Enter the comments in the field.

19. Click **Yes**.
20. After the regenerate action is completed, the status updates to **Completed**.

Regenerating Code Signing Certificate

To regenerate a code signing certificate,

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

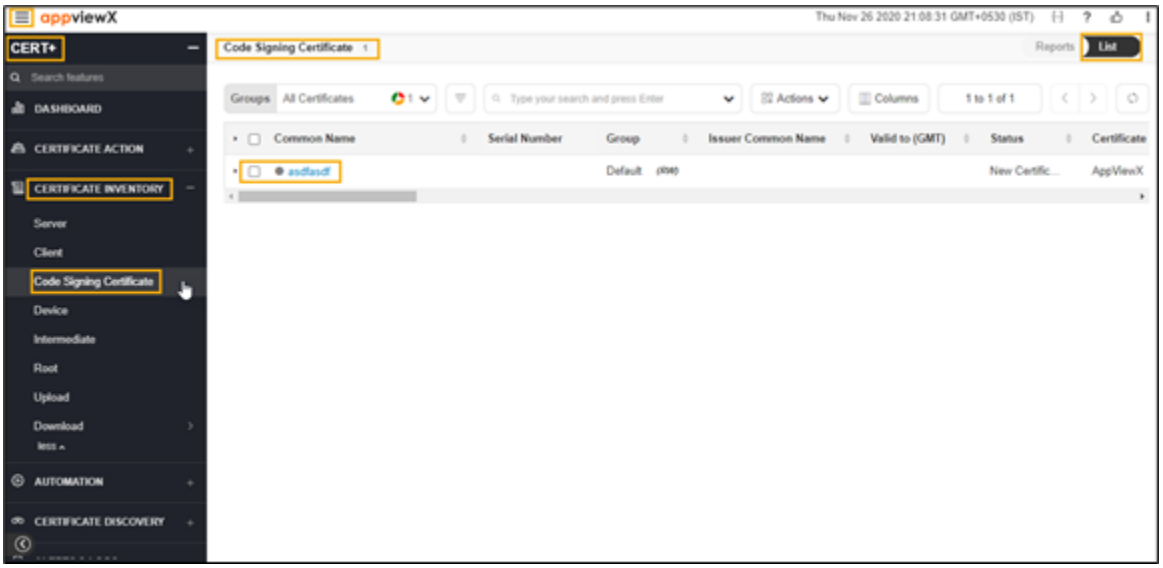
   The left navigation pane appears.

3. Click **CERT+**.

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

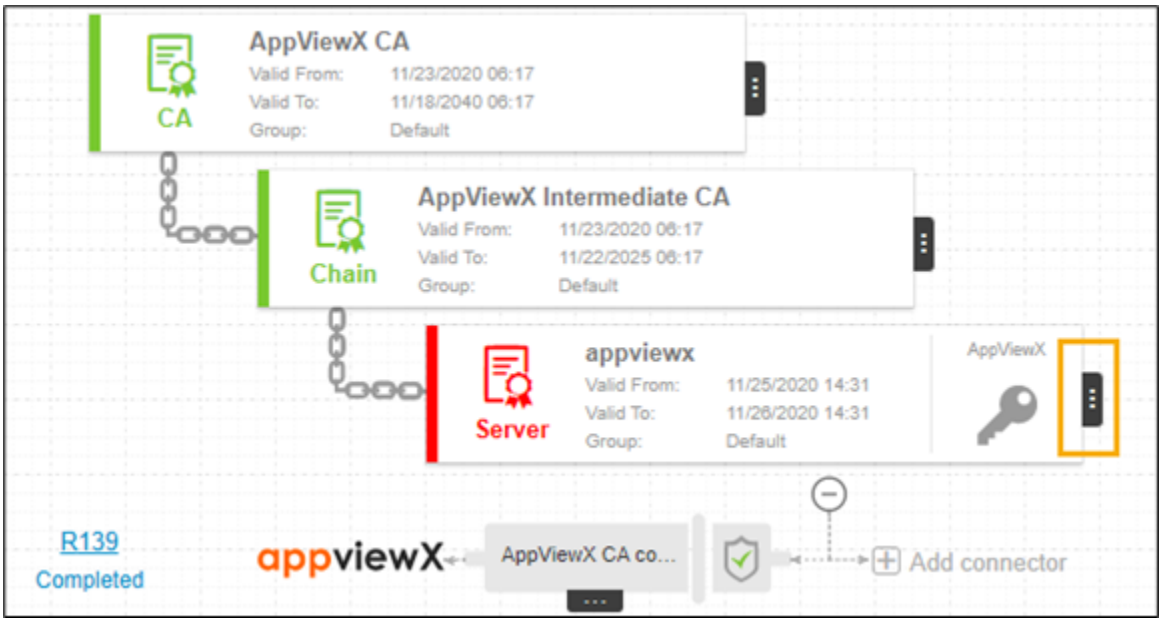
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.

   The **Code Signing Certificate** page appears.

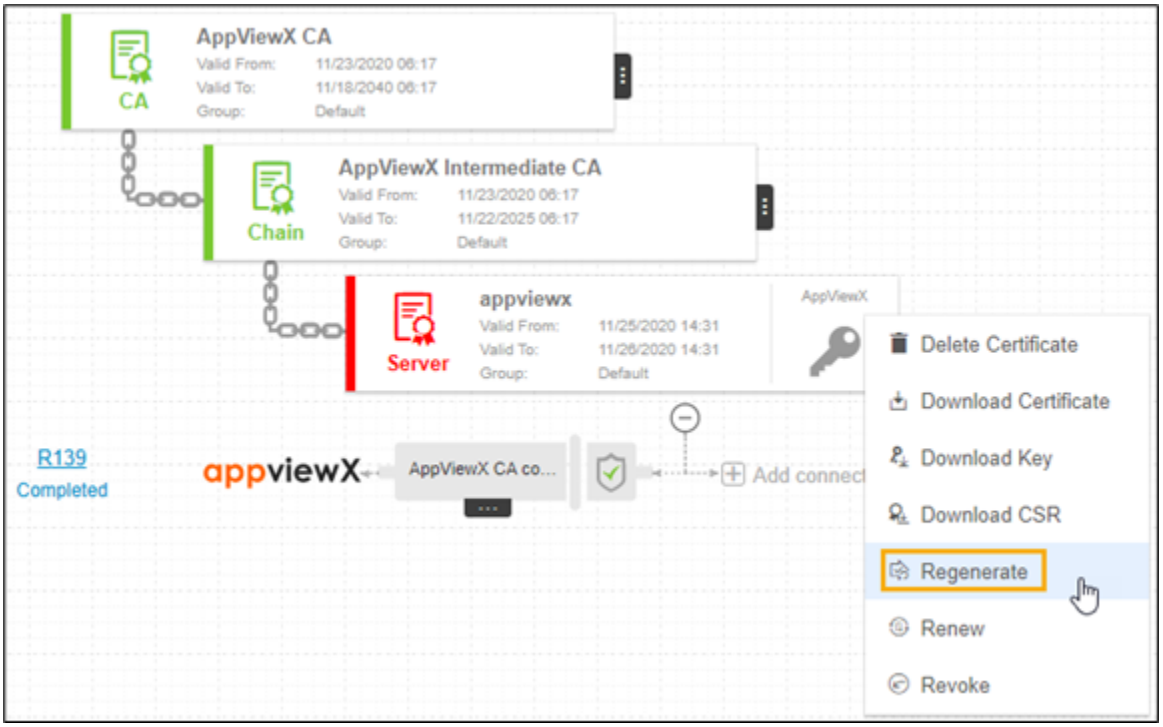


6. In the **Common Name** column certificate list, select the desired certificate that you want to regenerate a certificate.

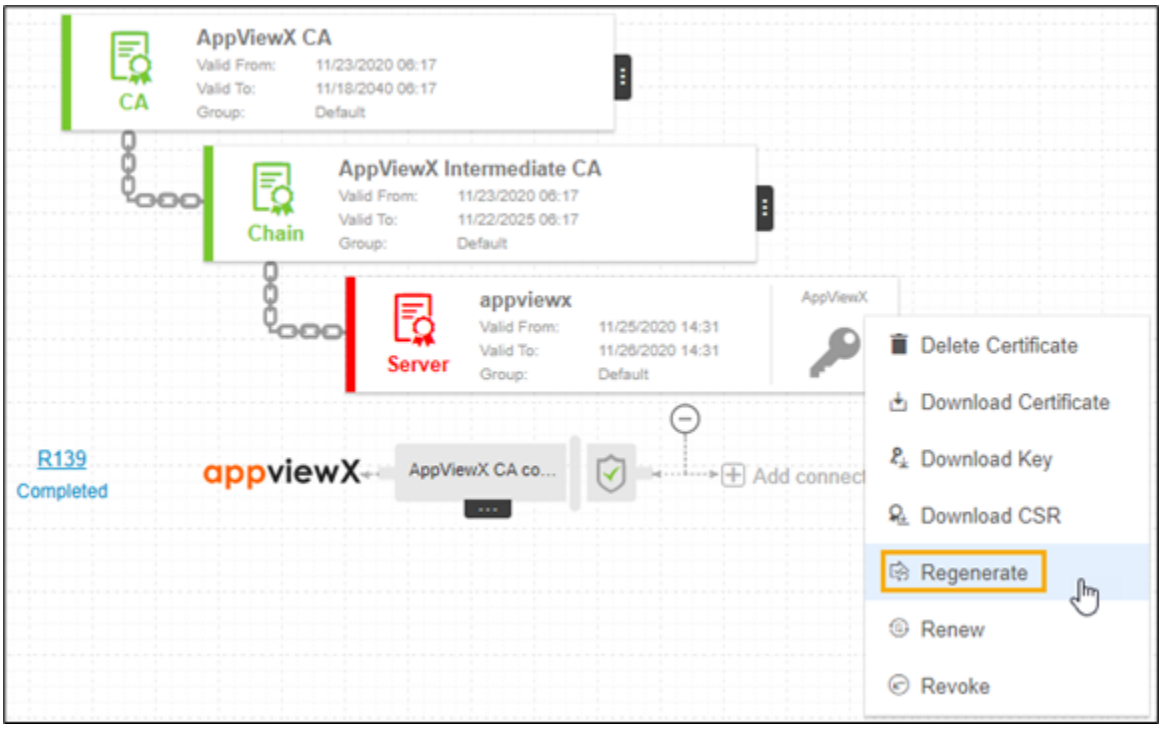
   The holistic view page appears.



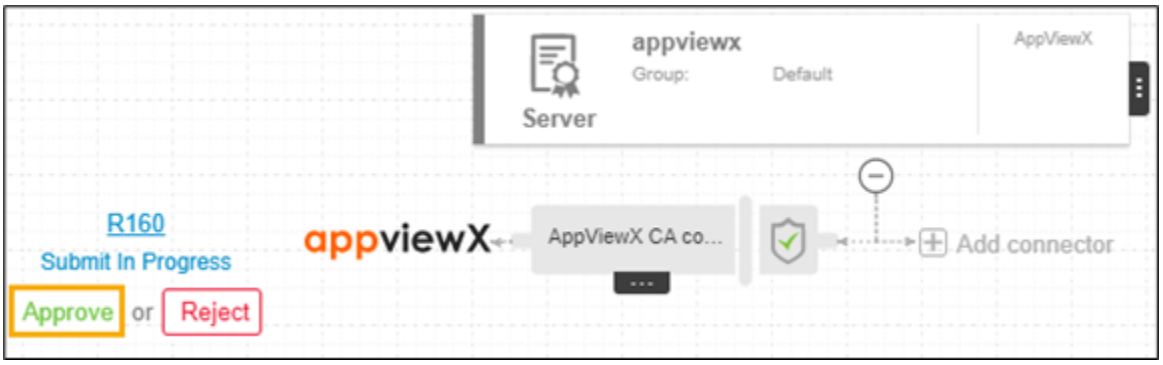
7. Click the vertical eclipsis icon, and then select **Regenerate** from the list.



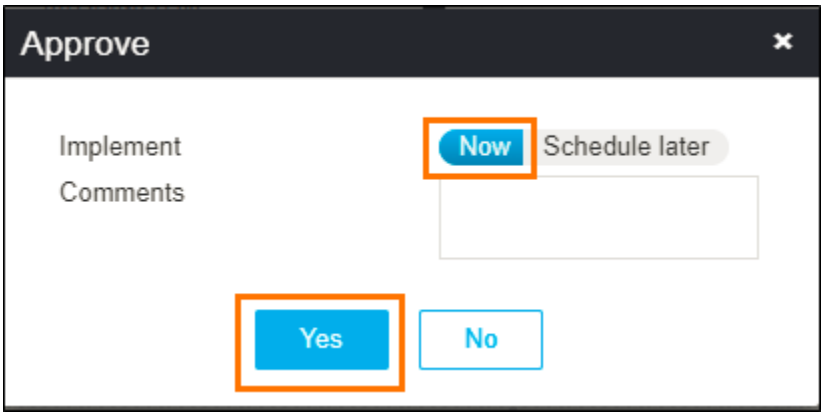
8. Modify the required details in the **General Information, CA Details, CSR Parameters, Attachments, Generic Fields, Vendor-Specific Details,** and **Custom Attributes** sections.
9. Click **Regenerate**.



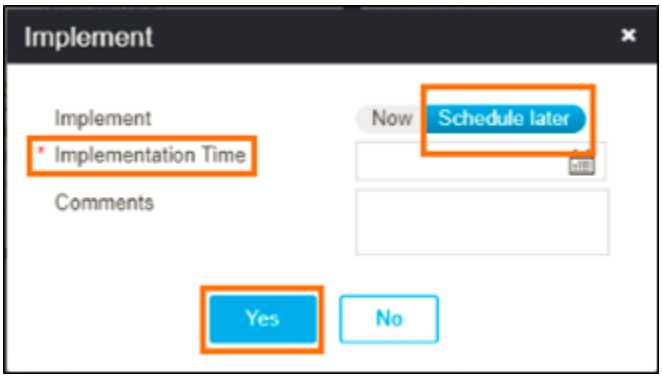
10. Regenerate process is initiated.
11. Click **Approve** to proceed.



12. The **Approve** pop-up window appears.



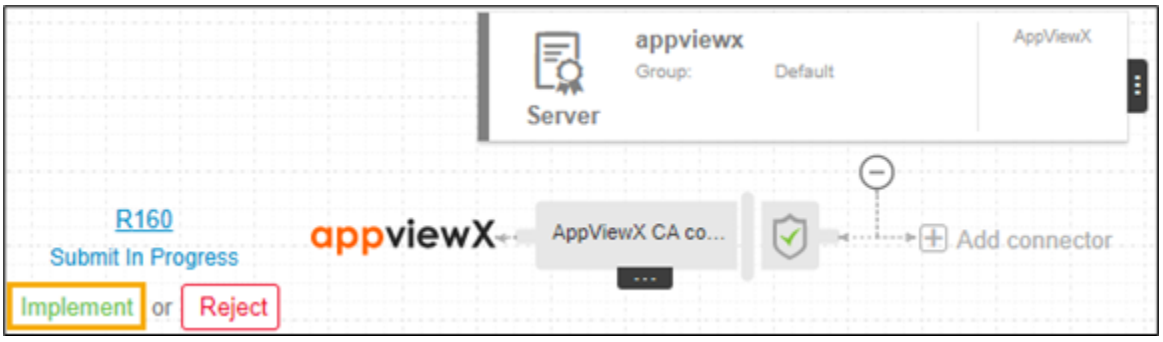
13. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.



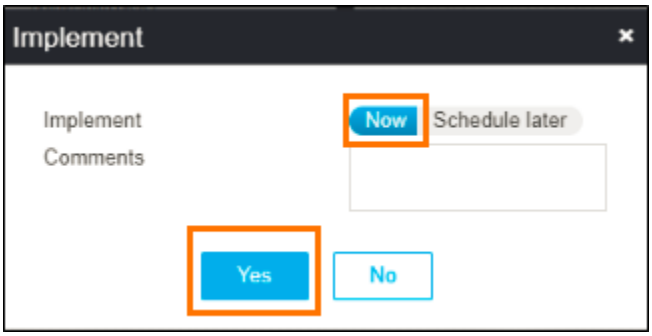
14. Select the **Implementation Time** from the calendar field.
15. Enter the comments in the field.
16. Click **Yes**.

    The approval process is initiated.

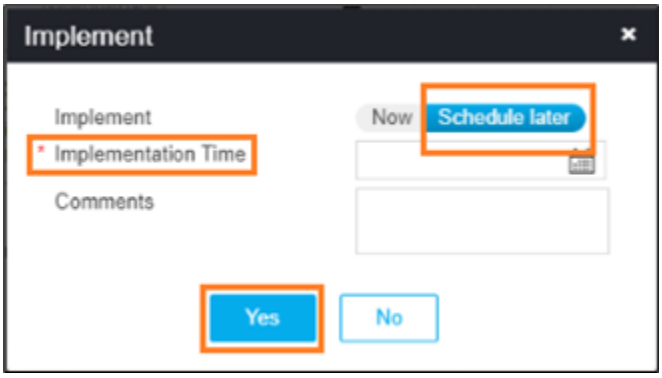
17. Click **Implement**.



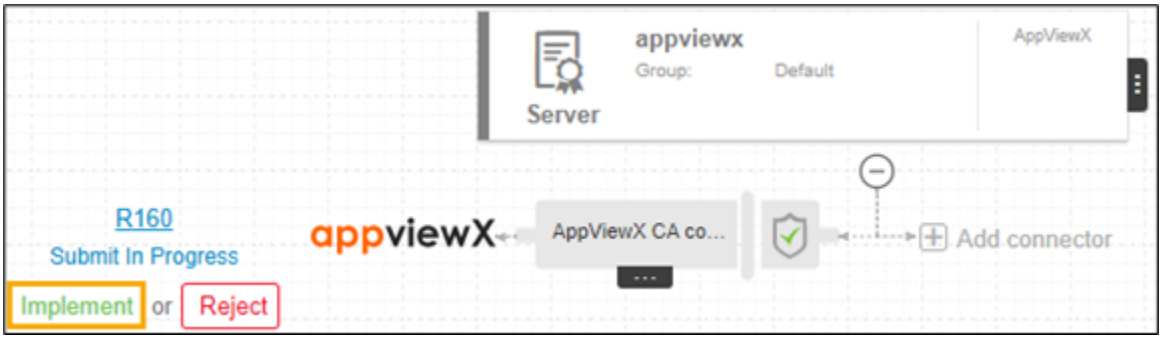
18. The **Implement** pop-up window appears.



19. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



20. Select the **Implementation Time** from the calendar field.
21. Enter the comments in the field.
22. Click **Yes**.
23. After the regenerate action is completed, the status updates to **Completed**.



Reinstating Certificate

- Overview
- Reinstating a Server Certificate

Overview

Reinstate is an action that can be applied only on the suspended certificate. Suspend is a temporary revocation of a certificate where the user is unsure about certificate usage. Once reinstated, the certificate will get resumed to serve its purpose normally. The suspend and reinstate are the actions supported only by a few CAs such as Microsoft, Entrust, and so on.

Note:
This option is available only for Microsoft and EJBCA certificate authorities.

Reinstating a Server Certificate

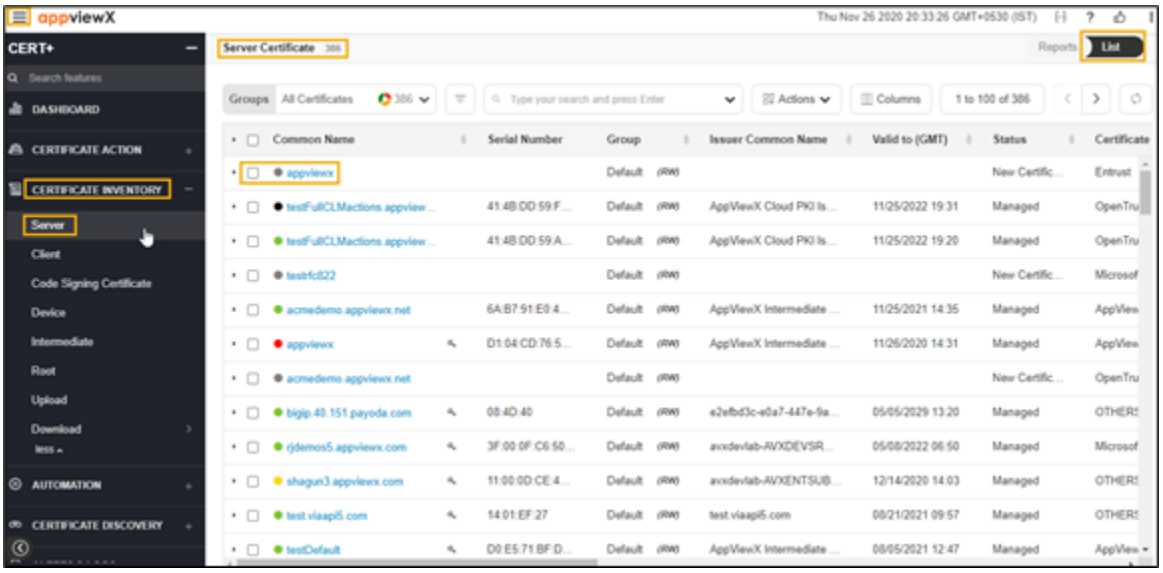
To reinstate a server certificate,

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+**.

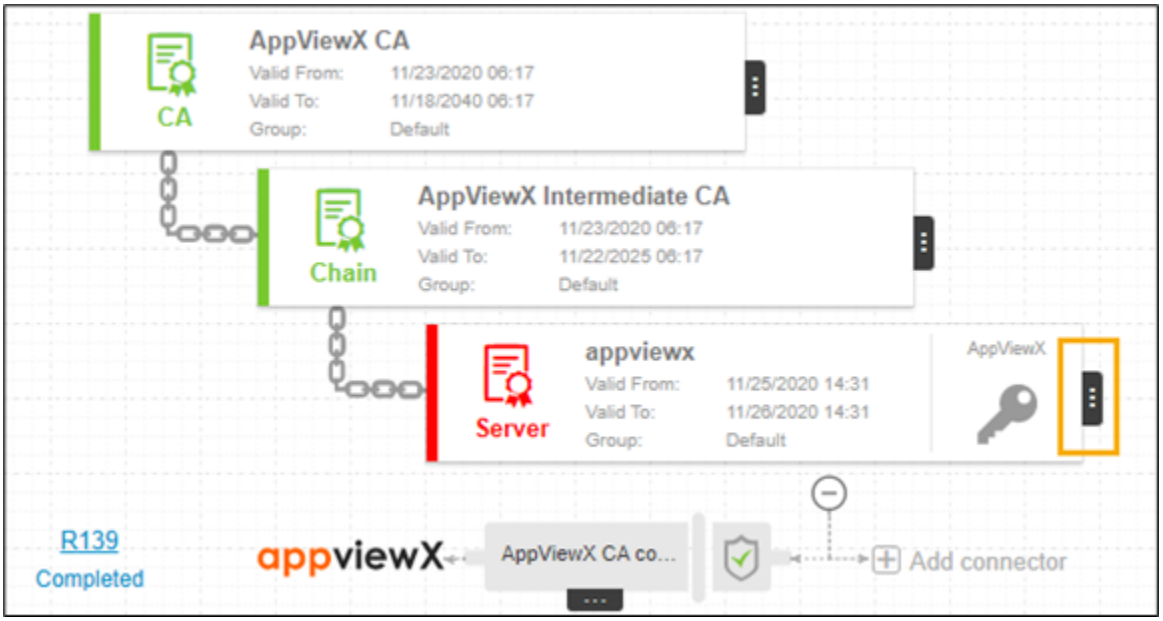
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Server**.

   The **Server Certificate** page appears.

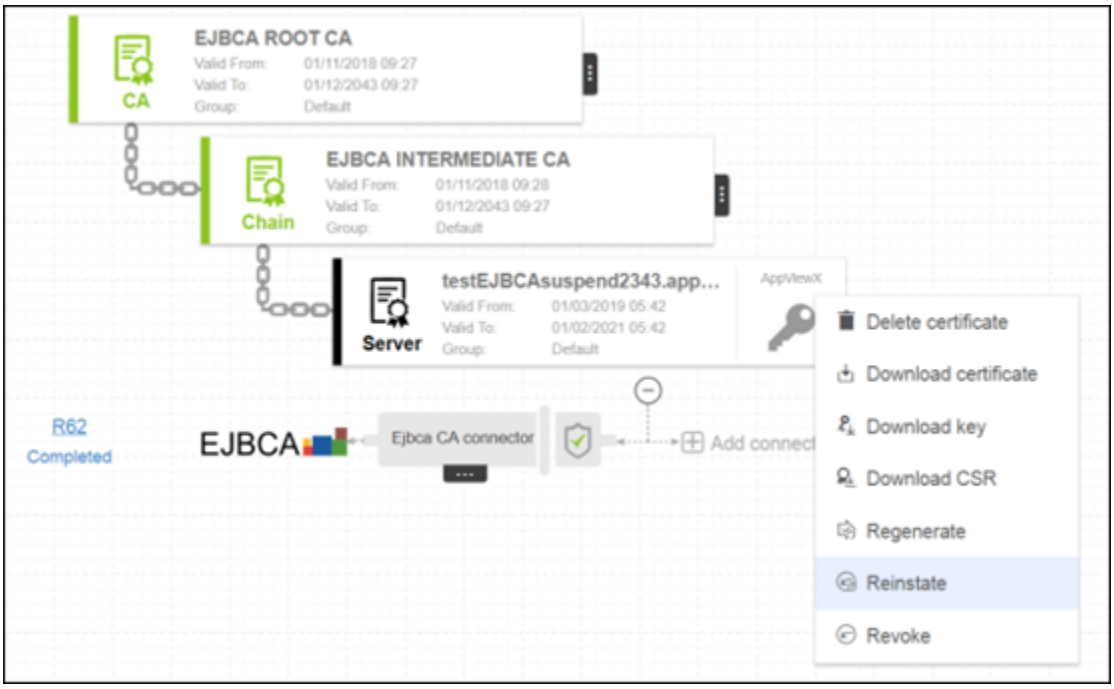


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to regenerate a certificate.

   The holistic view page appears.



7. Click the vertical eclipse icon, and then select **Regenerate** from the list.



The **Reinstate** pop-up window appears.

8. On the **Certificate reinstate** pop-up window, select a reason for reinstating the certificate from the list.
9. In the **Comments** field, enter details for reinstating the certificate.
10. Click **Yes**.

Reinstating Client Certificate

To reinstate a client certificate,

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

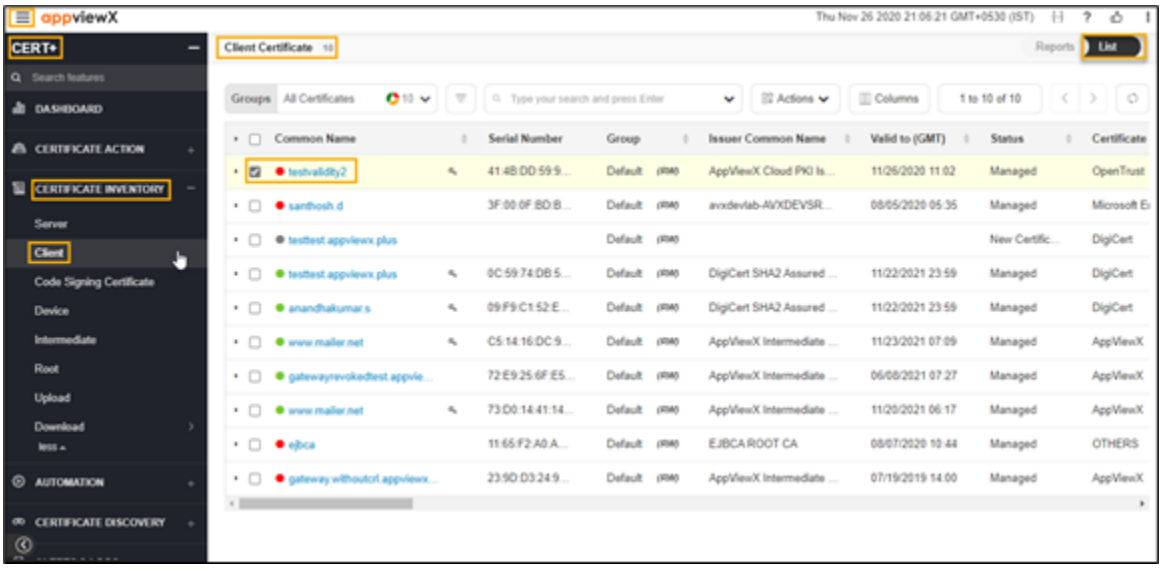
   The left navigation pane appears.

3. Click **CERT+**.

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

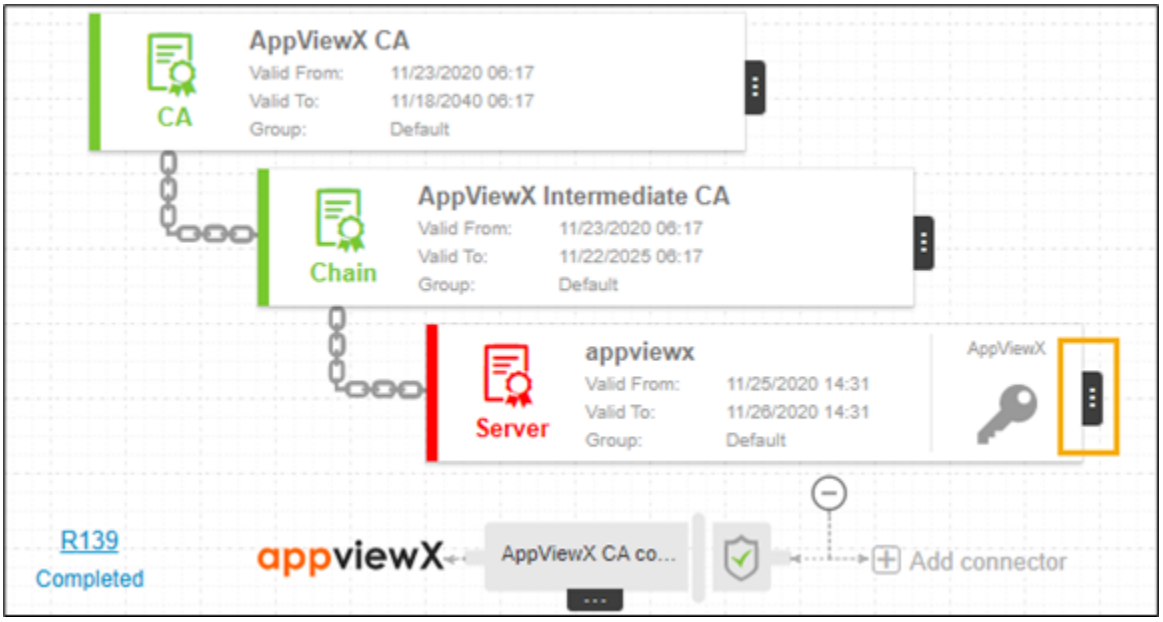
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.

   The **Client Certificate** page appears.

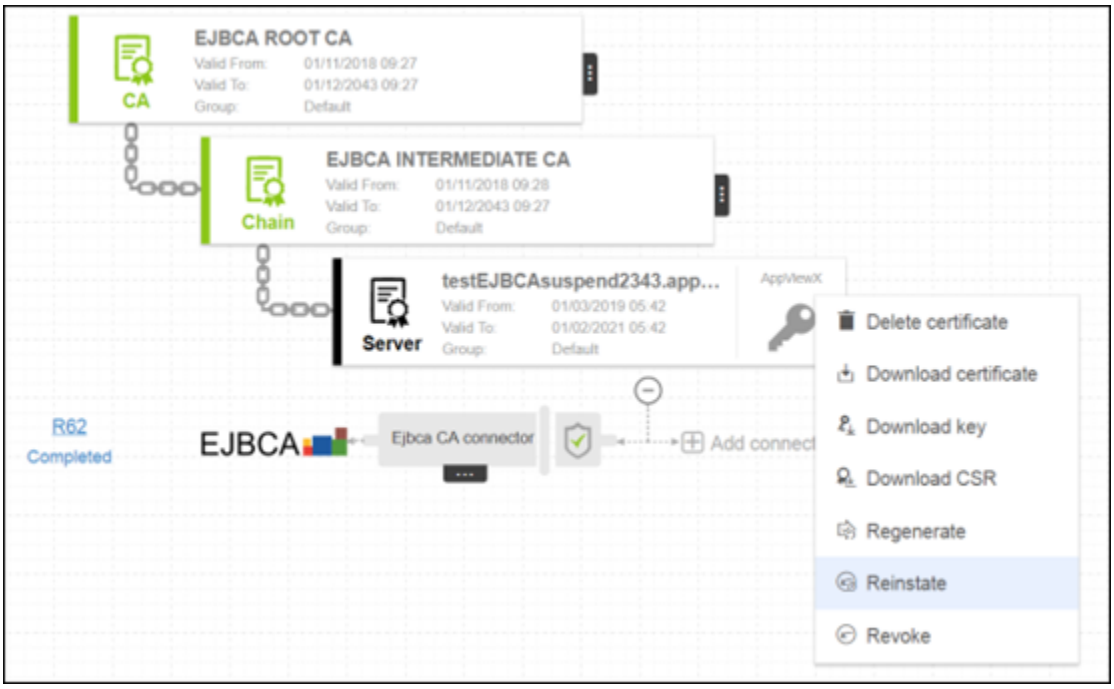


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to regenerate a certificate.

   The holistic view page appears.



7. Click the vertical eclipse icon, and then select **Regenerate** from the list.



The **Reinstate** pop-up window appears.

8. On the **Certificate reinstate** pop-up window, select a reason for reinstating the certificate from the list.
9. In the **Comments** field, enter details for reinstating the certificate.
10. Click **Yes**.

Reinstating Code Signing Certificate

To reinstate a code signing certificate,

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

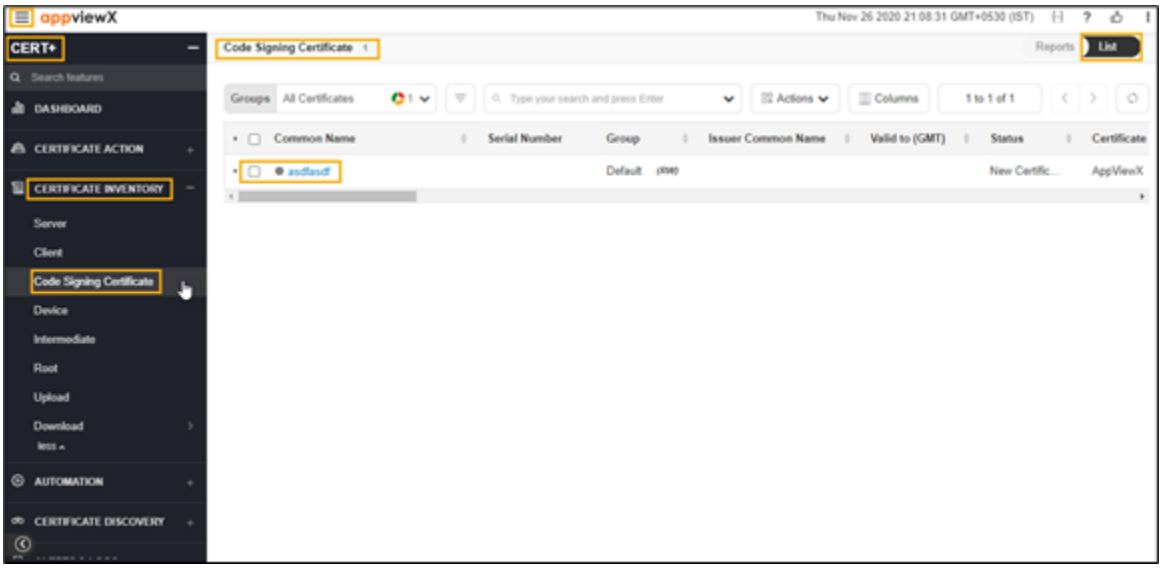
   The left navigation pane appears.

3. Click **CERT+**.

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

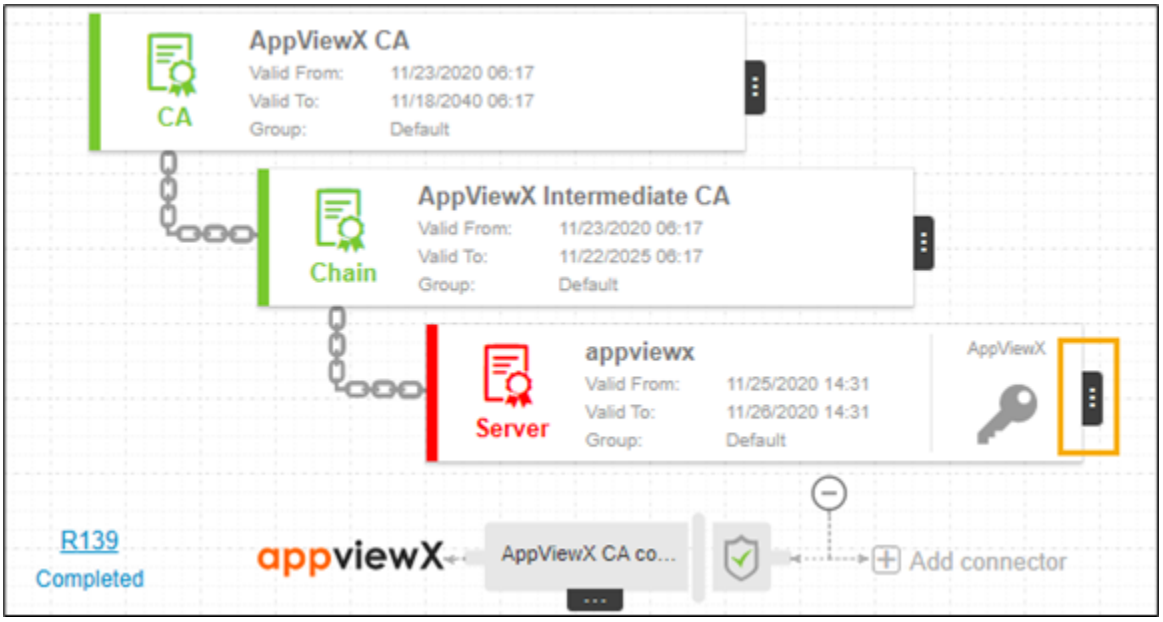
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.

   The **Code Signing Certificate** page appears.

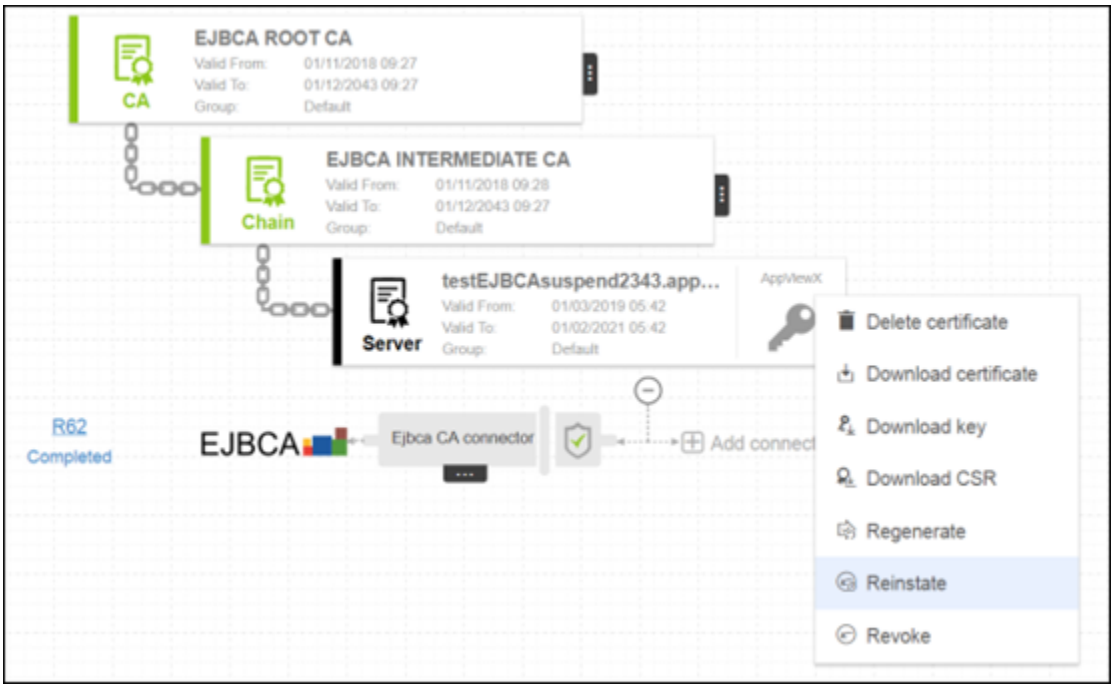


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to regenerate a certificate.

   The holistic view page appears.



7. Click the vertical eclipse icon, and then select **Regenerate** from the list.



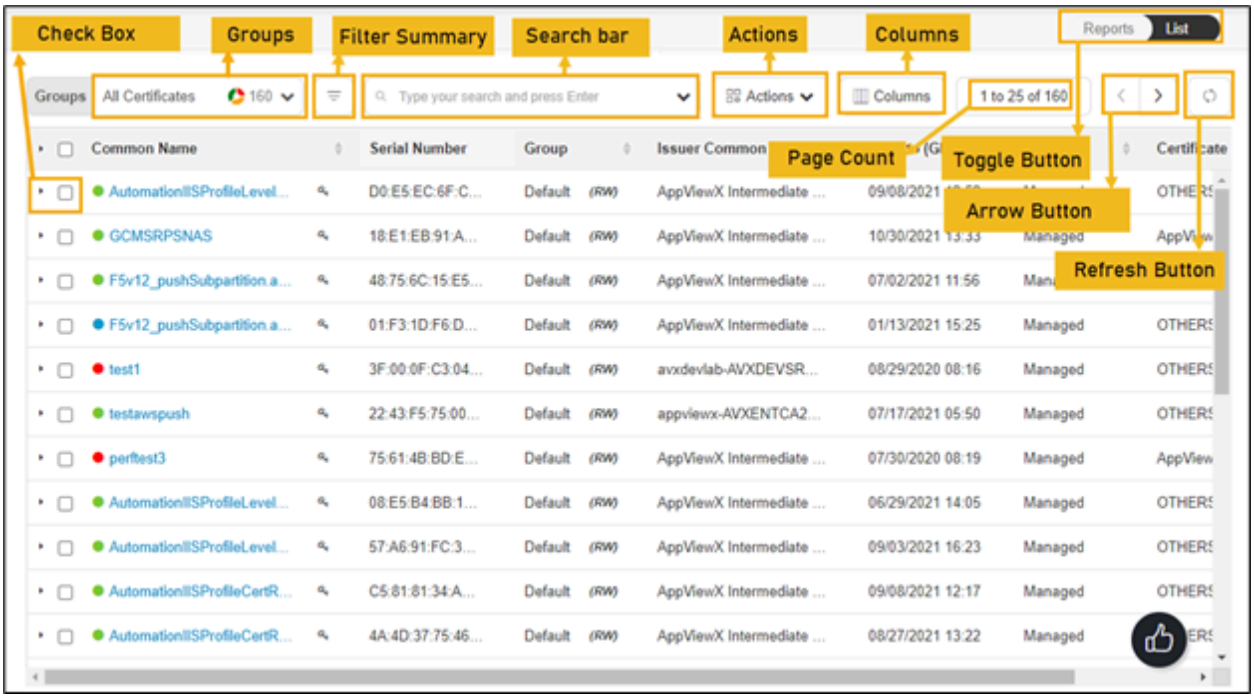
The **Reinstate** pop-up window appears.

8. On the **Certificate reinstate** pop-up window, select a reason for reinstating the certificate from the list.
9. In the **Comments** field, enter details for reinstating the certificate.
10. Click **Yes**.

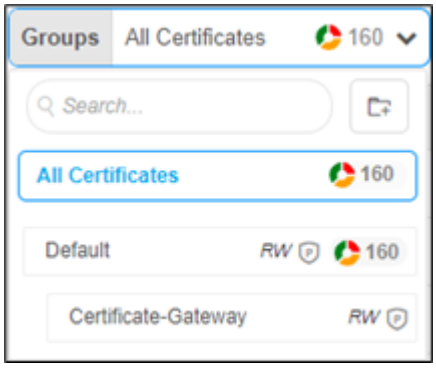
Running Revocation Check-OCSP

Overview

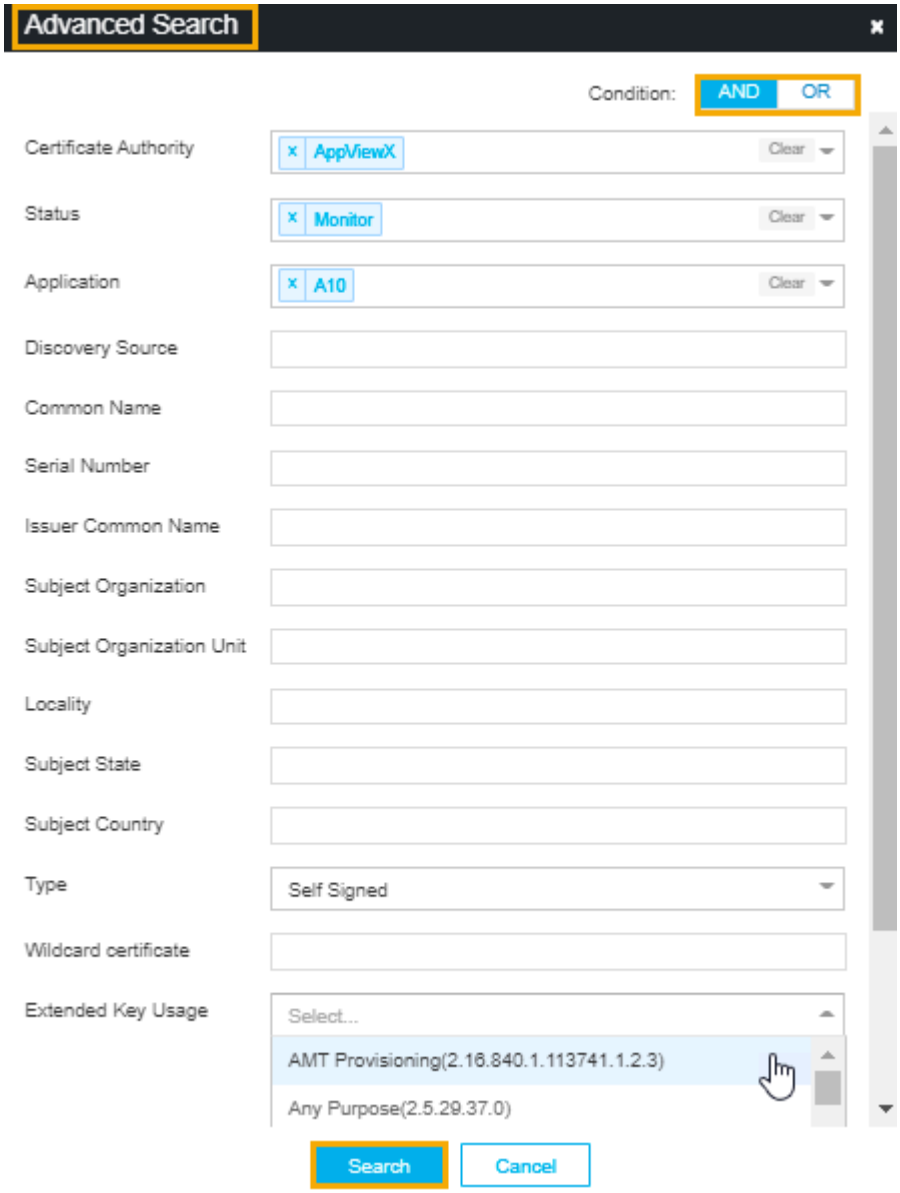
A sophisticated method of detecting revoked certificates is the Online Certificate Status Protocol (OCSP). Instead of downloading and parsing the entire CRL, the client can send the certificate in question to the CA. And then, the CA replies status of the certificate is good, revoked, or unknown. This method involves far less overhead than CRL and is also more reliable.



The following table describes the options available on the renew certificate page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state.

Options	Description
	
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description
	

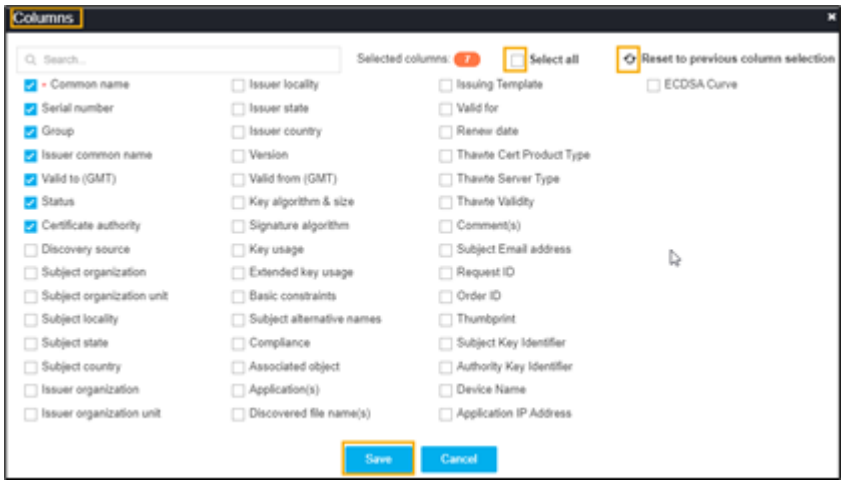
The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Options</th><th>Description</th></tr>
<tr><td>Certificate Authority</td><td>Allows you to select the desired CA from the dropdown list.</td></tr>
<tr><td>Status</td><td>Allows you to select the desired status certificate. The possible options are,

• Manage
• Monitor
• New certificate.</td></tr>
<tr><td>Discovery Source</td><td>Enter the source of the discovery.</td></tr>
<tr><td>Common Name</td><td>Enter the common name of the certificate.</td></tr>
<tr><td>Serial Number</td><td>Enter the serial number of the certificate.</td></tr>
<tr><td>Issuer Common Name</td><td>Enter the name of the certificate issuer.</td></tr>
<tr><td>Subject Organization</td><td>Enter the subject of the organization.</td></tr>
<tr><td>Subject Organization Unit</td><td>Enter the subject of the organization’s unit.</td></tr>
<tr><td>Locality</td><td>Enter the specific locality.</td></tr>
<tr><td>Subject State</td><td>State Enter the state of the certificate’s subject.</td></tr>
<tr><td>Subject Country</td><td>Country of the subject.</td></tr>
<tr><td>Type</td><td>Type of the certificate.</td></tr>
<tr><td>Wildcard certificate</td><td>Enter the wildcard certificates.</td></tr>
<tr><td>Extended Key Usage</td><td>Allows you to select the EKU from the dropdown list.</td></tr>
<tr><td>Search</td><td>Click the Search button to get the results from the search.</td></tr>
</table>
</td></tr>
<tr><td>Actions</td><td>Displays the list of actions. The possible actions are,

• Export Certificates
• Import Certificates</td></tr>
</table>

Options	Description
	• Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are,

Options	Description
	• Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Running Revocation Check for Server Certificate

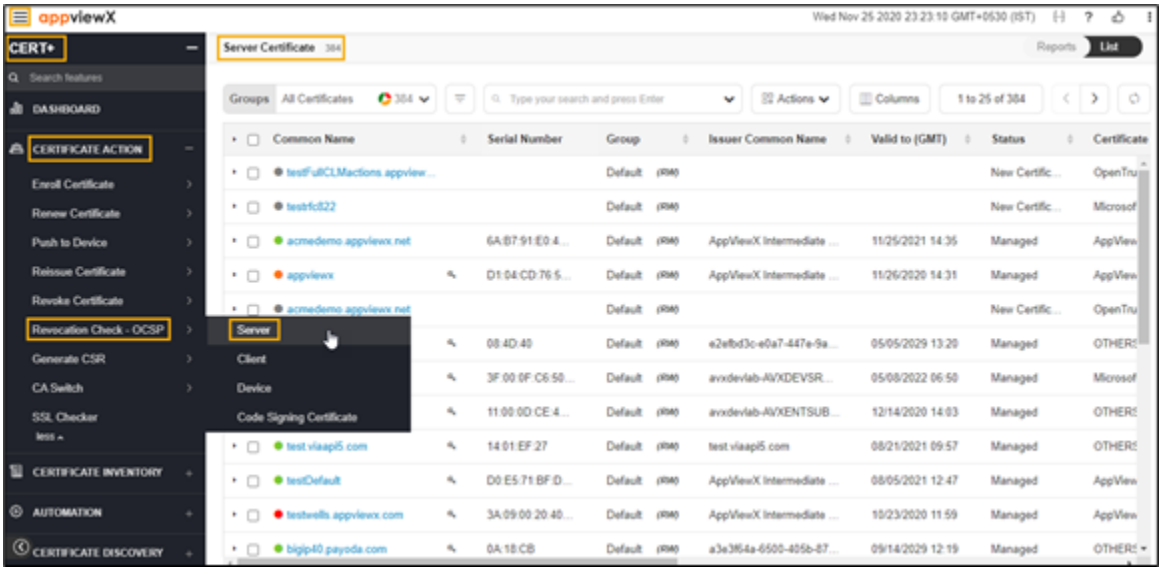
To perform revocation check for server certificate,

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

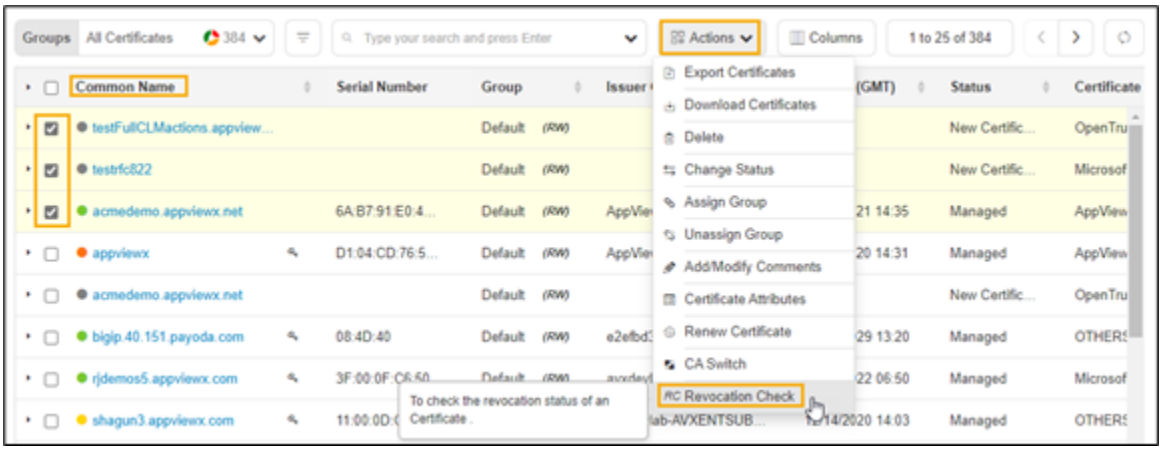
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE ACTION**.
5. Select **Revocation Check - OCSP**, and then **Server**.

   The **Server Certificate** page appears.

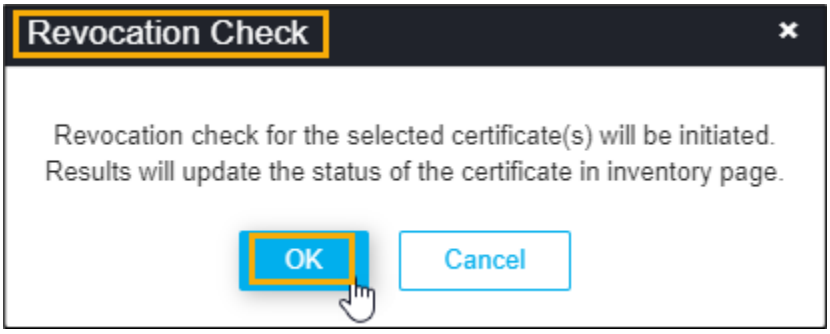


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to do the revocation check.



7. Click **Actions**, and then select **Revocation Check**.

   The **Revocation Check** pop-up window appears.



8. Click **OK**.

   The status of the revoked certificate is displayed on the **Valid to** (**GMT**) column.

Running Revocation Check for Client Certificate

To perform revocation check for client certificate,

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

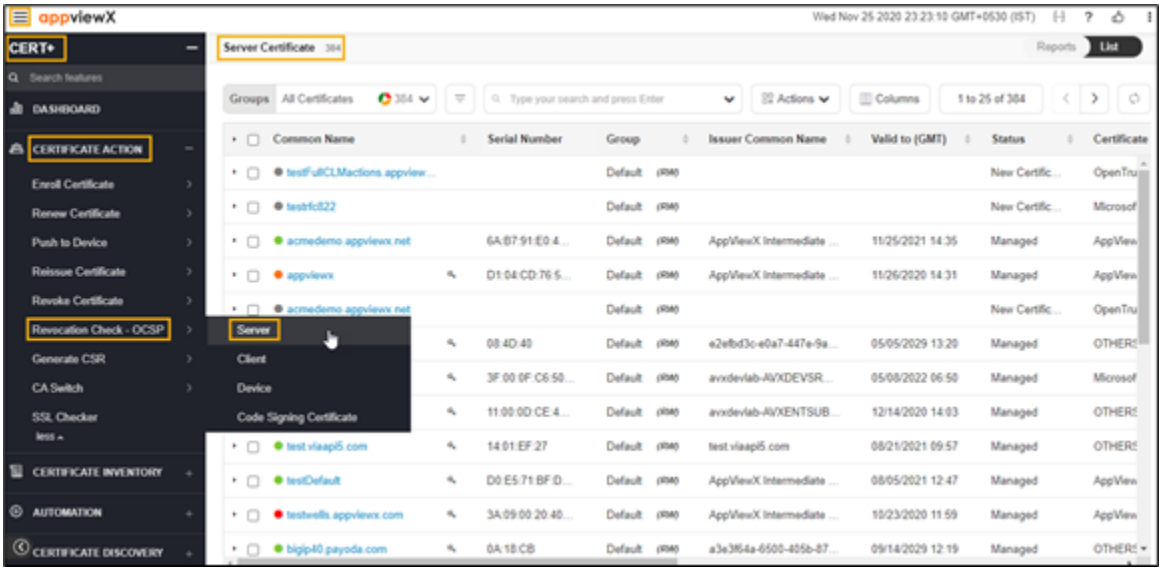
   The left navigation pane appears.

3. Click **CERT+**.

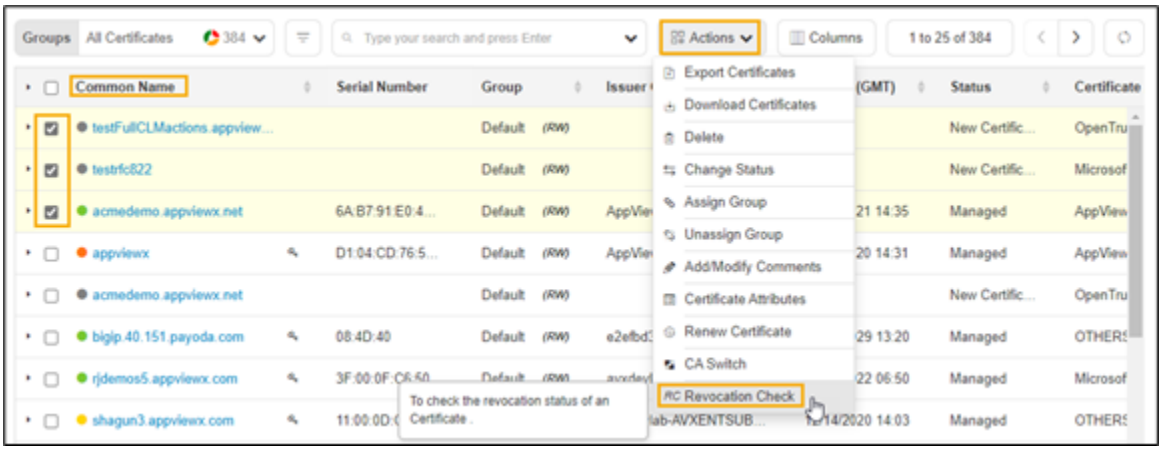
The **CERT+** left navigation pane appears.

4. Expand **CERTIFICATE ACTION**.
5. Select **Revocation Check - OCSP**, and then **Client**.

   The **Client Certificate** page appears.

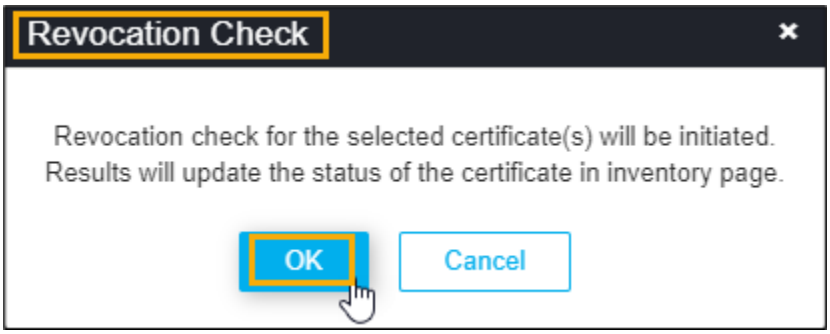


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to do the revocation check.



7. Click **Actions**, and then select **Revocation Check**.

   The **Revocation Check** pop-up window appears.



8. Click **OK**.

   The status of the revoked certificate is displayed on the **Valid to** (**GMT**) column.

Running Revocation Check for Device Certificate

To perform revocation check for device certificate,

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

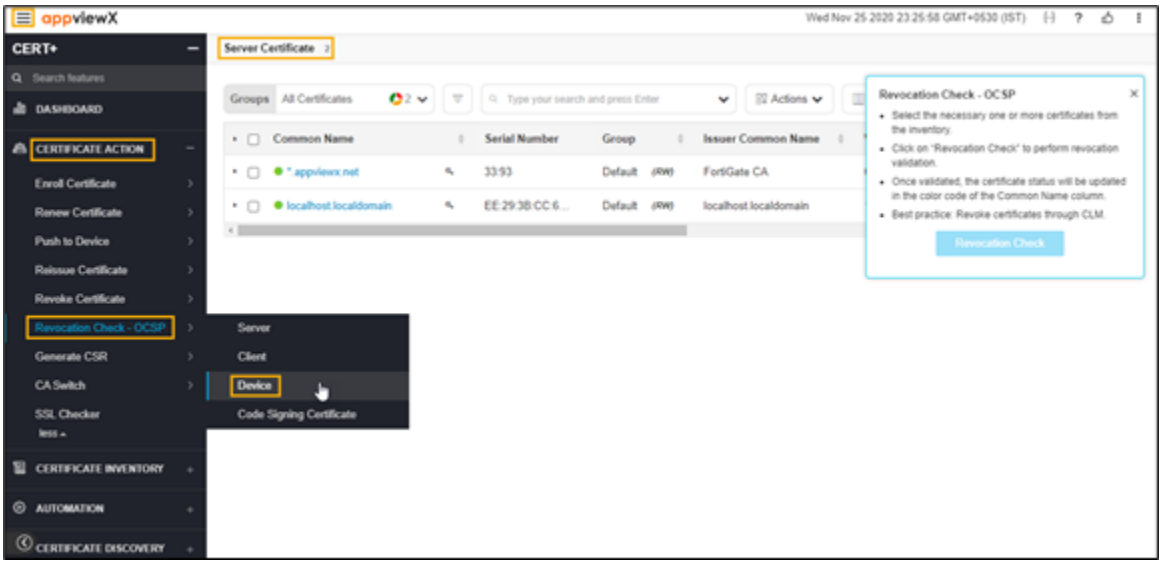
   The left navigation pane appears.

3. Click **CERT+**.

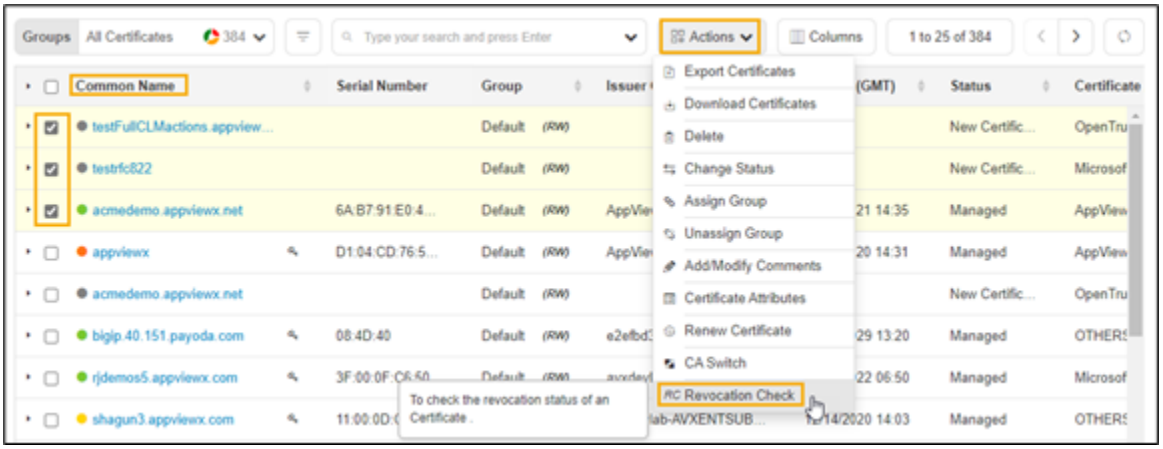
   The **CERT+** left navigation pane appears.

4. Expand **CERTIFICATE ACTION**.
5. Select **Revocation Check - OCSP**, and then **Device**.

   The **Device Certificate** page appears.

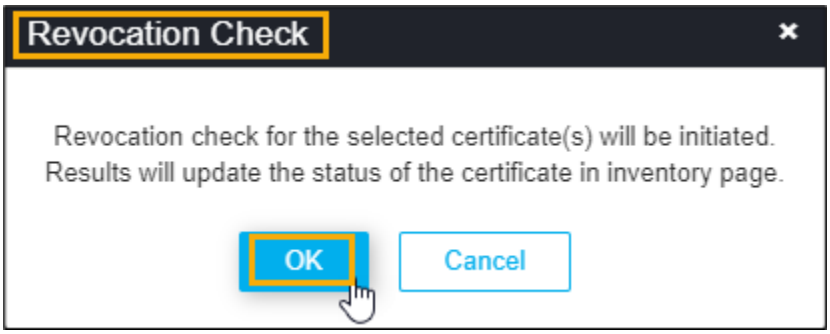


6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to do the revocation check.



7. Click **Actions**, and then select **Revocation Check**.

   The **Revocation Check** pop-up window appears.



8. Click **OK**.

   The status of the revoked certificate is displayed on the **Valid to** (**GMT**) column.

Running Revocation Check for Code Signing Certificate

To perform revocation check for certificate,

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

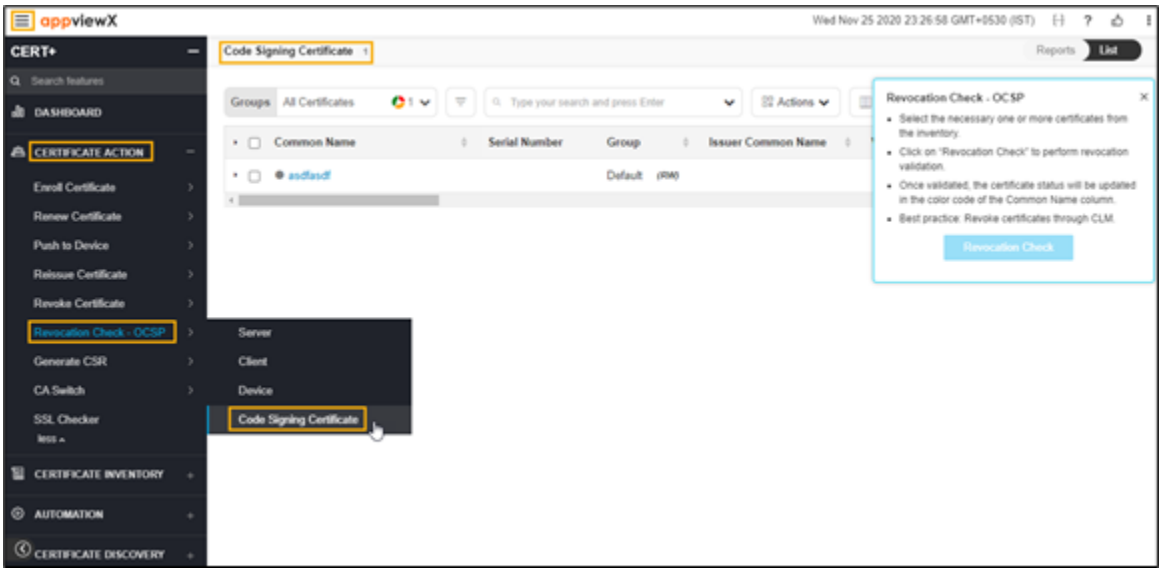
   The left navigation pane appears.

3. Click **CERT+**.

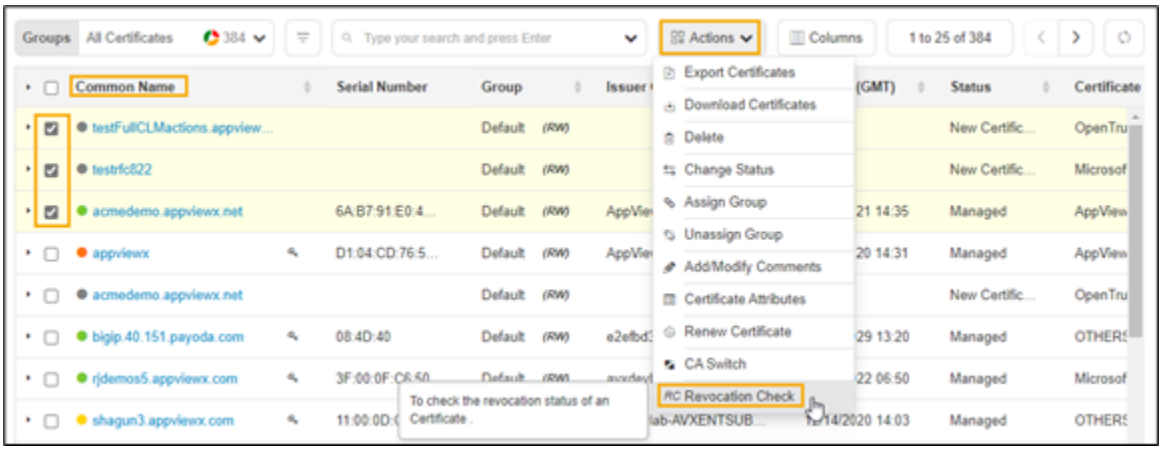
   The **CERT+** left navigation pane appears.

4. Expand **CERTIFICATE ACTION**.
5. Select **Revocation Check - OCSP**, and then **Code Signing Certificate**.

   The **Code Signing Certificate** page appears.

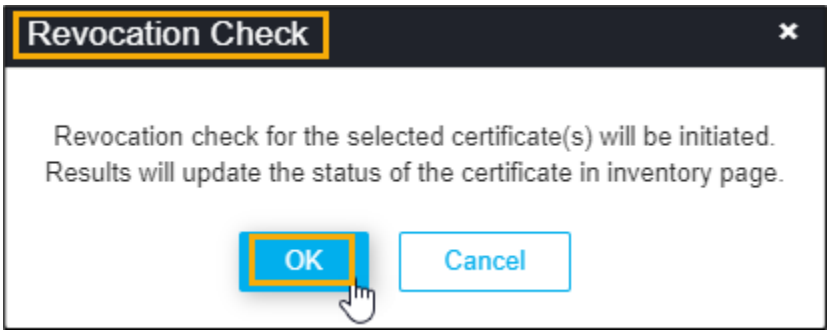


6. In the **Common Name** column certificate list, select the desired certificate that you want to do the revocation check.



7. Click **Actions**, and then select **Revocation Check**.

   The **Revocation Check** pop-up window appears.



8. Click **OK**.

   The status of the revoked certificate is displayed on the **Valid to** (**GMT**) column.

Generating Certificate Signing Request (CSR)

- Overview
- Generating Manual CSR for Server Certificate
- Generating Manual CSR for Code Signing Certificate

Overview

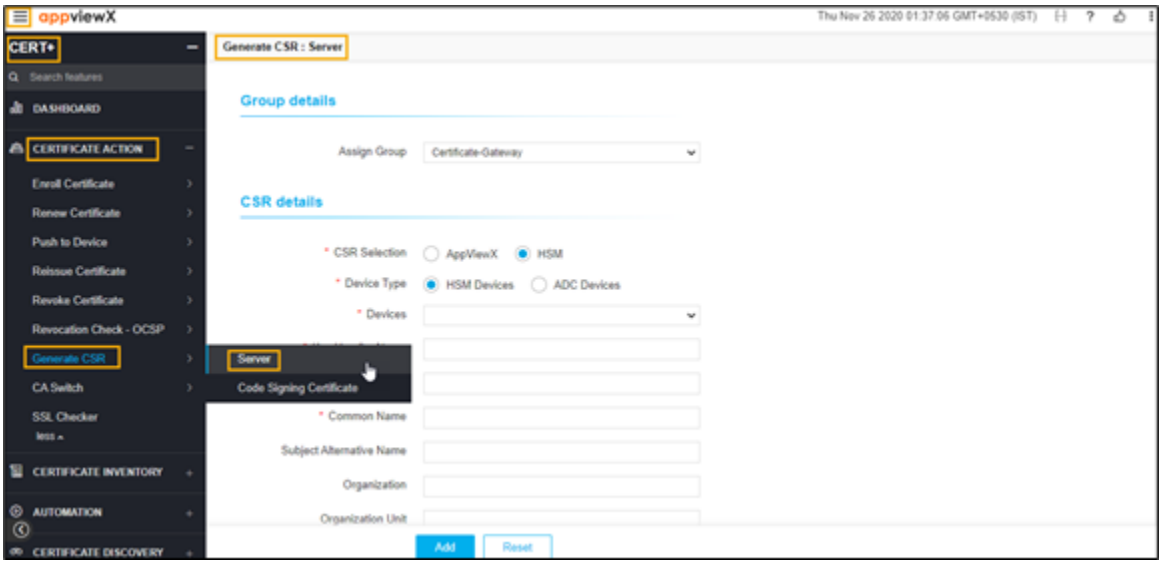
CERT+ can be used as a CSR generation tool where you can choose either the keys that can be generated in the filesystem or any HSM device integrated with AppViewX.The CSR is the certificate

signing request which consists of requester info in a standardized way. Based on the organization's needs and the business model, the CSR generation and approval flow can be customized.

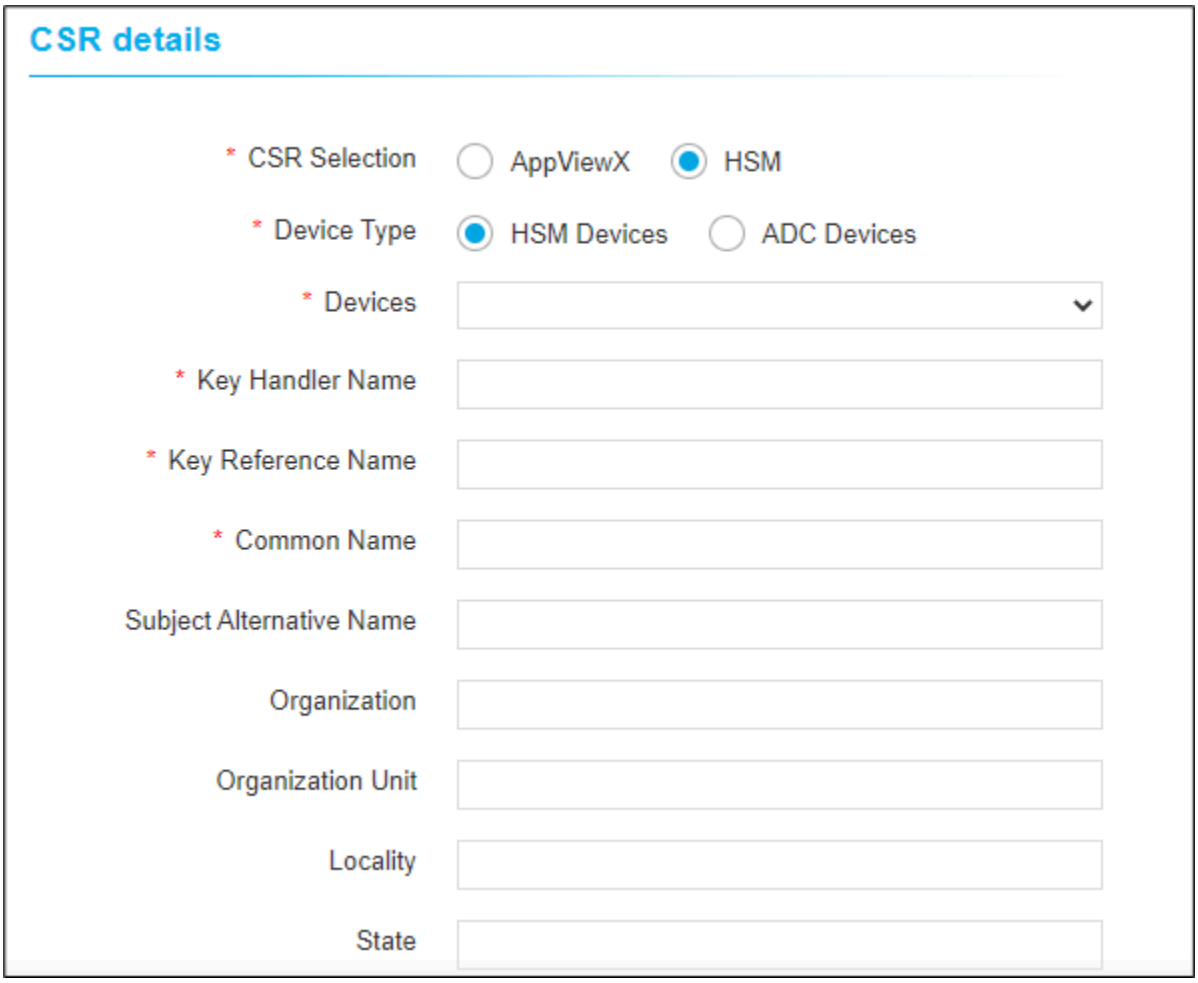
Generating Manual CSR for Server Certificate

To generate a manual CSR for the server certificate,

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 ACTION**.
5. Select **Generate CSR**, and then **Server**.
   The **Generate CSR:Server** page appears.



6. In the Group details section, select the **Assign Group** from the dropdown list that you want to assign a CSR to the desired group of certificates.
7. In the CSR details section, select/enter the details as follows:



The following table describes the options available in the CSR Parameters section:

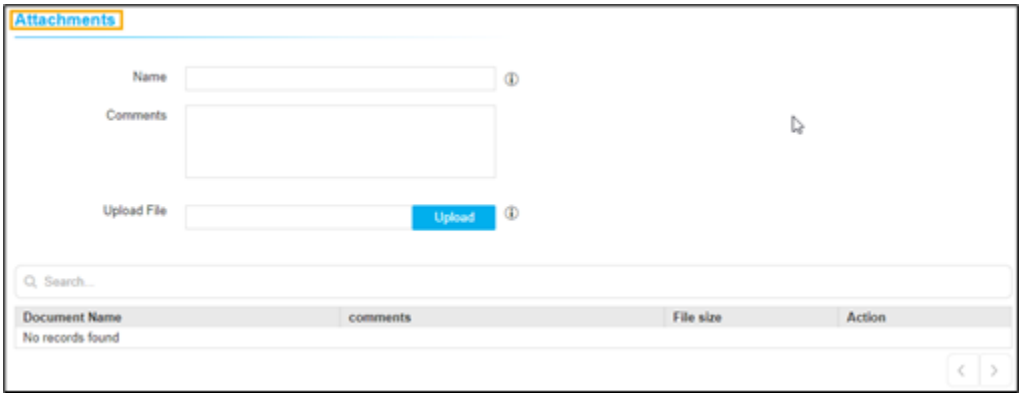
Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM.
***Device Type**	Select the type of device as required: Options are: • **HSM Devices** • **ADC Devices.**
***Device**	Select the device from the dropdown list.

Option	Description
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate. **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.

Option	Description
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.

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

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



The following table describes the options available in the attachments section:

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

Field	Description
	Note: You can enter a maximum of 2000 words in the field.
Upload File	Click the **Upload** button to select the file.

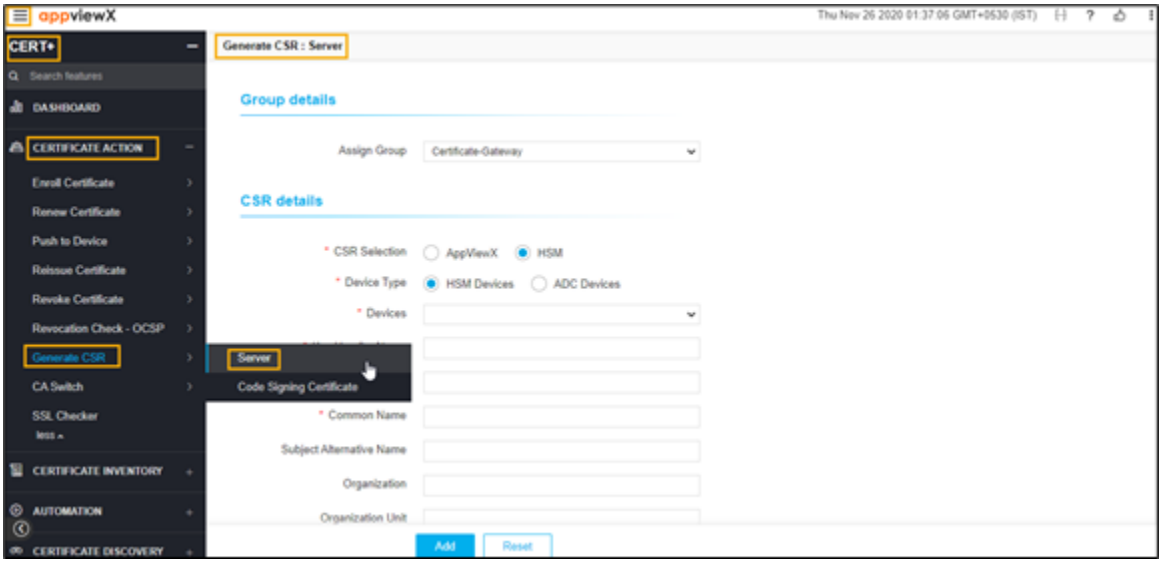
Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.

9. You can use **the Search** option to find the attachments from the attachment list.
10. Click **Add** to generate the CSR and add it to the intended group.

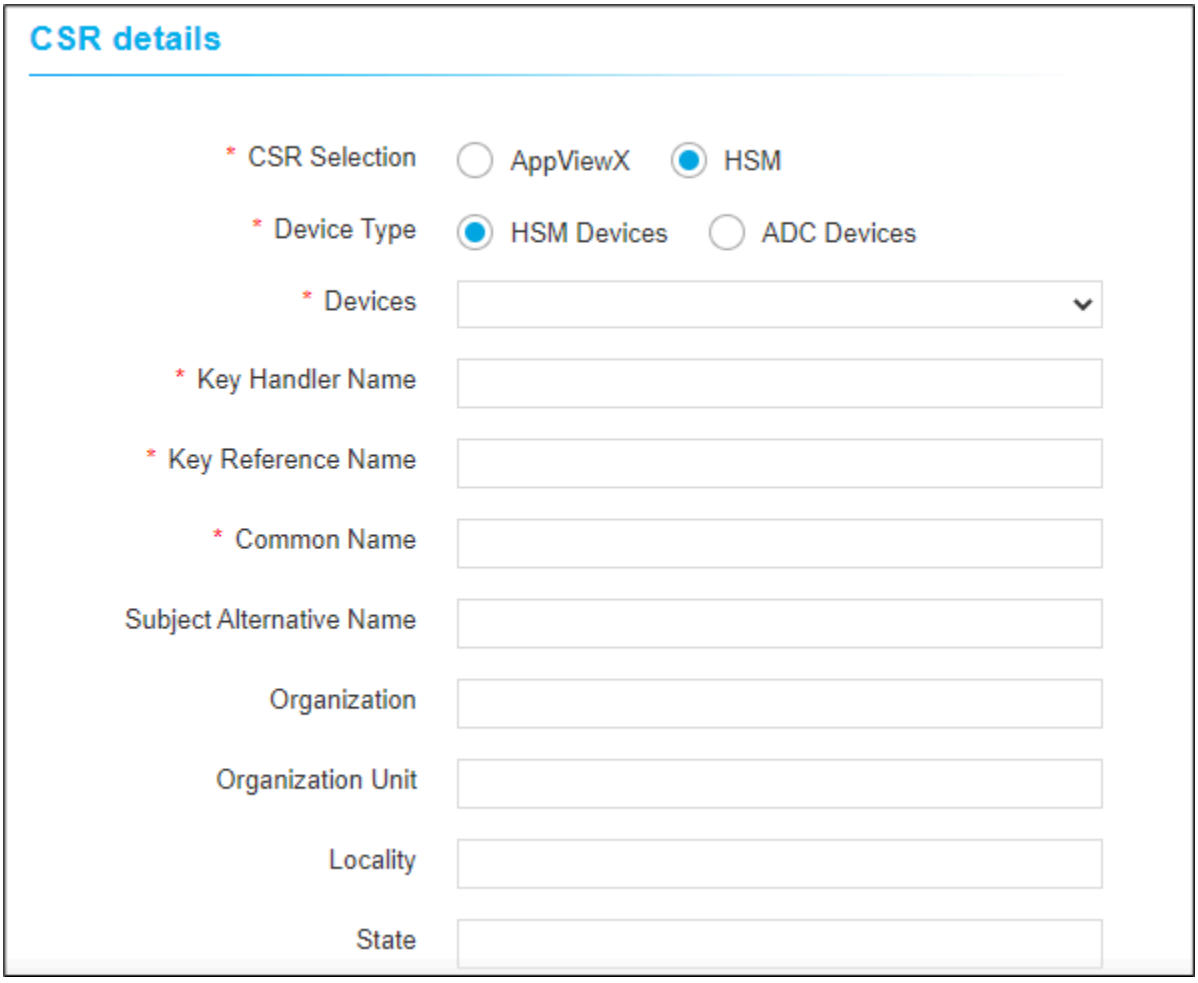
Generating Manual CSR for Code Signing Certificate

To generate a manual CSR for the code signing certificate,

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 ACTION**.
5. Select **Generate CSR**, and then **Server**.
   The **Generate CSR:Server** page appears.



6. In the Group details section, select the **Assign Group** from the dropdown list that you want to assign a CSR to the desired group of certificates.
7. In the CSR details section, select/enter the details as follows:



The following table describes the options available in the CSR Parameters section:

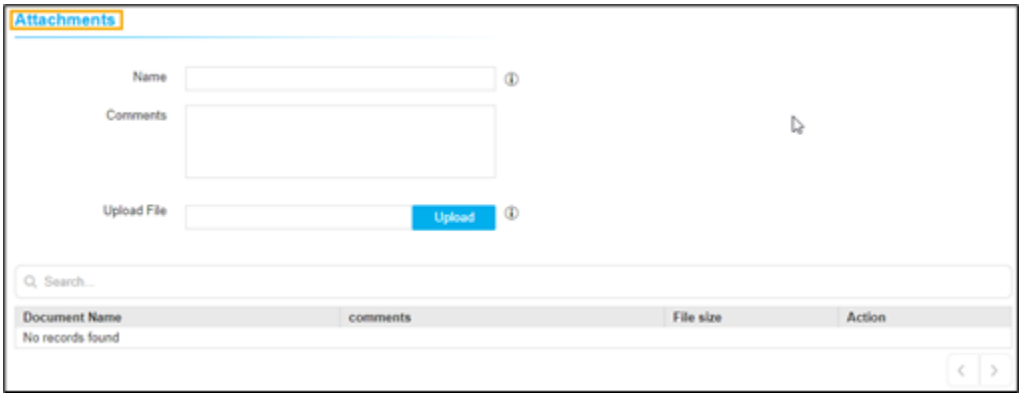
Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM.
***Device Type**	Select the type of device as required: Options are:

Option	Description
	• **HSM Devices** • **ADC Devices.**
***Device**	Select the device from the dropdown list.
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate. **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).

Option	Description
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.

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

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



The following table describes the options available in the attachments section:

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** You can enter a maximum of 2000 words in the field.
Upload File	Click the **Upload** button to select the file.
Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.	

9. You can use **the Search** option to find the attachments from the attachment list.
10. Click **Add** to generate the CSR and add it to the intended group.

CA Switch

Overview

The CA Switch feature in the **Inventory** module allows you to re-enroll the certificates from one CA to another CA. Once triggered, the certificate migration readiness for every certificate will be shown in the **Process Explorer**, which needs to be validated before the CA switch is performed.

Migrating the CA for Server Certificate

To migrate the CA for server certificate,

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.

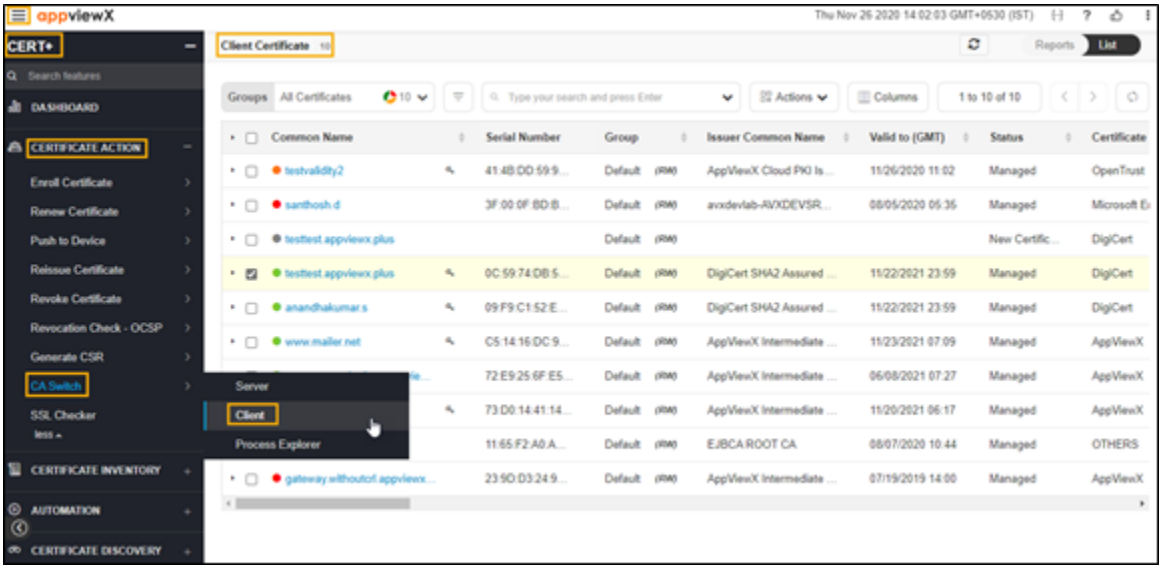
3. Click **CERT+**.

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

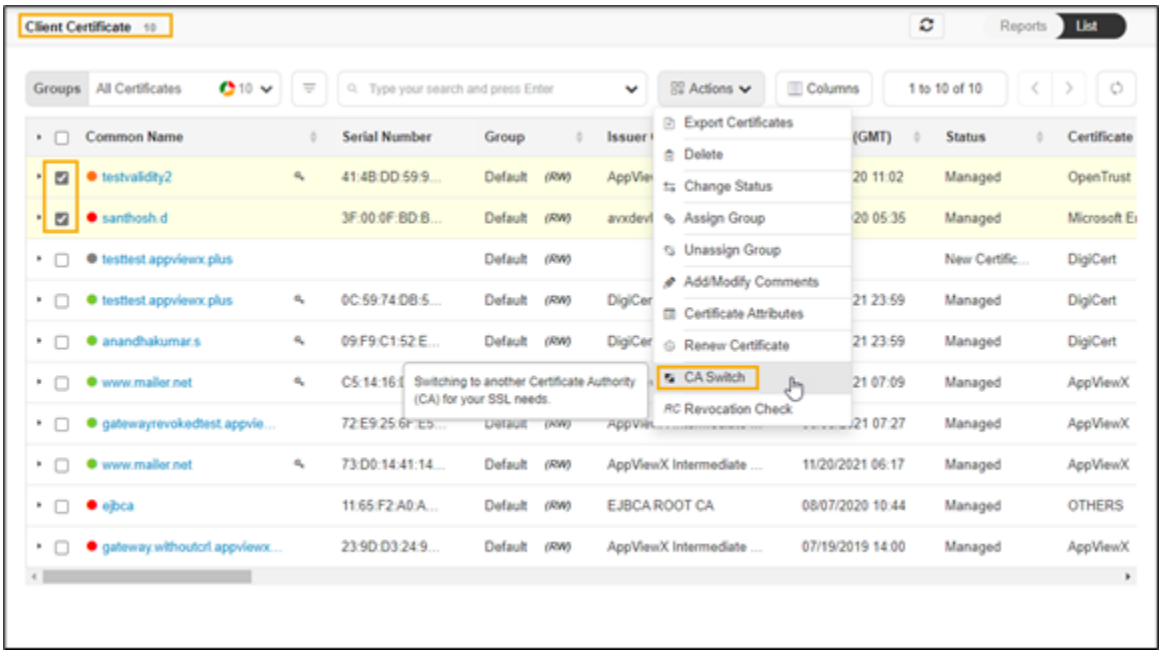
4. Expand **CERTIFICATE ACTION**.

5. Select **CA Switch**, and then **Server**.

   The **Server Certificate** page appears.

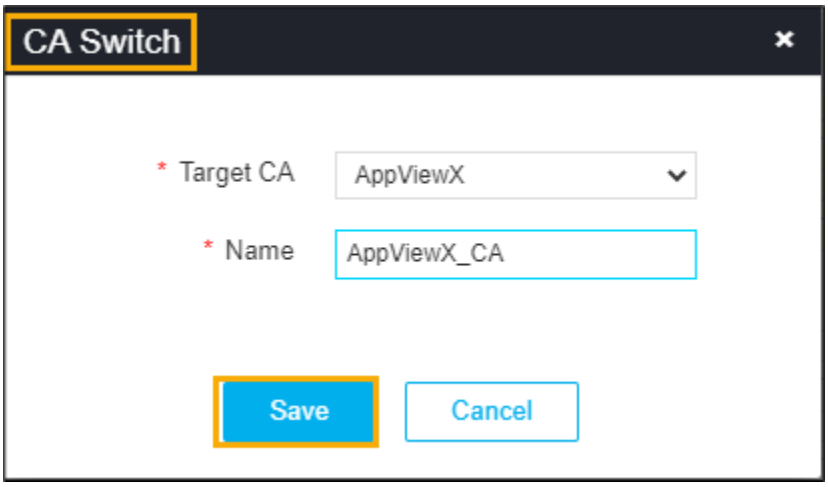


6. In the **Common Name** column certificate list, select the desired certificate that you want to migrate to the CA.



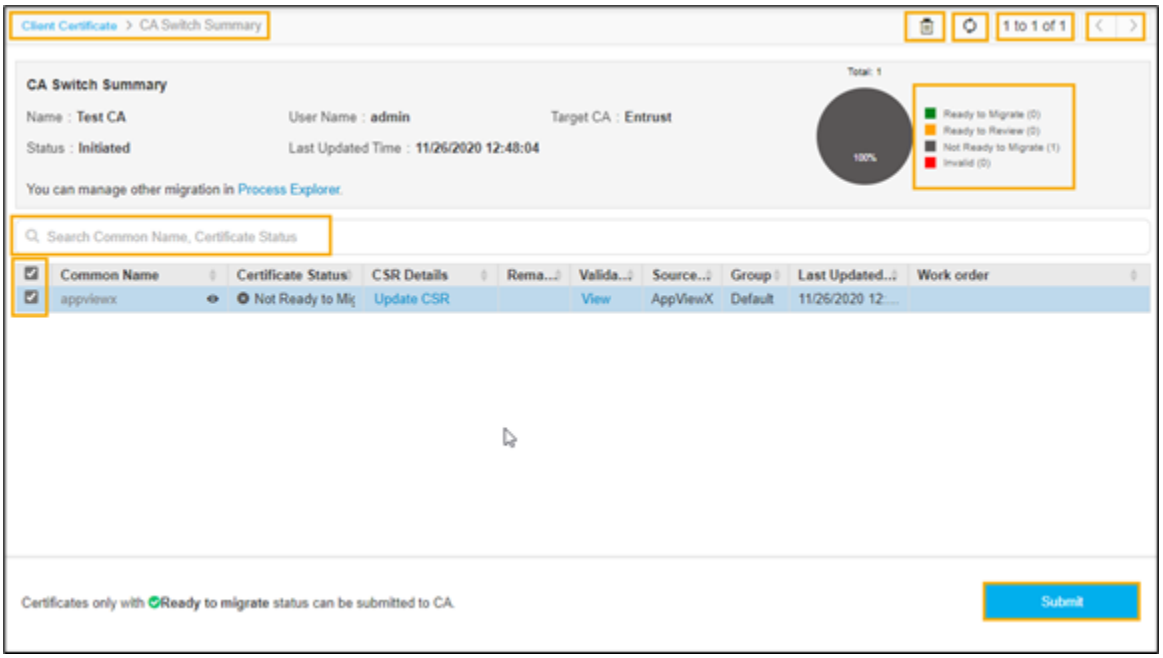
7. Click **Actions**, and then select **CA Switch**.

The **CA Switch** pop-up window appears.



8. From the **Target CA** list, choose the desired CA to migrate.
9. **Note:** The Issuer Location and Issuer Name dropdown fields are displayed only when you are migrating to Google CA. This is because, for Google CA, one policy can contain several intermediary CAs.

   If you are migrating to the Google CA:
   a. From the **Issuer Location** dropdown list, select the issuer location.
   b. From the **Issuer Name** dropdown list, select the issuer name.
10. For migrating to other CAs, skip this step.
11. Enter **the Name** of the triggered migration.
12. Click **Save**
13. The **CA Switch Summary** page appears.



The following table describes the options available in the CA Switch Summary page:

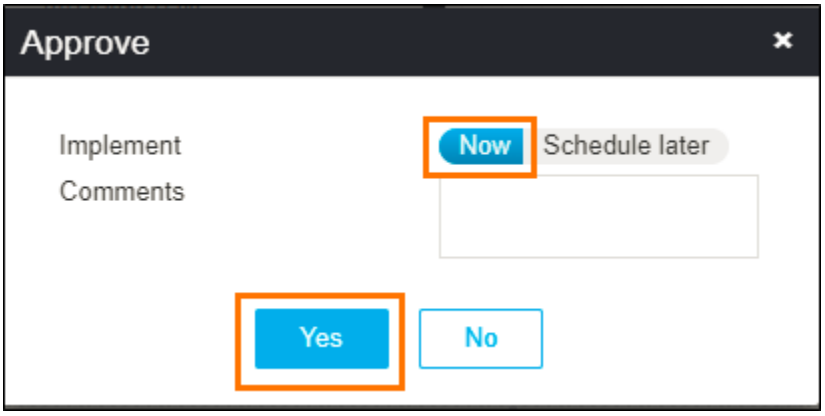
Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

14. In the check box column certificate list, select the desired certificate that you want to migrate.
15. In the **Common Name** column, click the eye icon to view certificate details.

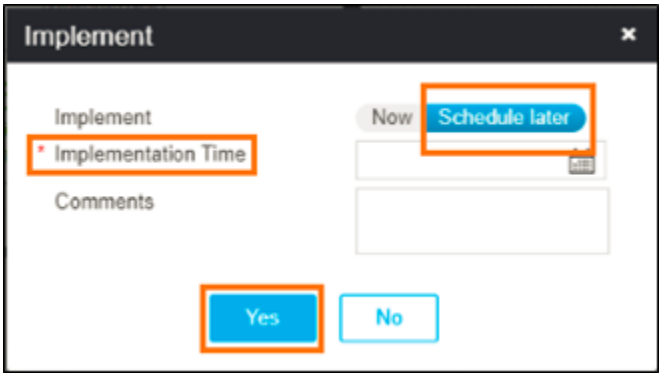
16. In the **CSR details** column, click **Update CSR** to review the details.
17. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
18. Click **Submit**.
19. Perform the required actions in the Work order column.

20. In the **Work order** column, click **Approve**.

    The **Approve** pop-up window appears.

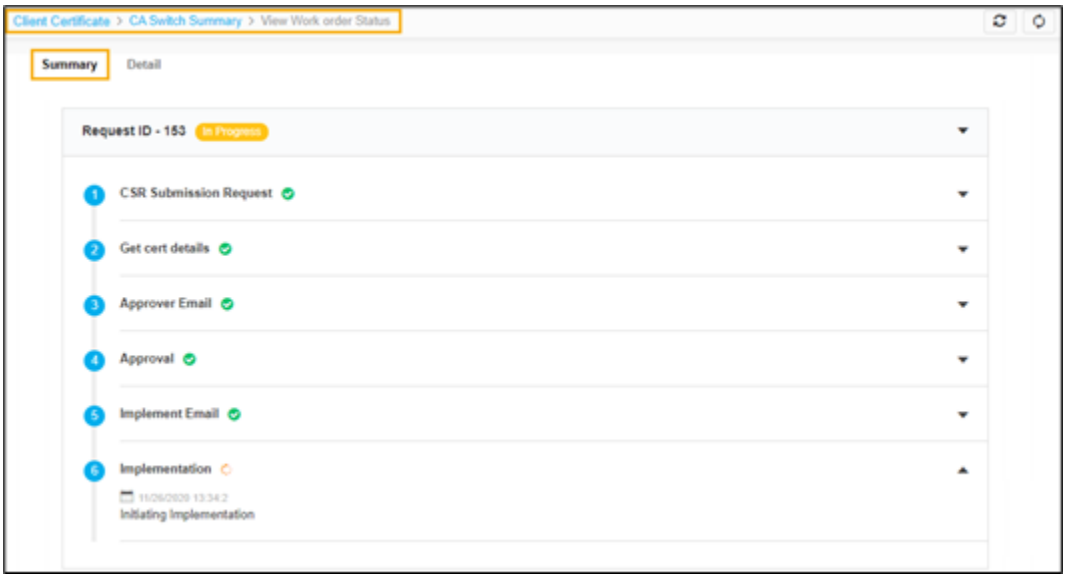


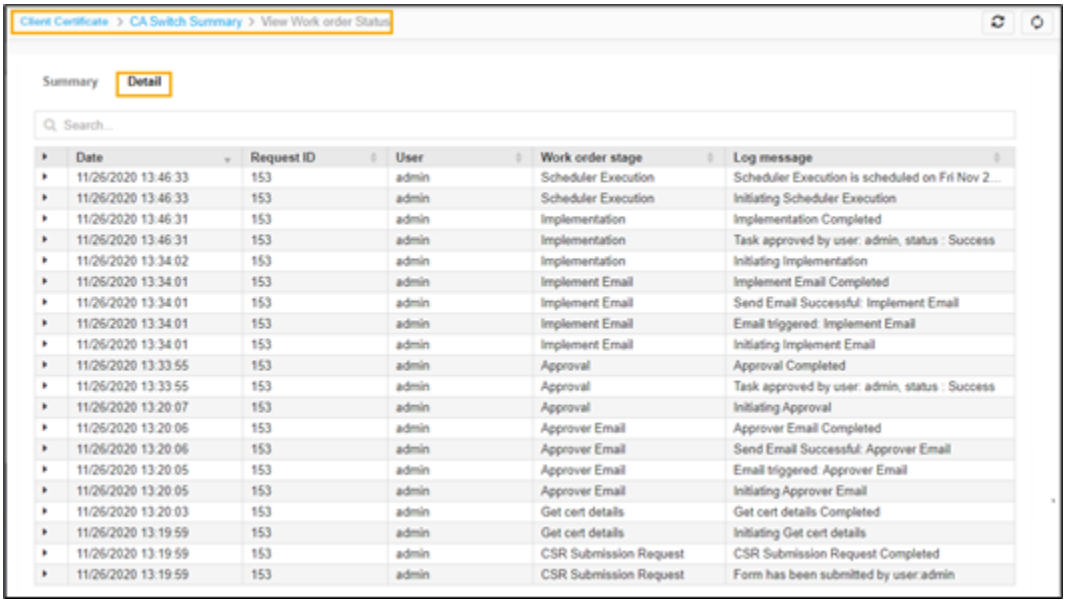
21. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.



22. Select the **Implementation Time** from the calendar field.
23. Enter the **Comments**.
24. Click **Yes**.
25. In the **Work order** column, click the status if you want to see the Summary and Details status of the progress.

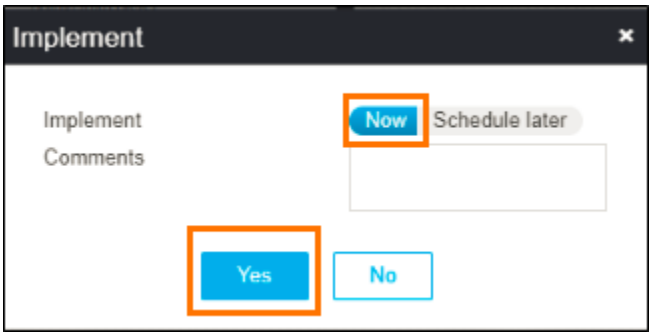
    The **View Work order Status** page appears.



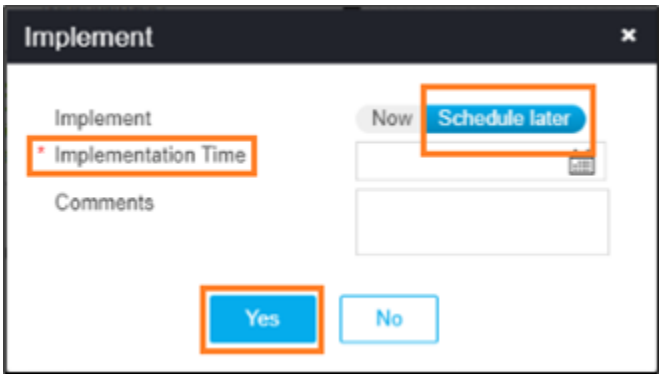


26. In the **Work order** column, click **Implement**.

    The **Implement** pop-up window appears.

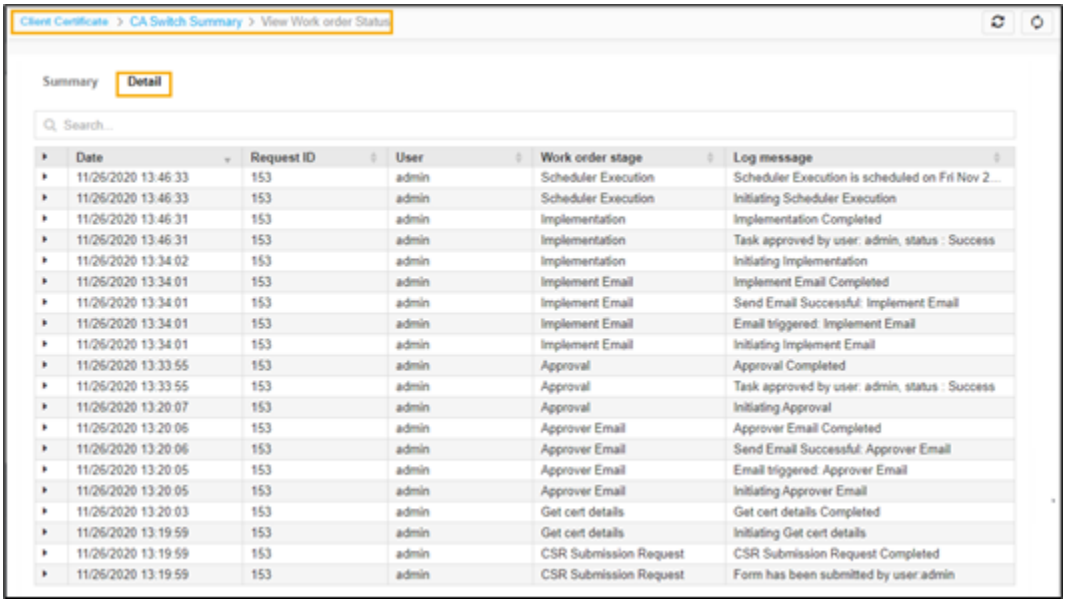


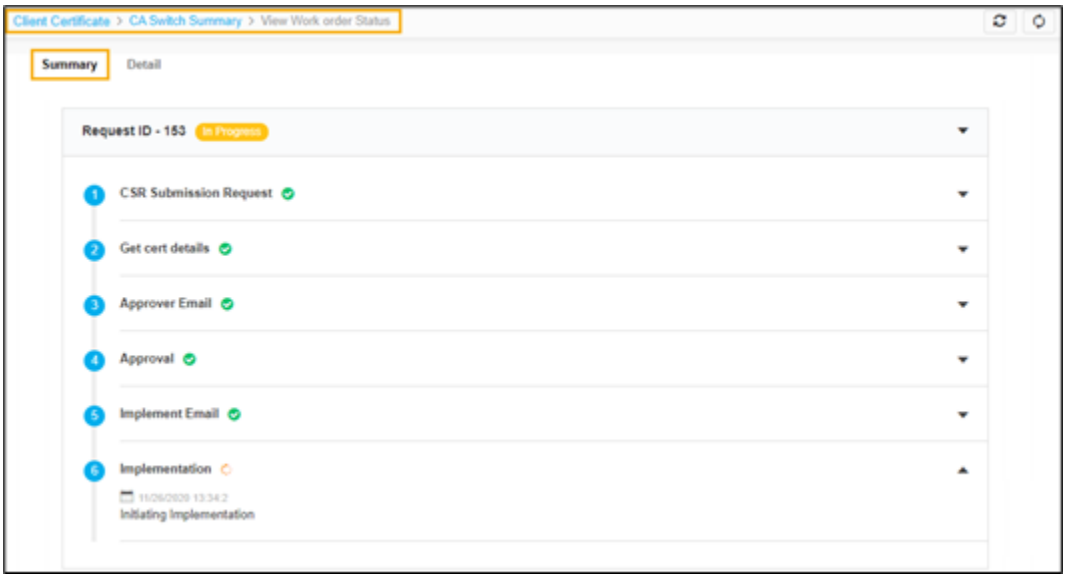
27. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



28. Select the **Implementation Time** from the calendar field.
29. Enter the **Comments** in the field.
30. Click **Yes**.
31. In the **Work order** column, click the status if you want to see the Summary and Details status of the progress.

    The **View Work order Status** page appears.



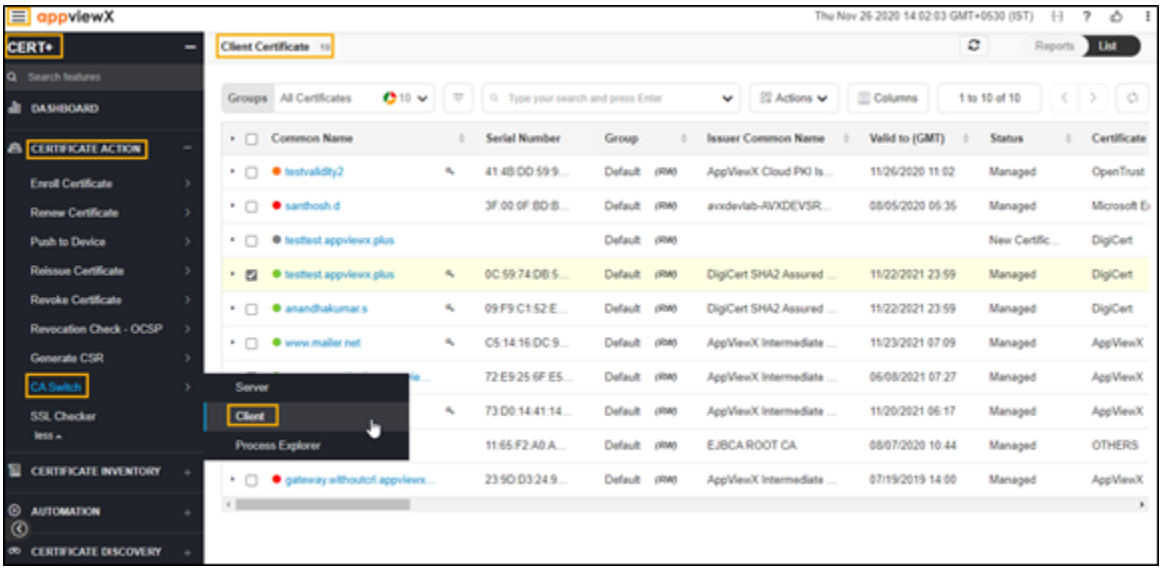


32. Click the refresh icon on the top-right of the page to update the Work Order status. After the CA Switch is completed, the Work order status changes to **Completed**.

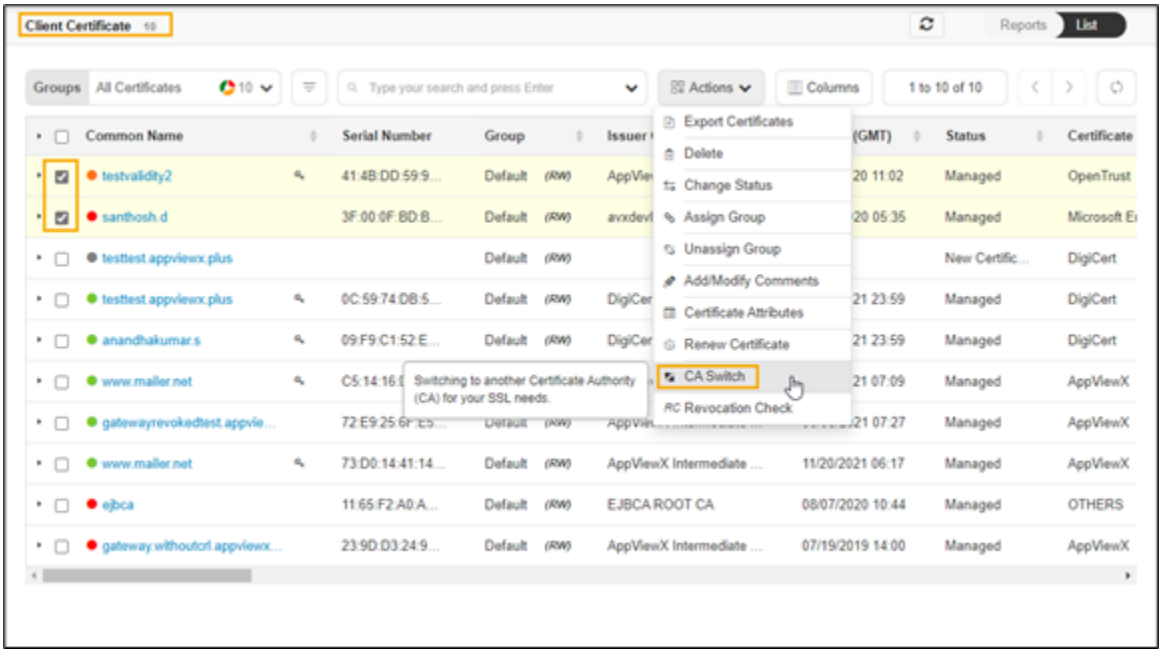
Migrating the CA for Client Certificate

To migrate the CA client certificate,

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 ACTION**.
5. Select **CA Switch**, and then **Client**.
   The **Client Certificate** page appears.

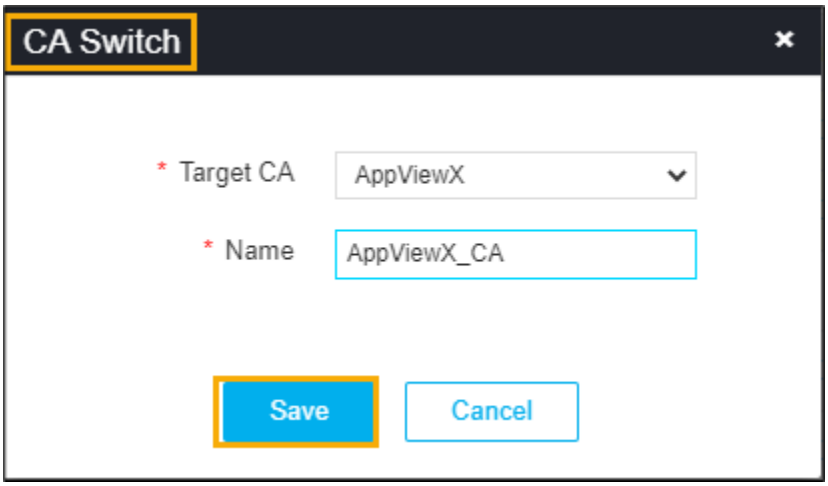


6. In the **Common Name** column certificate list, select the desired certificate that you want to migrate to the CA.



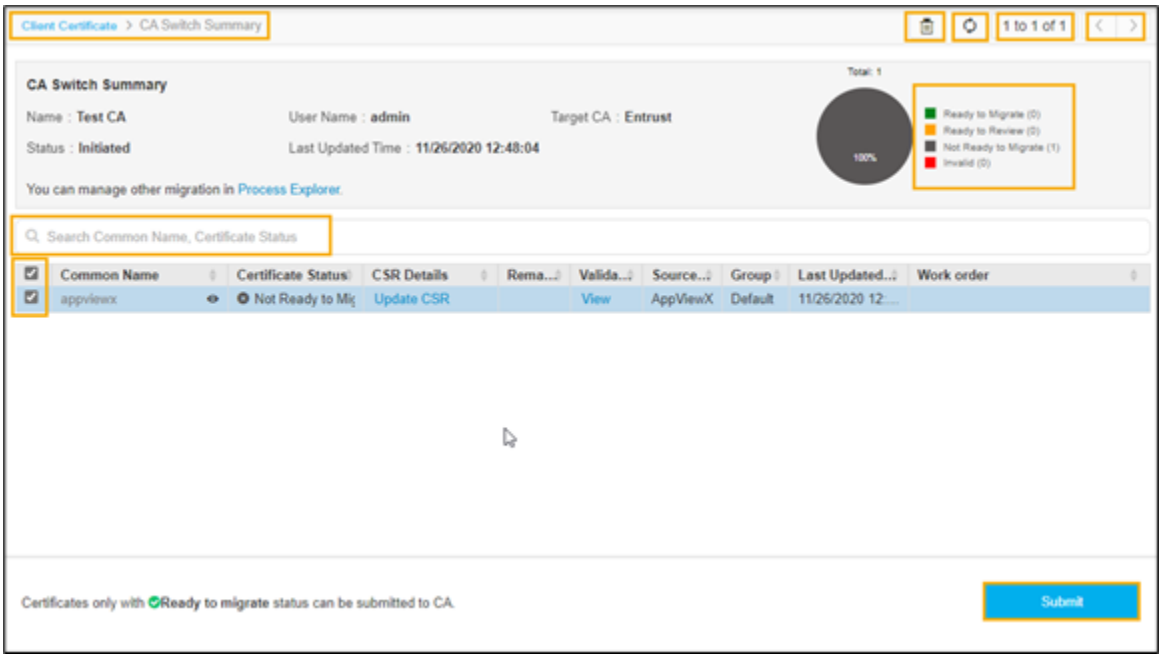
7. Click **Actions**, and then select **CA Switch**.

   The **CA Switch** pop-up window appears.



8. From the **Target CA** list, choose the desired CA to migrate.
9. **Note:** The Issuer Location and Issuer Name dropdown fields are displayed only when you are migrating to Google CA. This is because, for Google CA, one policy can contain several intermediary CAs.

   If you are migrating to the Google CA:
   a. From the **Issuer Location** dropdown list, select the issuer location.
   b. From the **Issuer Name** dropdown list, select the issuer name.
10. For migrating to other CAs, skip this step.
11. Enter **the Name** of the triggered migration.
12. Click **Save**
13. The **CA Switch Summary** page appears.



The following table describes the options available in the CA Switch Summary page:

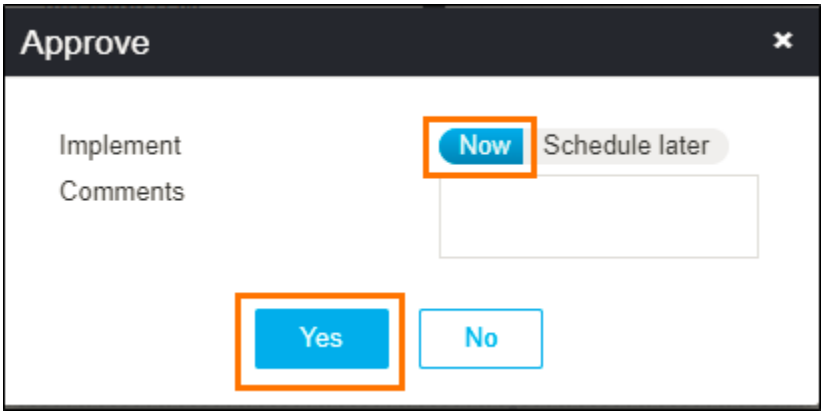
Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

14. In the check box column certificate list, select the desired certificate that you want to migrate.
15. In the **Common Name** column, click the eye icon to view certificate details.

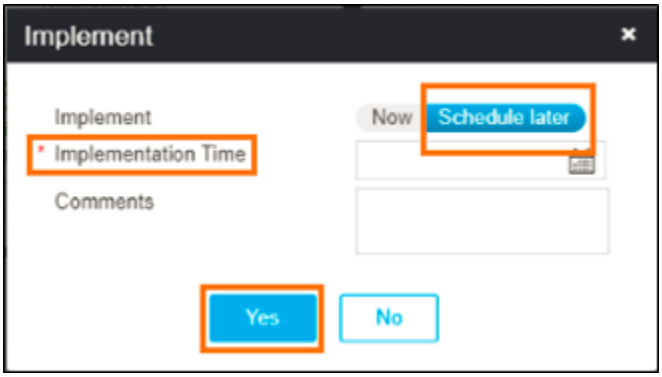
16. In the **CSR details** column, click **Update CSR** to review the details.
17. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
18. Click **Submit**.
19. Perform the required actions in the Work order column.

20. In the **Work order** column, click **Approve**.

    The **Approve** pop-up window appears.

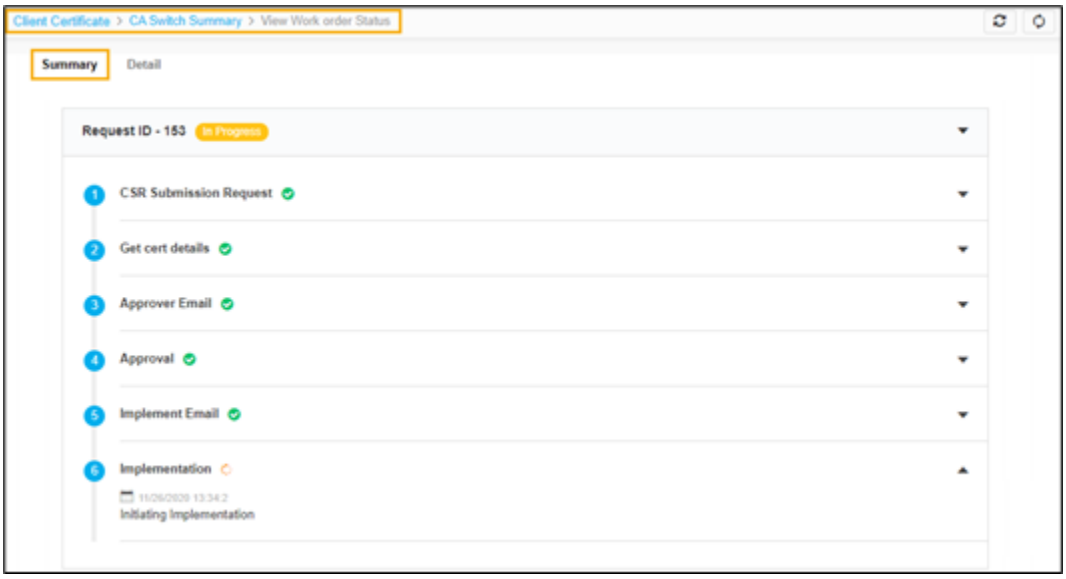


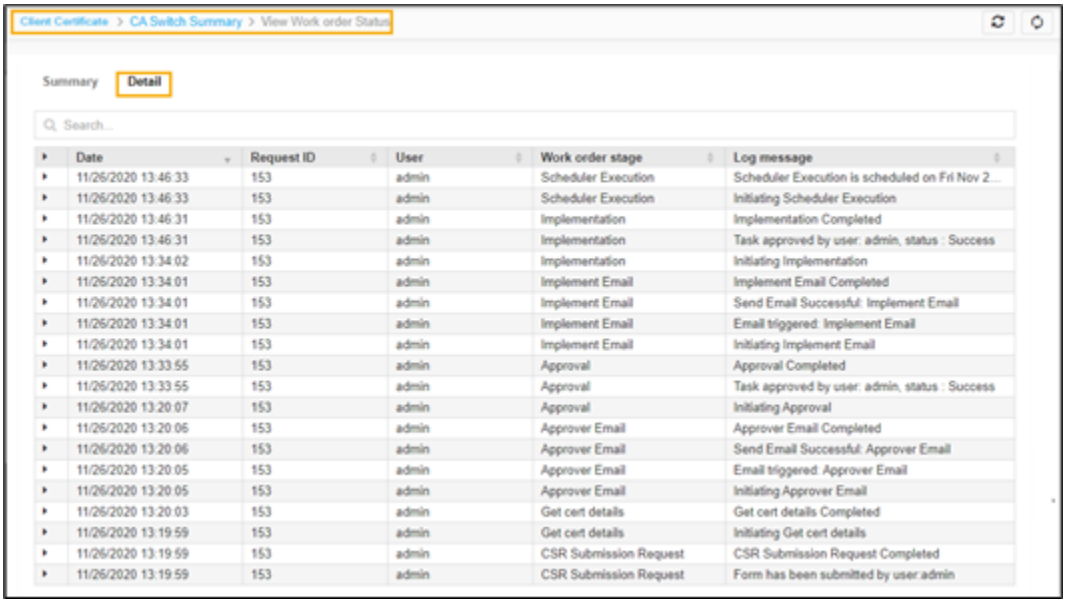
21. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.



22. Select the **Implementation Time** from the calendar field.
23. Enter the **Comments**.
24. Click **Yes**.
25. In the **Work order** column, click the status if you want to see the Summary and Details status of the progress.

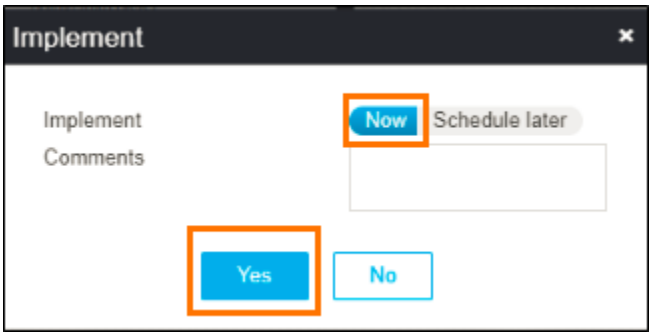
    The **View Work order Status** page appears.



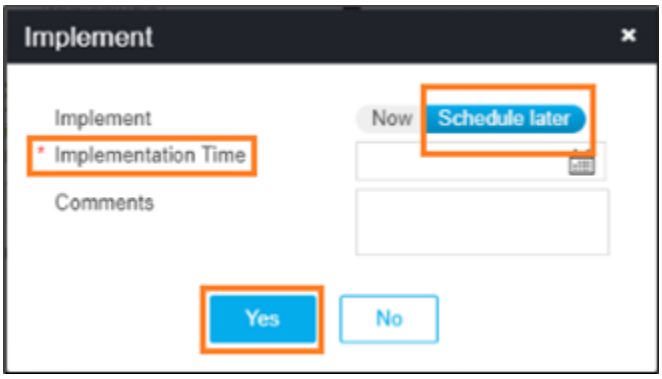


26. In the **Work order** column, click **Implement**.

    The **Implement** pop-up window appears.

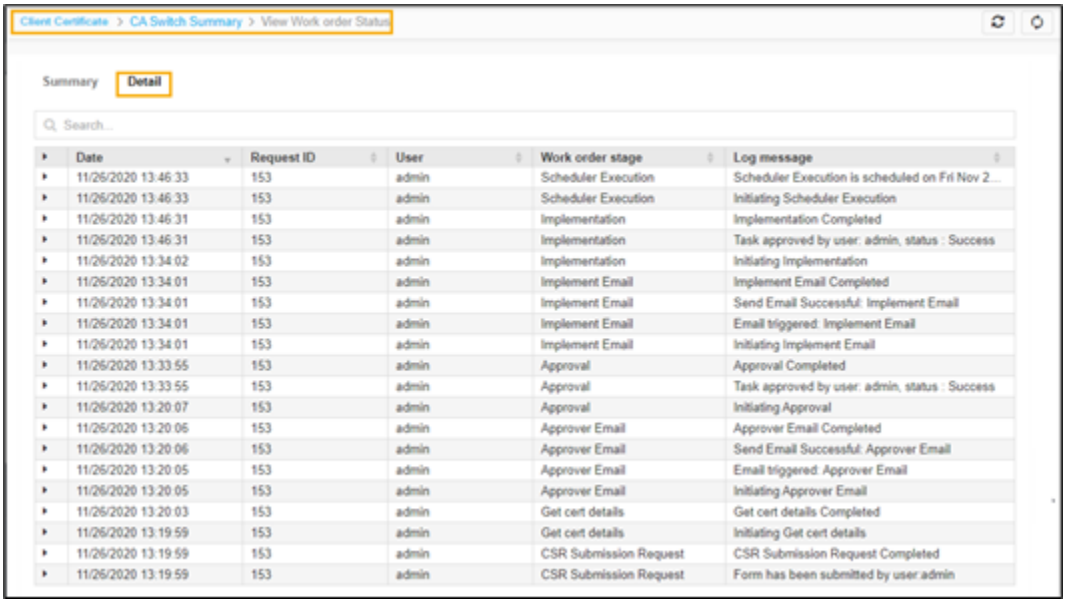


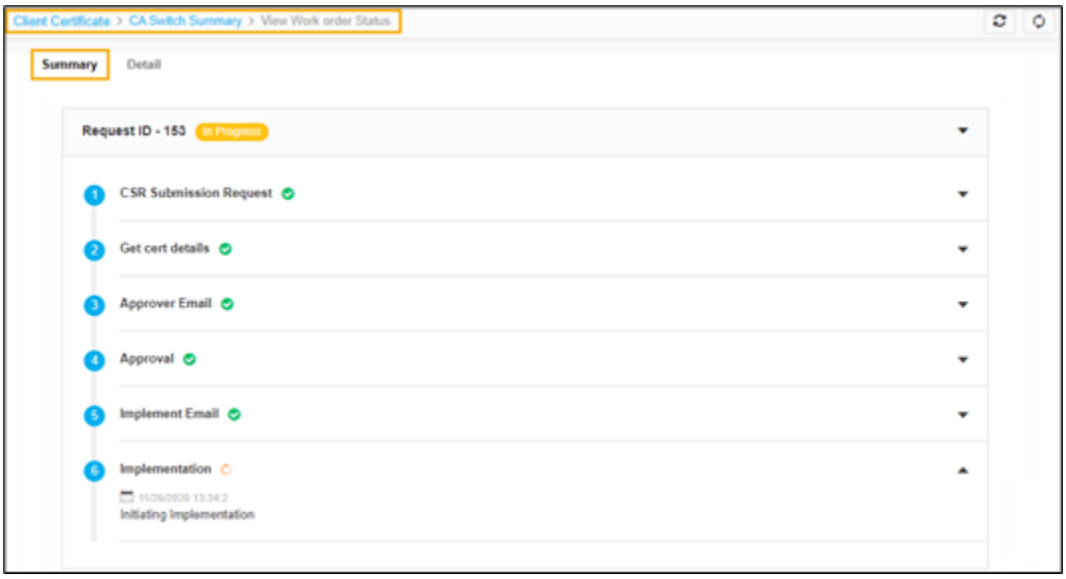
27. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.



28. Select the **Implementation Time** from the calendar field.
29. Enter the **Comments** in the field.
30. Click **Yes**.
31. In the **Work order** column, click the status if you want to see the Summary and Details status of the progress.

    The **View Work order Status** page appears.





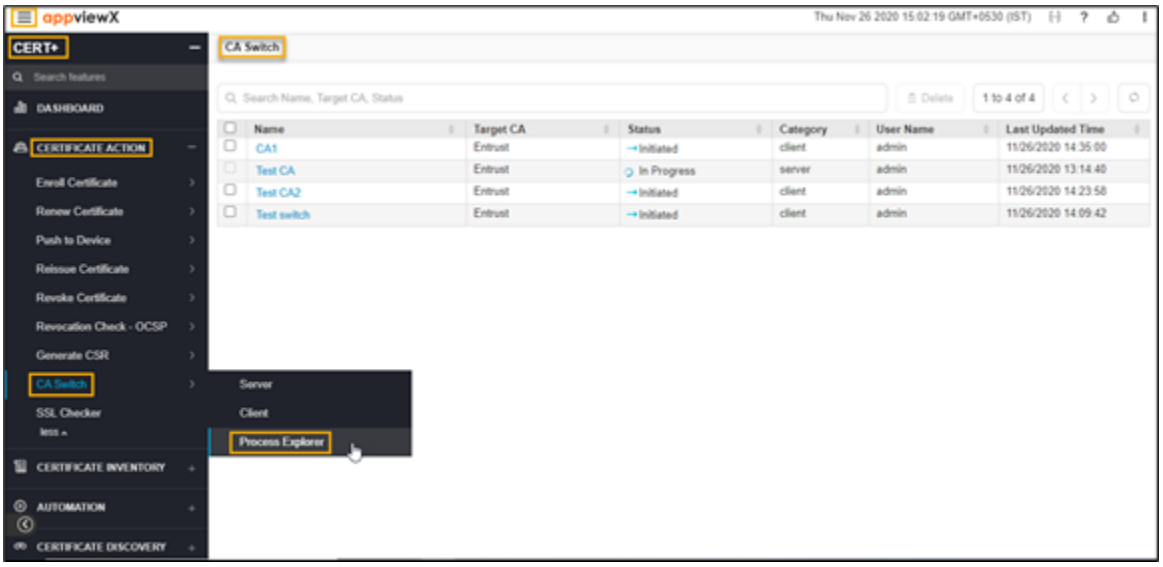
32. Click the refresh icon on the top-right of the page to update the Work Order status. After the CA Switch is completed, the Work order status changes to **Completed**.

Process Explorer

Whenever the bulk renewal and CA migration operations get performed, in the process explorer window, the status of every certificate will be shown according to the operation done. The user is allowed to verify and modify the data from the process explorer as well.

To perform process explorer,

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 ACTION**.
5. Select **CA Switch**, and then **Process Explorer**.



The **Process Explorer** page appears.

SSL Checker

SSL certificate deployment can be validated using the SSL checker feature in AppViewX. This validates the SSL certificate deployment, trustchain, ciphersuites, and supported TLS versions for a given service endpoint.

- Running SSL Checker for Certificate

Running SSL Checker for Certificate

To run SSL checker on a certificate,

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 ACTION**.
5. Click **SSL Checker**.

The **SSL Checker** page appears.

The following table describes the options available in the SSL Checker page:

Options	Description
FQDN	Enter the fully qualified domain name (FQDN) in the field.
IP address: Port	Enter the valid IP address with the port number.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.

6. Click **Add**
7. Click **Validate** to run SSL checker.

Chapter 5: Certificate Inventory

Overview

The Certificate Inventory allows you to take inventory of, and proactively manage all your certificates. This will be a single source of truth for all the certificates in the organization. Every certificate action can be performed from the inventory.

Benefits

- Take inventory of all your digital certificates
- Keeps you informed of impending expirations
- Creates certificate tasks via workflows to renew expiring certificates
- Creates incidents for already expired certificates
- Prioritizes certificate importance
- Helps you proactively manage your certificates
- Helps you avoid manually tracking a large volume of certificates
- Prevents security breaches due to expired or expiring certificates

In the Certificate Inventory section, you can:

- enroll a certificate
- renew a certificate

- push to device
- reissue a certificate
- revoke a certificate
- regenerate a certificate
- reinstate a certificate
- revocation check
- upload a certificate
- download a certificate.

Server Certificate Inventory

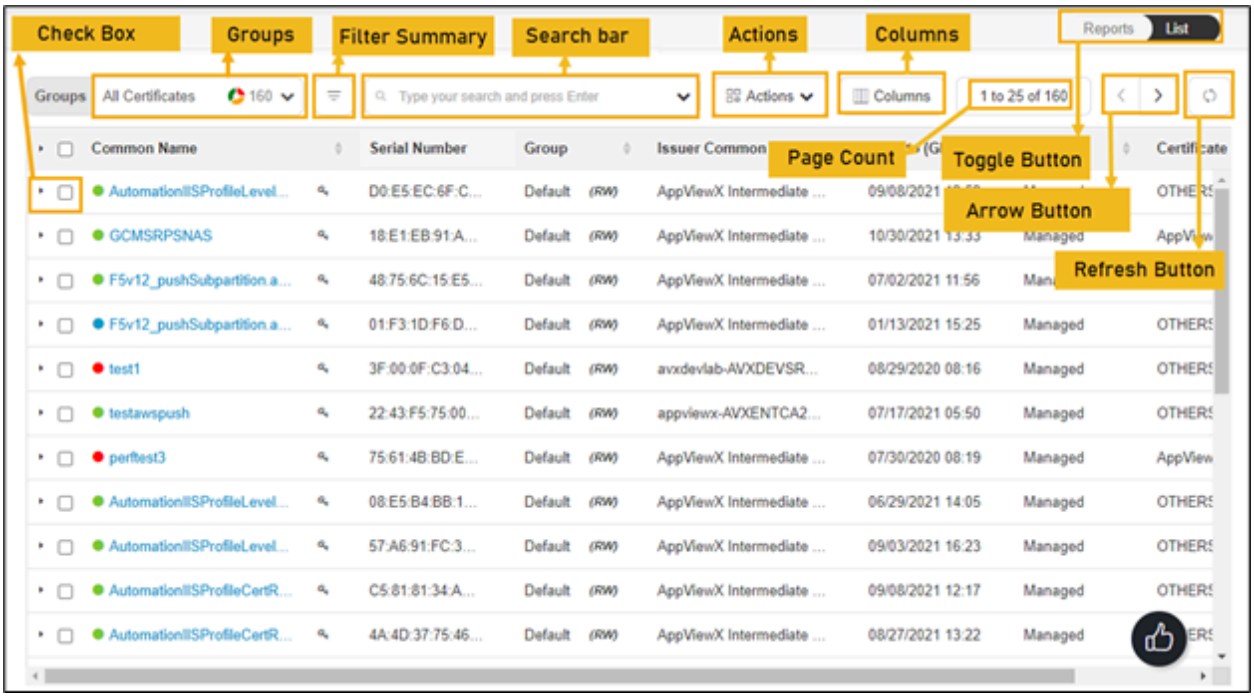
Overview

Server certificate inventory is where all the server certificates with the EKU (Extended/enhanced Key Usage) Server and Client authentication will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificate renewal, bulk certificates CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

In the **Certificate Inventory** > **Server Certificate** page, all the server certificates are listed. You can perform the following actions:

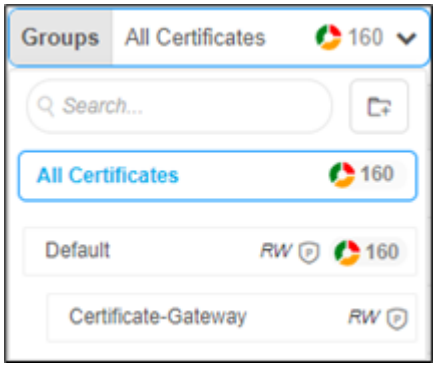
- Export Certificates - To export the server certificate.
- Delete - To delete the server certificate.

- Change Status - To change the server certificate status.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To Unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.
- Certificate Attributes - To update the certificate attributes.

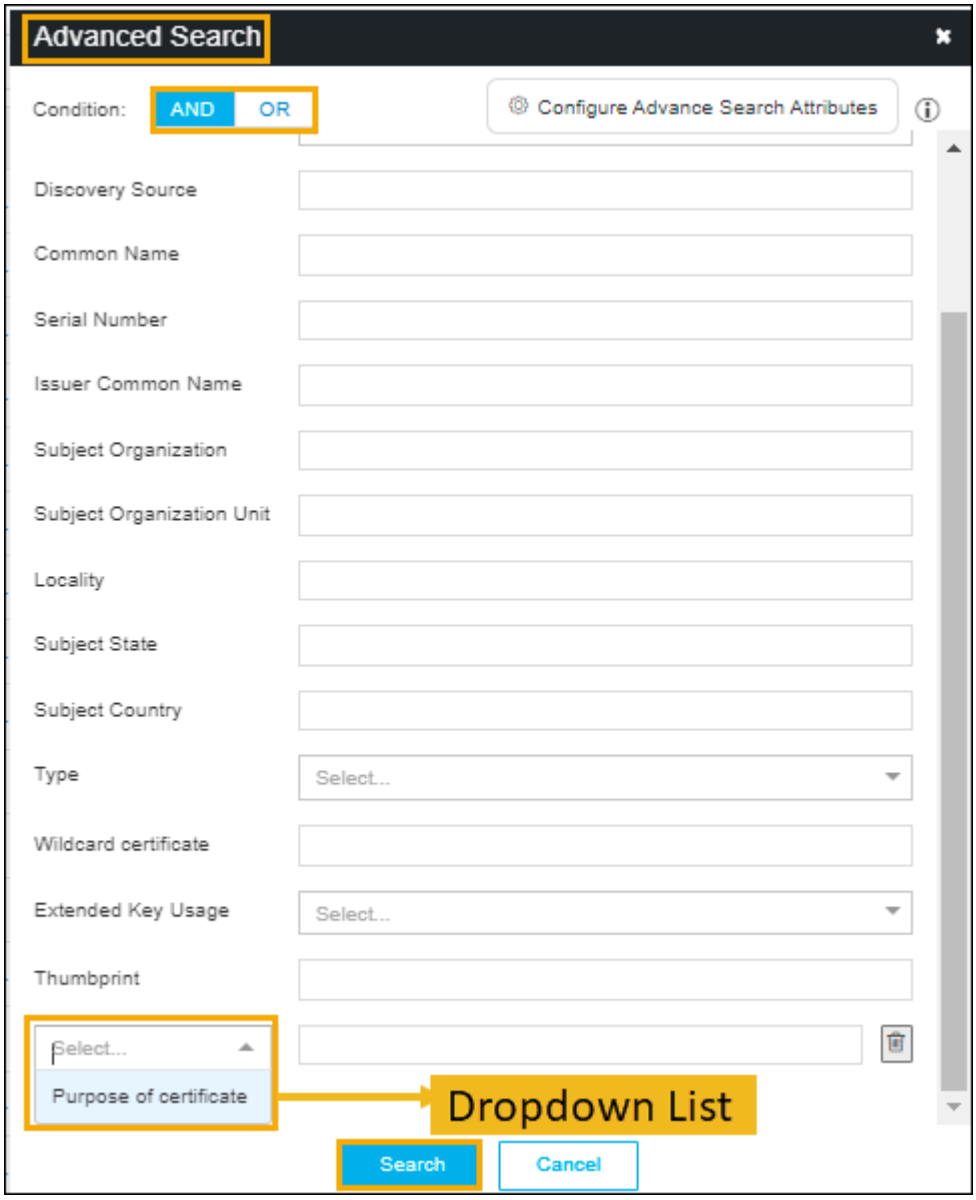


The following table describes the options available on the server certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected.

Options	Description
	
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

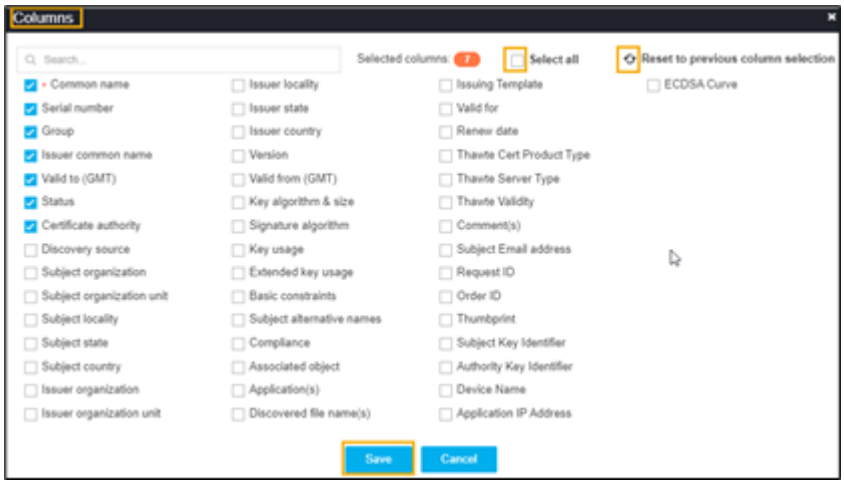


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

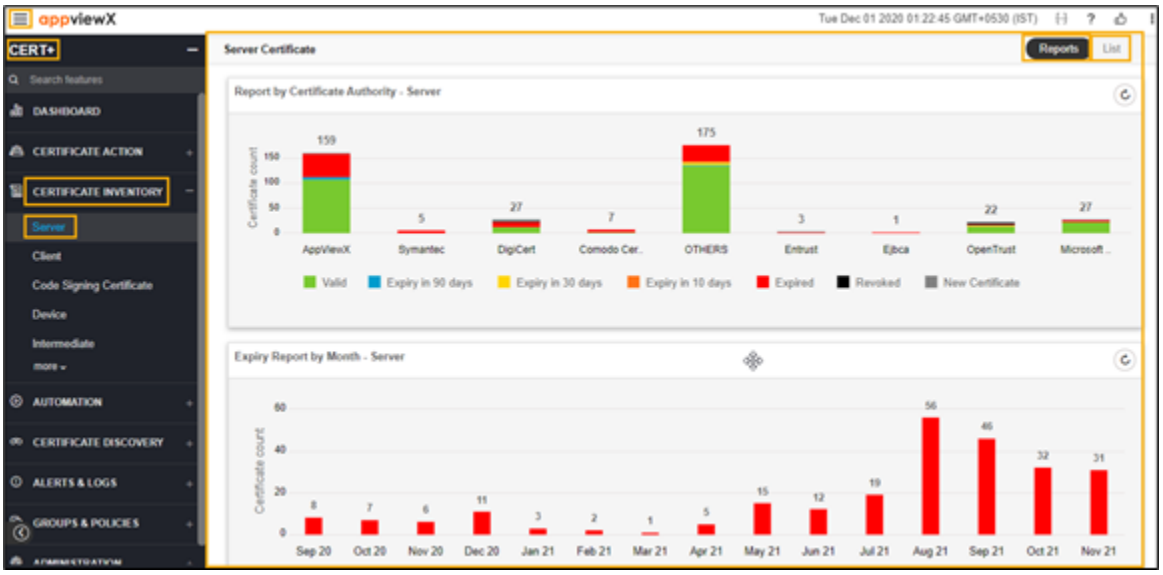
Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Exporting Server Certificate

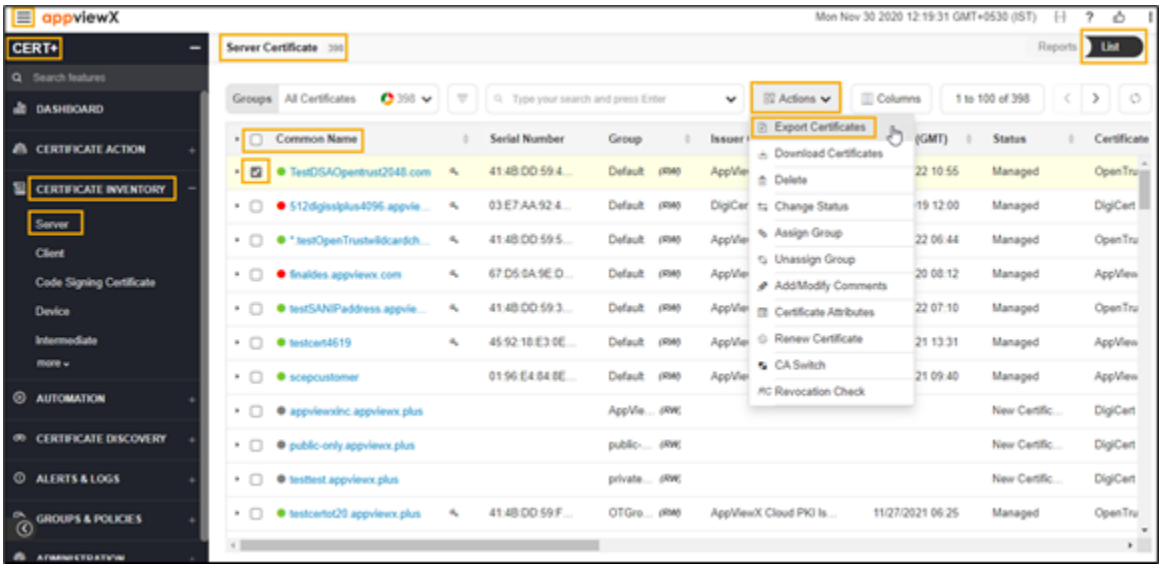
Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in <.xls> or <.csv> format. This can be used for reporting or making another inventory.

To export server certificate,

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. Click **Server**.
   The **Server Certificate** page appears.

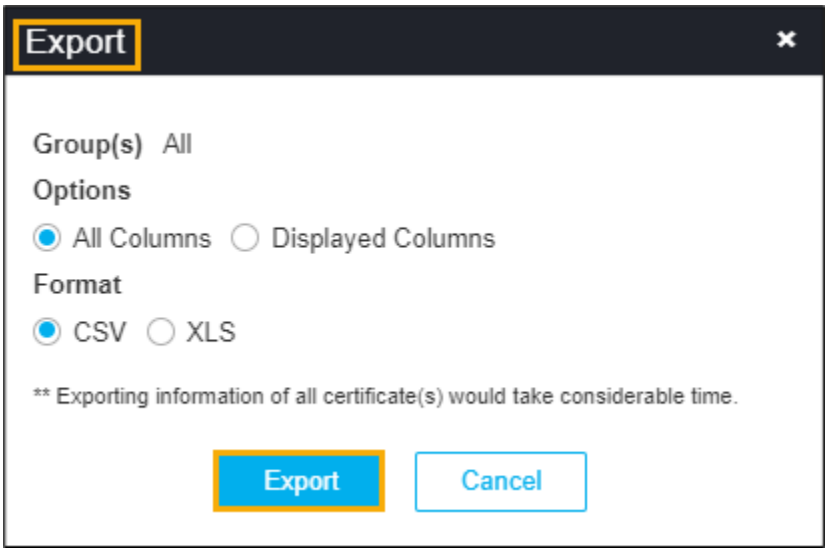


6. Click the **List** toggle button on the right top corner of the server certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to export a certificate.
8. Click **Actions**, and then select **Export Certificates** from the list.

   The **Export** pop-up window appears.



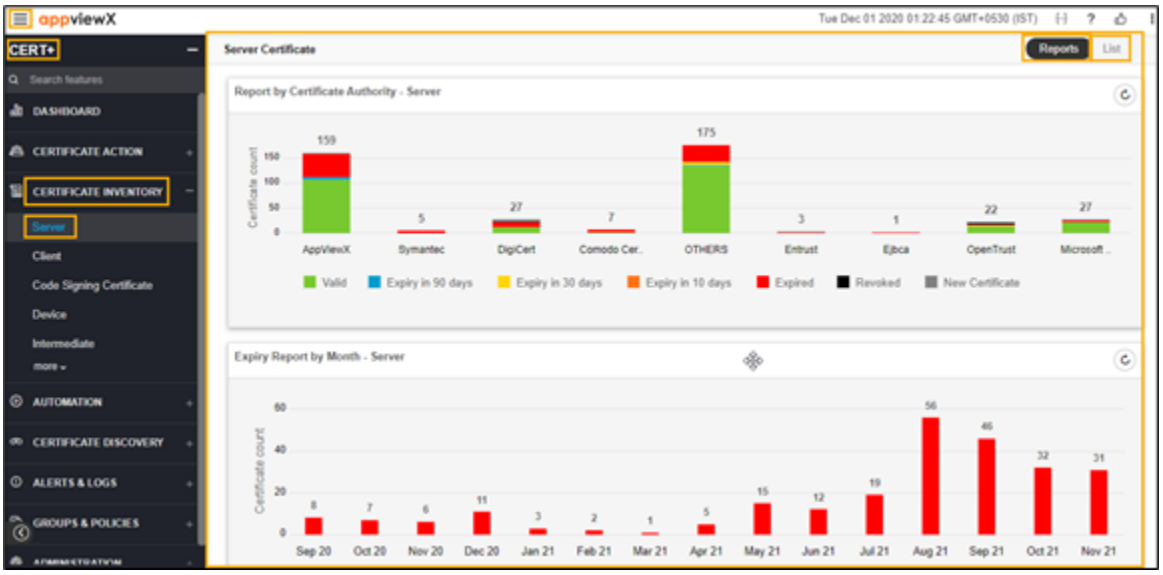
9. Select the desired **Options** and **Format** in the **Export** pop-up window.
   The selected certificate is exported to your local machine.

Deleting Server Certificate

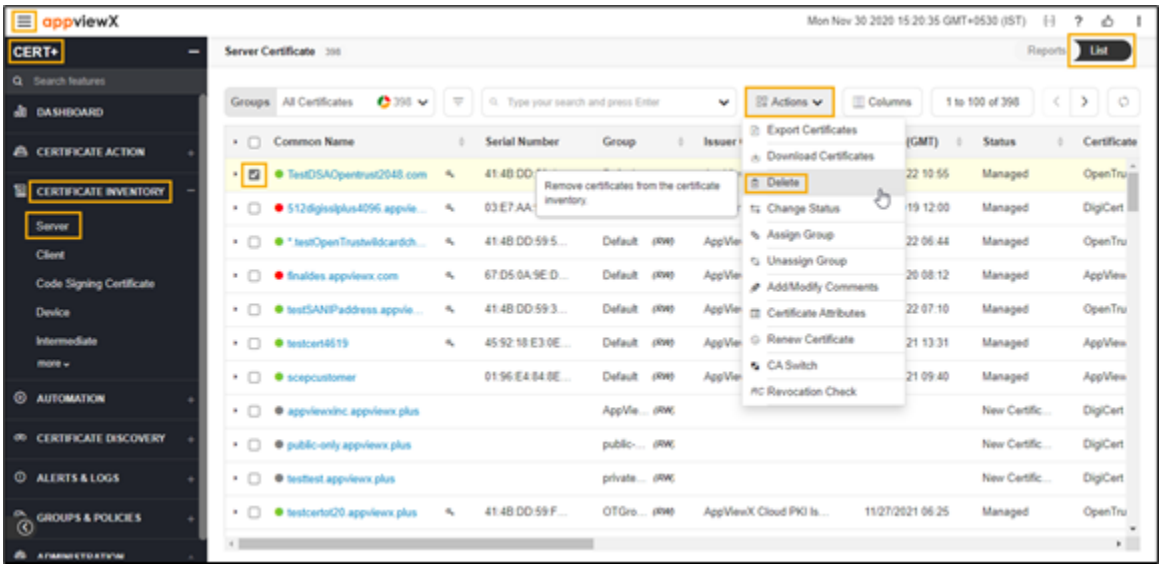
Deleting server certificate feature allows you to delete a certificate from the server certificate inventory only in AppViewX. Once the certificate gets deleted from the inventory, the same will not be shown in the reports and for alerts.

To delete server certificate,

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. Click **Server**.
   The **Server Certificate** page appears.

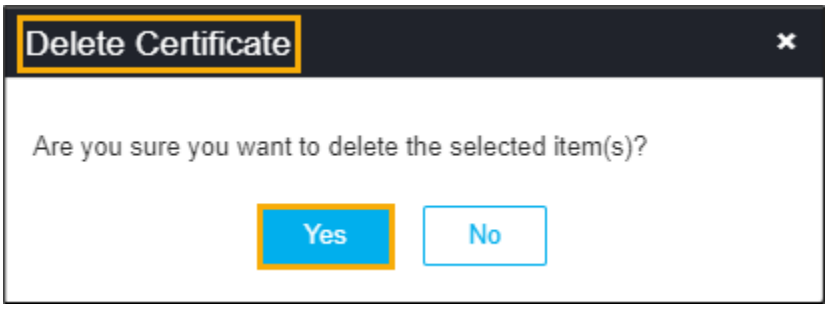


6. Click the **List** toggle button on the right top corner of the server certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to delete.
8. Click **Actions**, and then select **Delete** from the drop-down list.

   The **Delete** pop-up window appears.



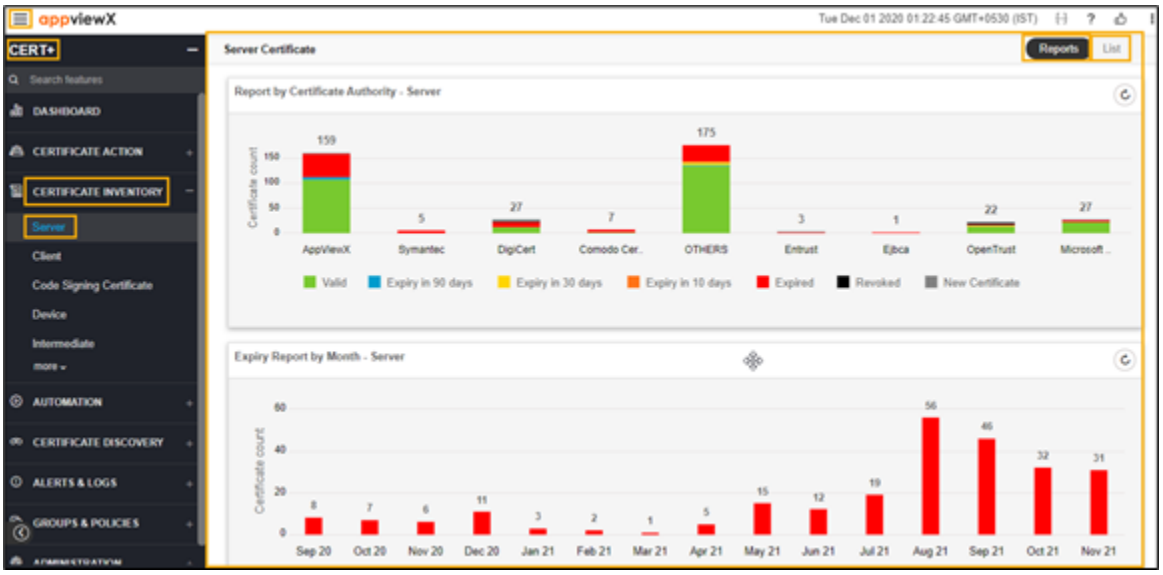
9. Click **Yes**.
   The server certificate is deleted and the pop-up message appears as "**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**".

Deleting Server Certificates via Holistic View

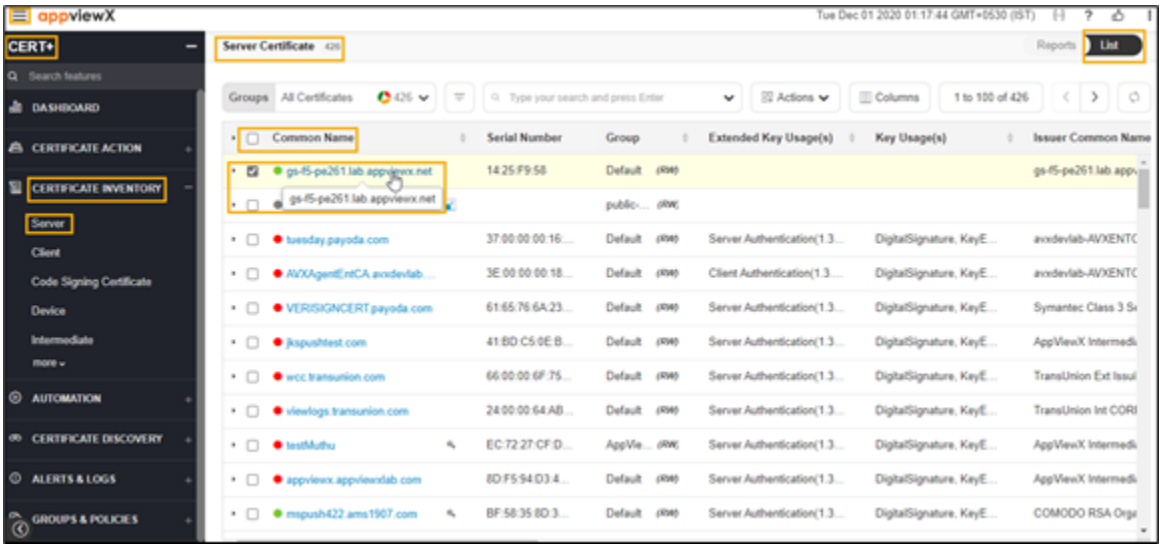
In the Holistic view, the user will find the entire chain of trust of the certificates along with the devices/ objects with which the certificates are associated. The primary actions that can be performed from the holistic view are Certificate creation, renewal, reissue, revoke, regenerate, install the certificates to the devices and objects. The other supported actions in the holistic view are download certificates and private keys, delete the certificate in the AppViewX certificate inventory, perform rollback action on the associated certificate and disassociate the certificate from the objects in the device.

To delete a server certificate via holistic view,

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. Click **Server**.
   The **Server Certificate** page appears.



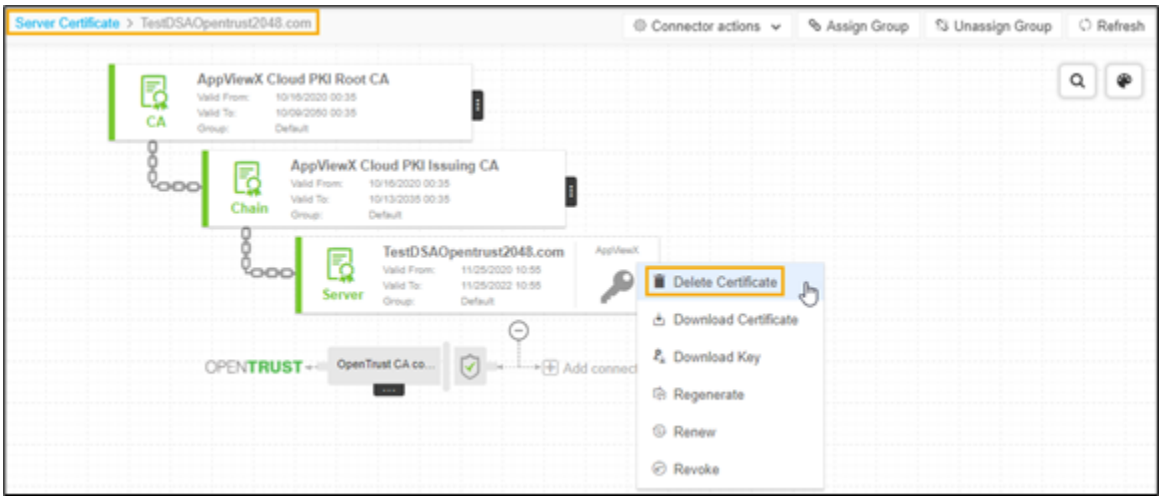
6. Click the **List** toggle button on the right top corner of the server certificate page.



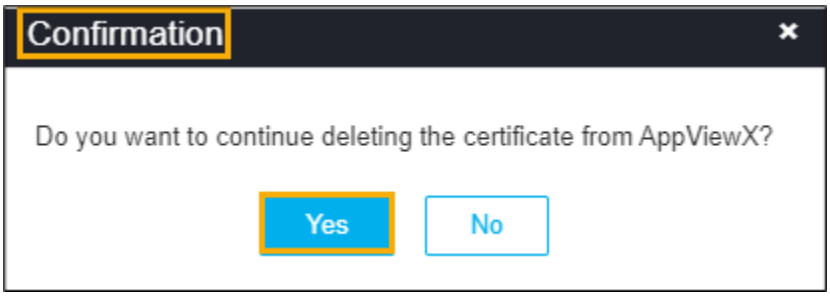
7. In the **Common Name** column certificate list, select the desired certificate that you want to delete the CA.

   The holistic view appears.

8. Click vertical eclipse in the holistic view, and then select **Delete Certificate** from the list.



The **Delete Certificate** pop-up window appears.



9. Click **Yes**.

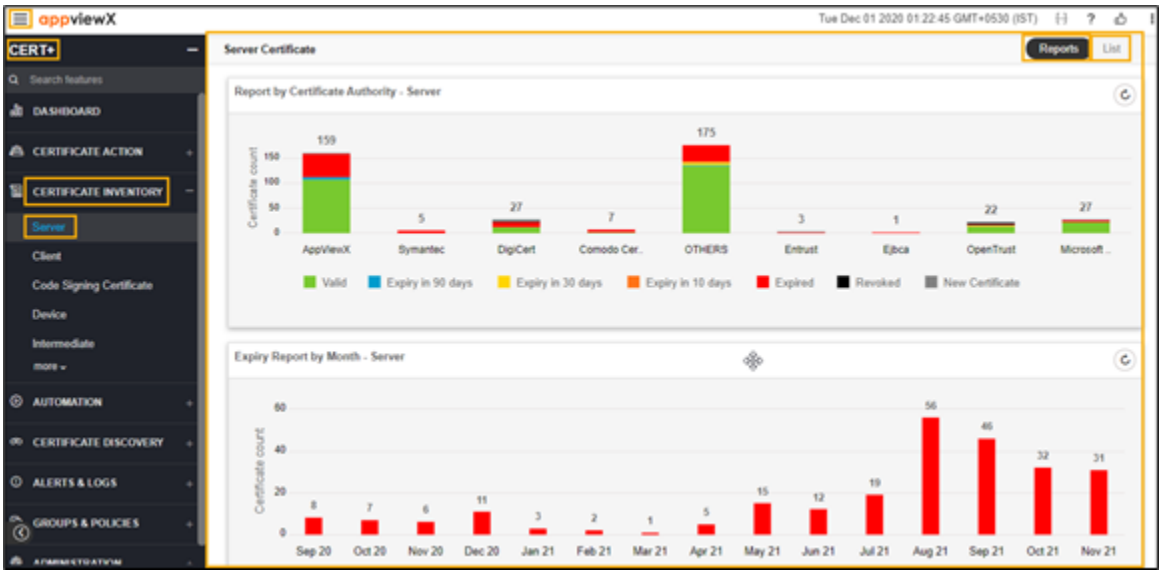
   The server certificate is deleted and the pop-up message appears as **Selected certificate(s) with RW permission has been deleted from AppViewX inventory**.

Changing Client Certificate Status

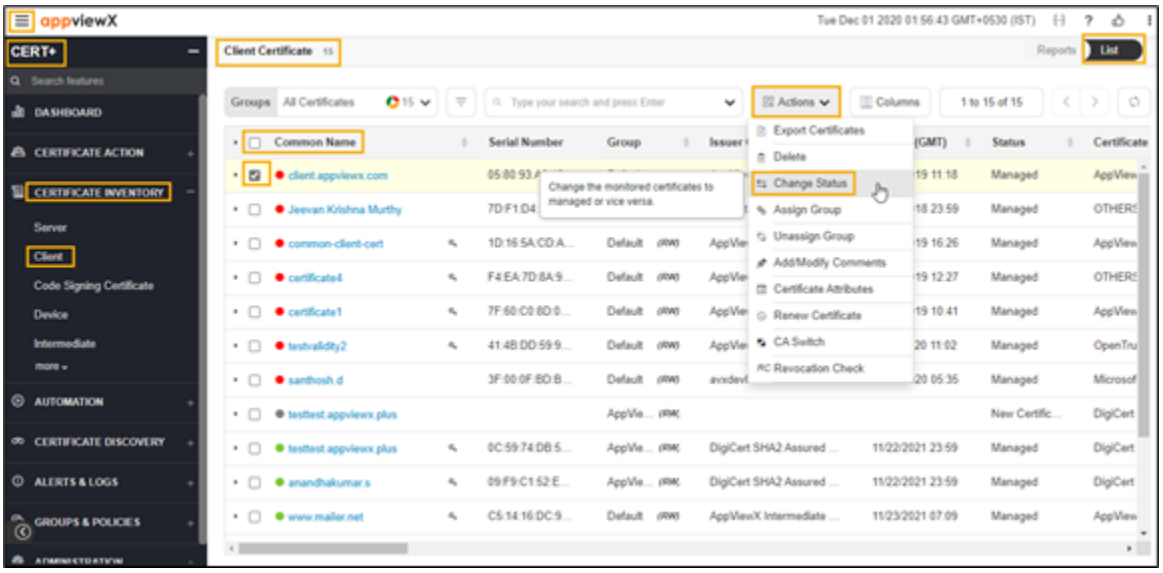
The certificate status can be set as monitored/managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, only viewing of the certificate details in terms of reports and inventory provided with alerting mechanisms can be done. When the certificates are set as Managed, the certificates-related actions along with push/bind operation can be performed along with viewing of the certificates in the reports and inventory.

To change the Client certificate status,

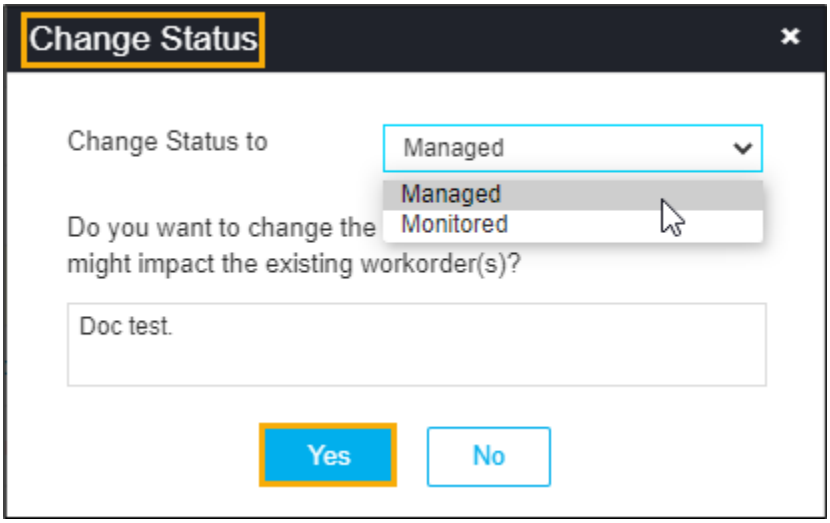
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.
   The **Client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



6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to change the certificate status.
8. Click **Actions**, and then select **Change Status** from the drop-down list.
   The Change Status pop-up window appears.



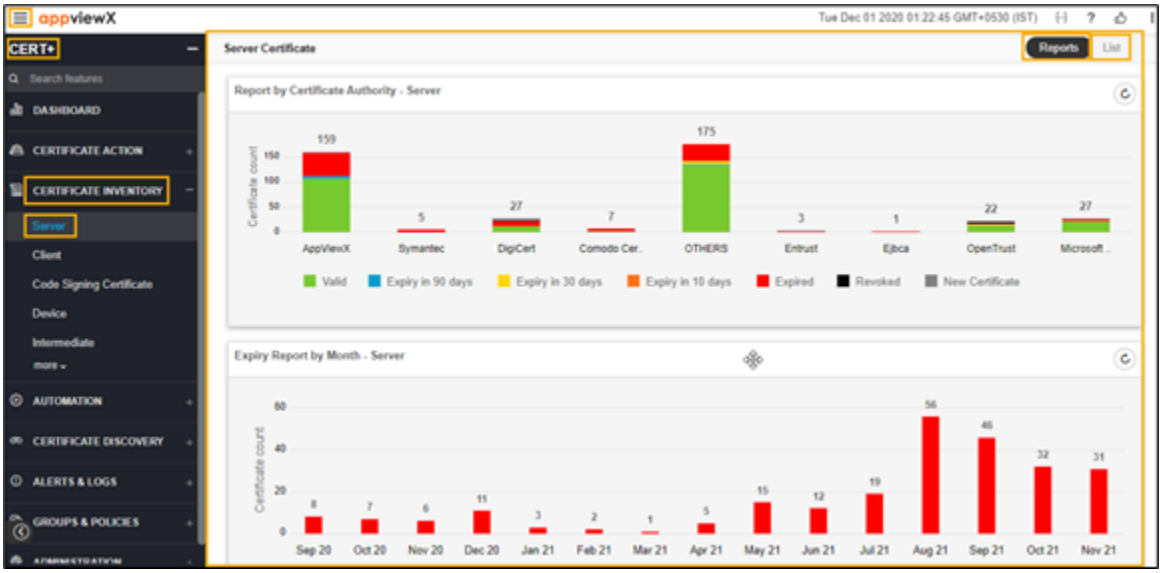
   a. Select the desired status from the **Change Status to** drop-down list.
   b. Enter the reason for changing the status in the description field.
   c. Click **Yes**.
9. The certificate status is changed to Managed or Monitored as selected from the drop-down list.
   The pop-up message appears as **Updated**.

Assigning Server Certificate Group

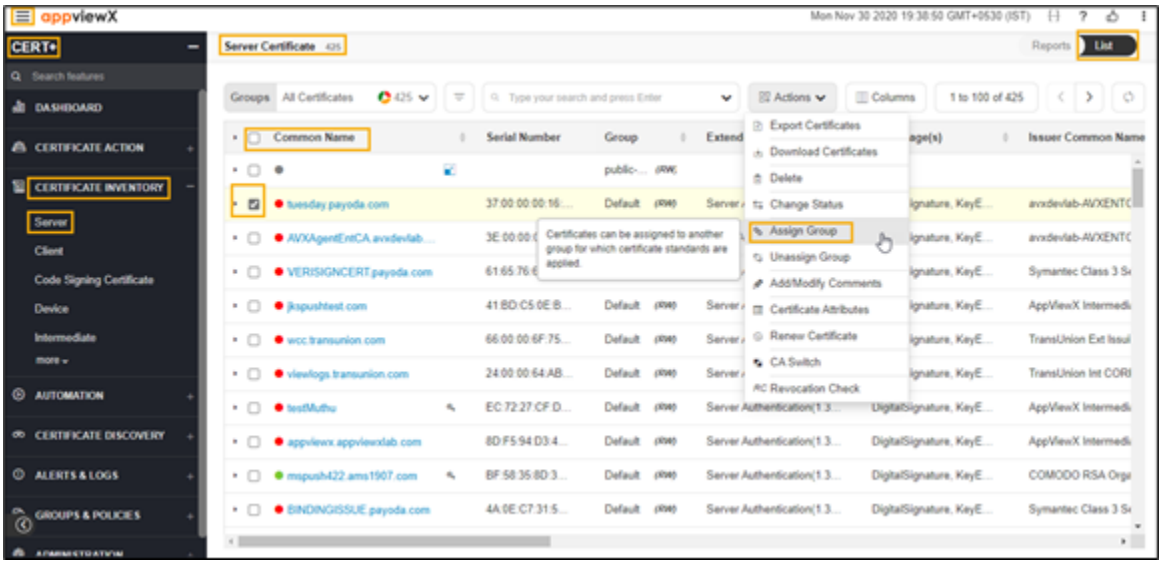
The certificates of any common criteria can be grouped together to perform compliance checks against the policy details, to enable auto-renewal and auto-push operations. The viewing of the certificates can also be done on a group basis.

To assign server certificate group,

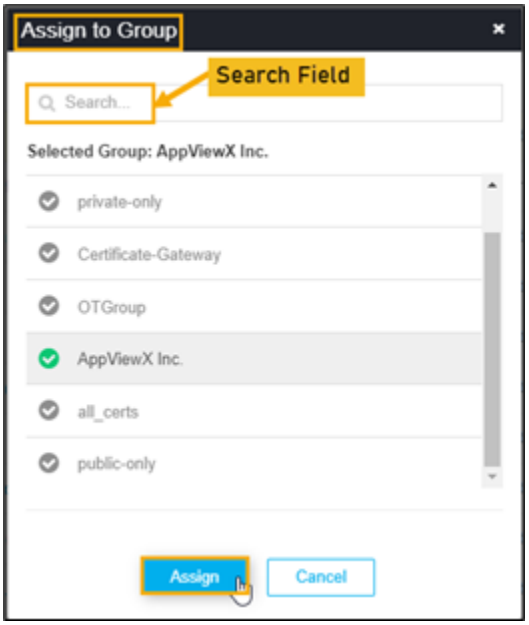
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**. The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Server**.
   The **Server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



6. Click the **List** toggle button on the right top corner of the server certificate page.



7. In the **Common Name** column certificate list, select the desired certificate(s) that you want to assign the certificate group.
8. Click **Actions**, and then select **Assign Group** from the drop-down list.
   The **Assign Group** pop-up window appears.



   a. Enter keywords if you want to search for a specific group from the list.
   b. Select the desired group from the listed groups.

c. Click **Assign**.

The pop-up message appears as **<certificate_name> assigned to <group_name>**.

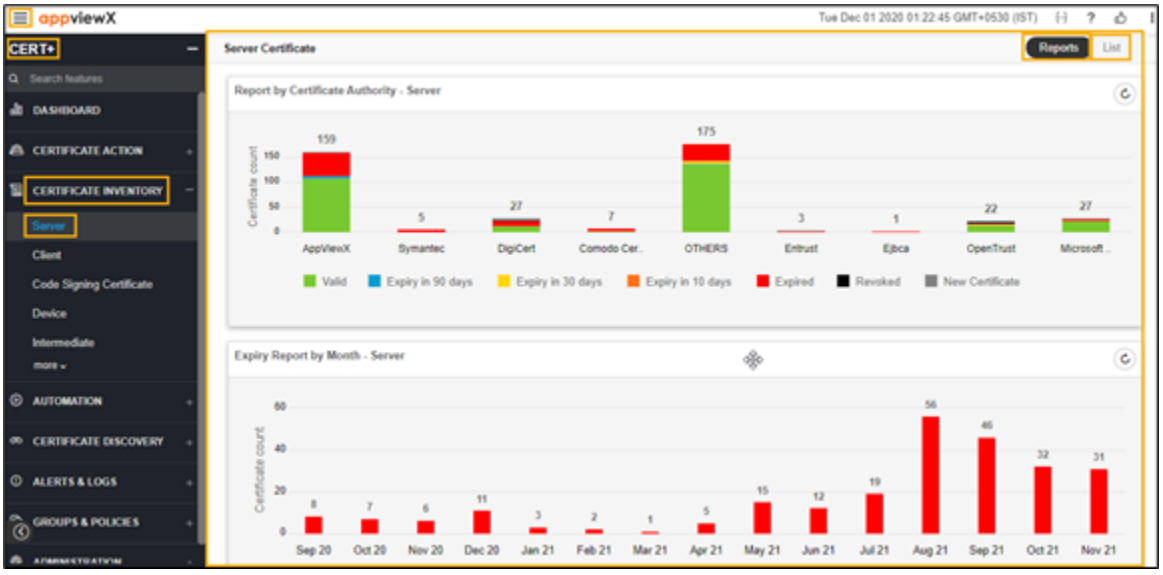
9. The certificate is assigned to a selected group.

Unassigning server Certificate Group

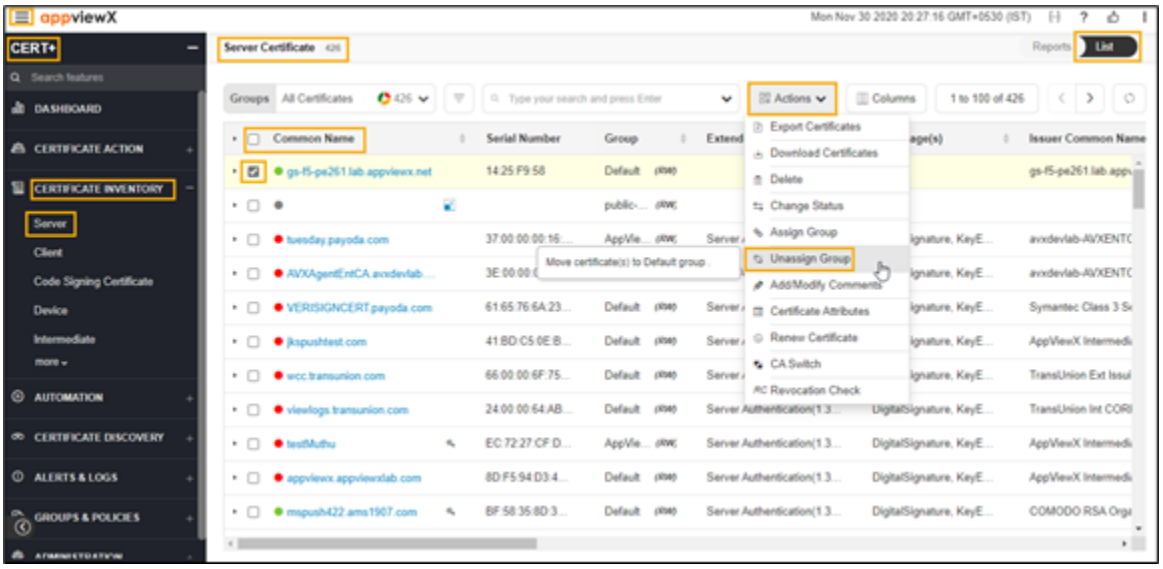
The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign server 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. Expand **CERTIFICATE INVENTORY**.
5. Click **Server**.
   The **Server Certificate** page appears.



6. Click the **List** toggle button on the right top corner of the server certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to unassign the certificate group.
8. Click **Actions**, and then select **Unassign Group** from the drop-down list.
9. The selected certificate is assigned to the default group. The pop-up message appears as **<certificate_name> assign to undefined**.

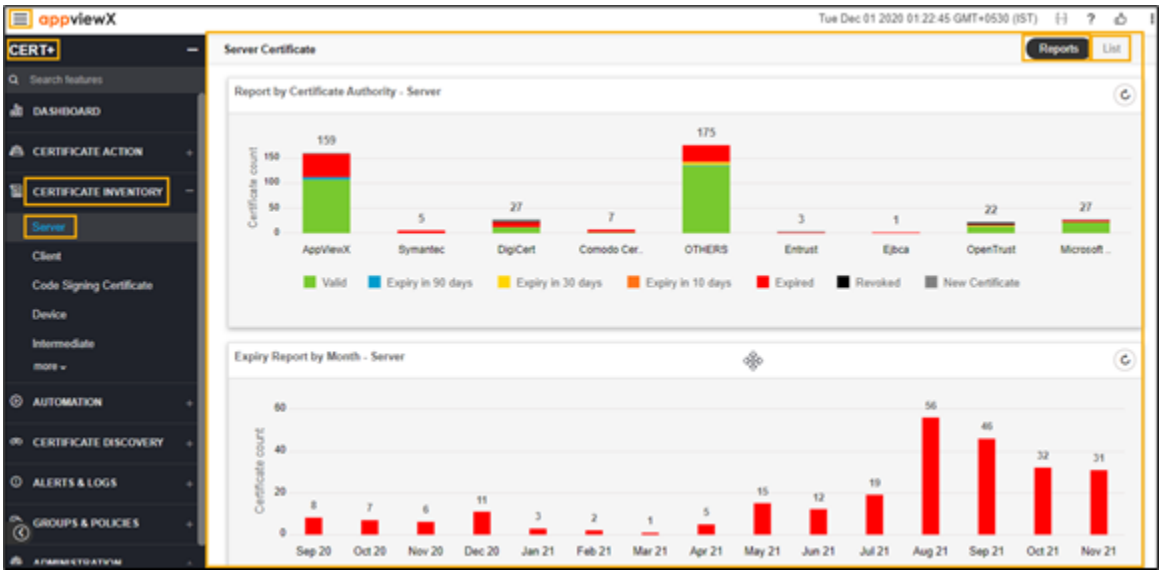
Bulk Server Certificate Revoke Action

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

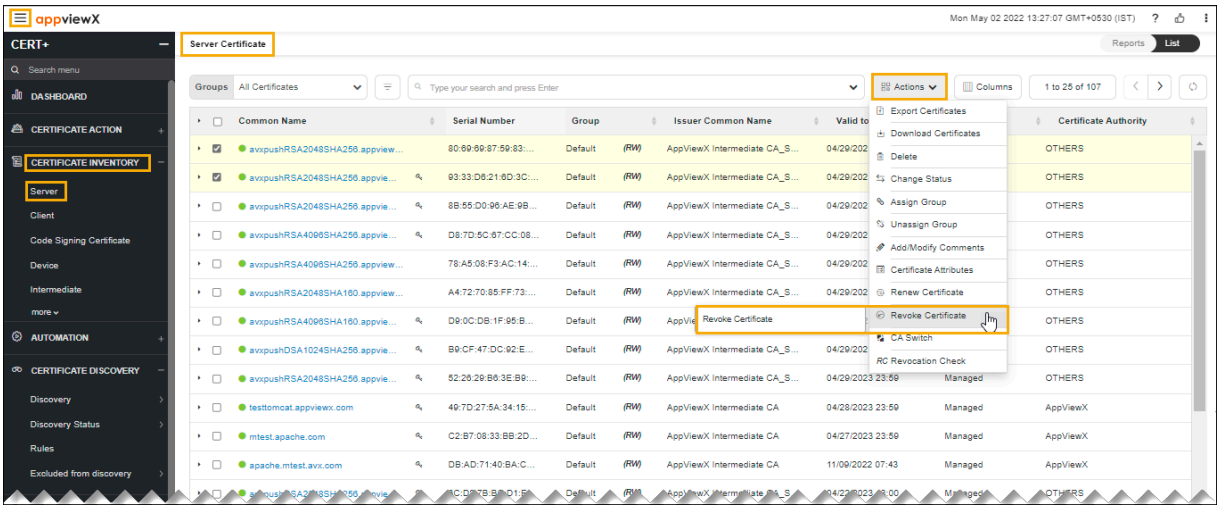
To revoke a server certificate:

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. Click **Server**.
   The **Server Certificate** page appears.

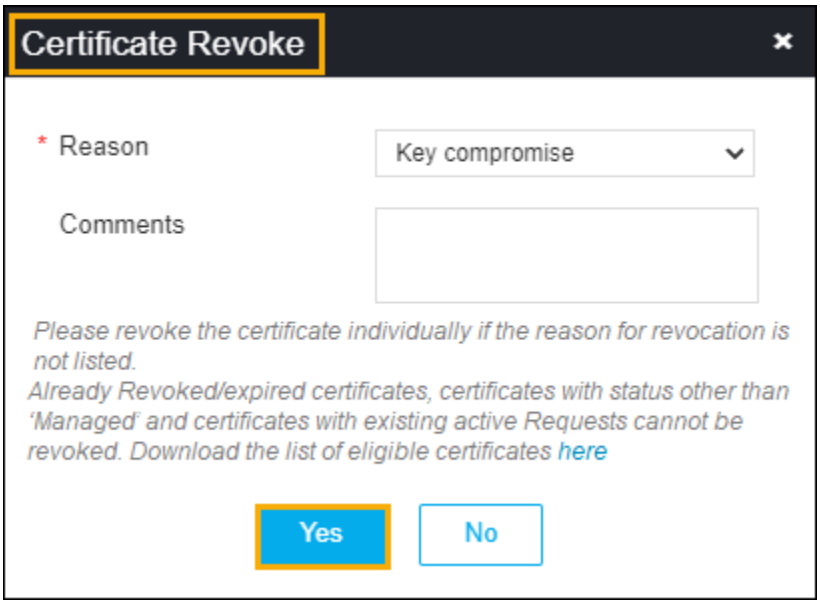


6. Click the **List** toggle button on the right top corner of the server certificate page.



7. Select the required certificate check box.
8. Click **Actions**, and then select **Revoke Certificate** from the list.

   The certificate revoke window page appears.



The following table describes the options available on the revoke certificate page:

Field	Description
Reason	The required option from the dropdown list. The possible options are, • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Type the required comments.

9. Click **Yes**.

Add/Modify Comments for Server Certificate

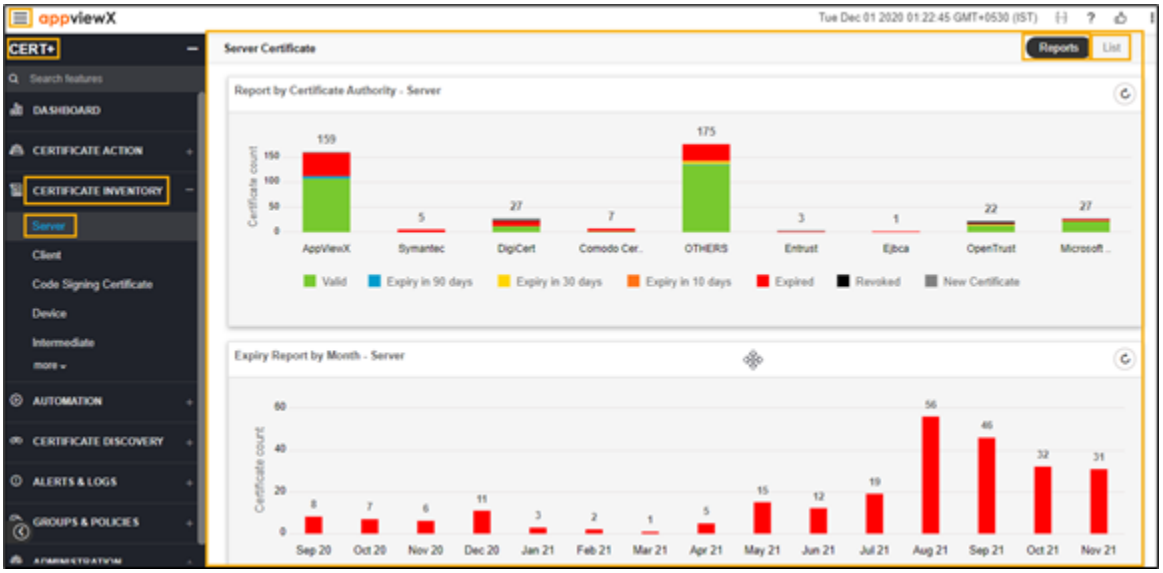
To add/modify comments in the server certificate,

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.

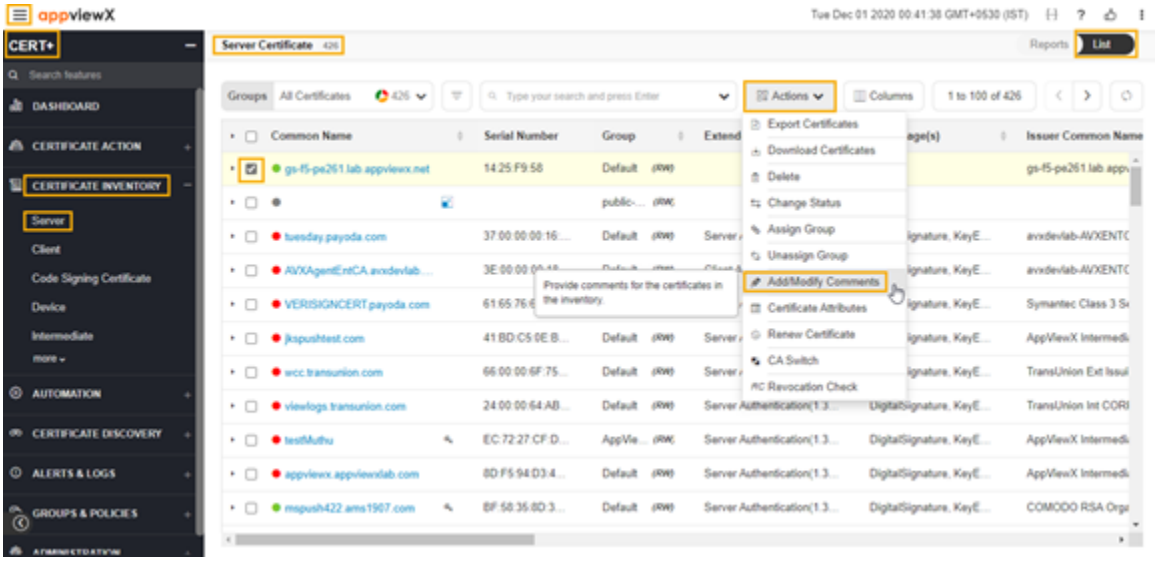
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Server**.

   The **Server Certificate** page appears.

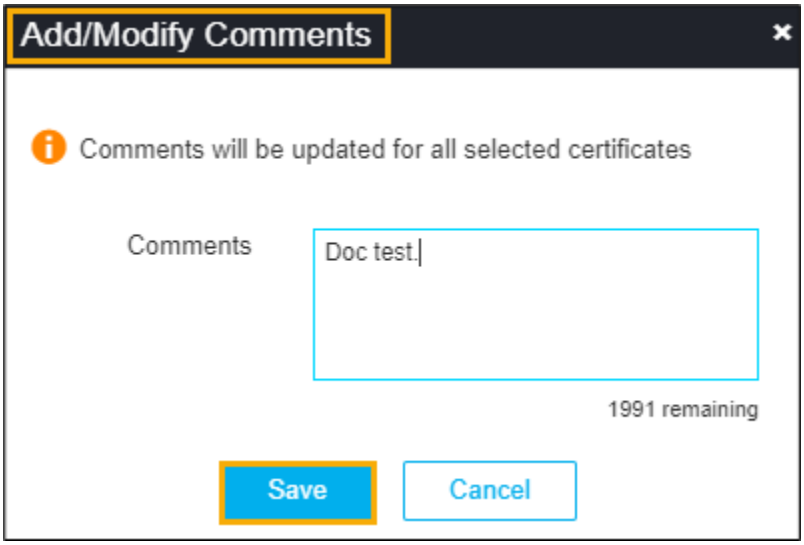


6. Click the **List** toggle button on the right top corner of the server certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to add/modify the certificate comments.
8. Click **Actions**, and then select **Add/Modify Comments** from the drop-down list.

The **Add/Modify Comments** pop-up window appears.

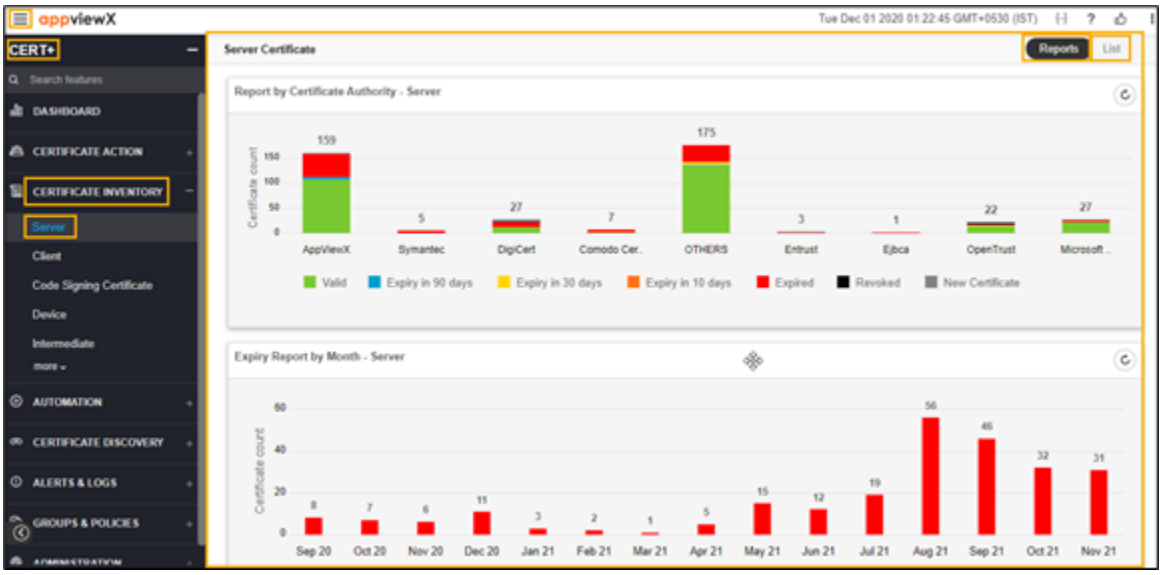


Updating Certificate Attributes for Server Certificate

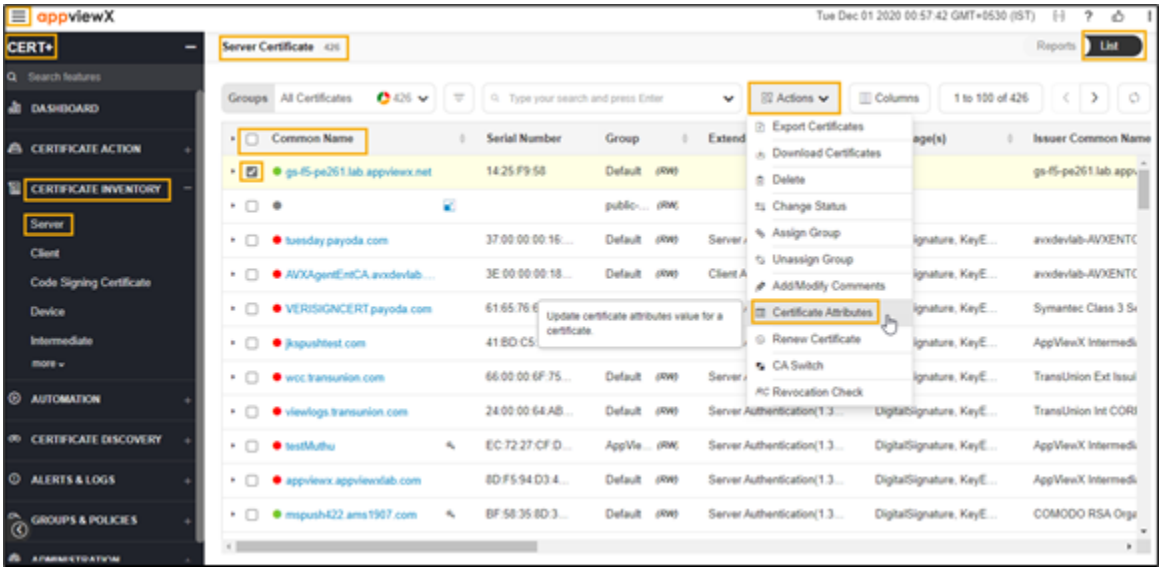
Other than the fields that are defined for CSR, the user can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a server certificate,

1. 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. Click **Server**.
   The **Server Certificate** page appears.



6. Click the **List** toggle button on the right top corner of the server certificate page.
   Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to add attributes.
8. Click **Actions**, and then select **Certificate Attributes** from the drop-down list.

Client Certificate Inventory

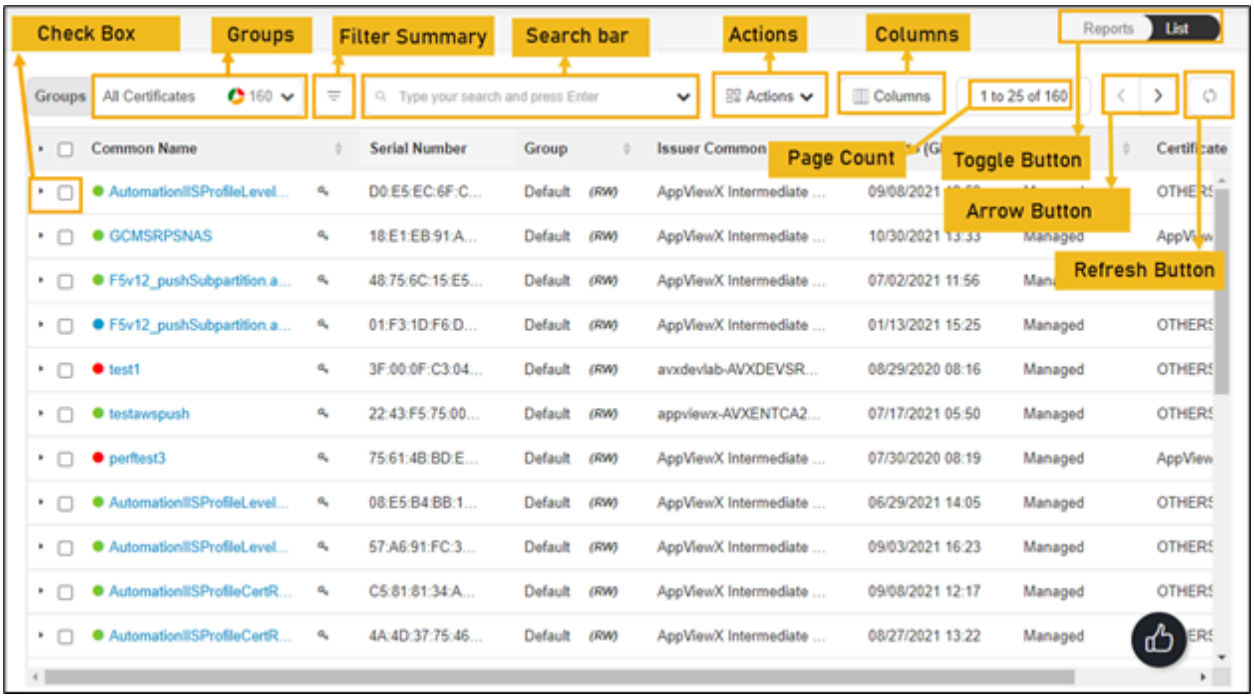
- Overview
- Exporting Client Certificate

Overview

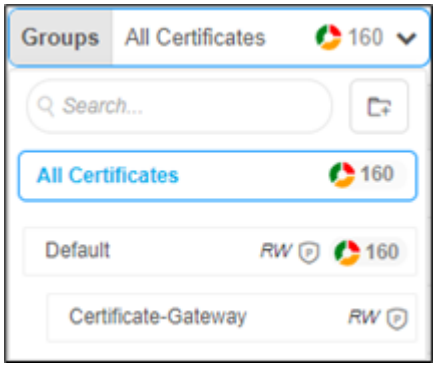
Client certificate inventory is where all the client certificates with the EKU(Extended/enhanced key usage) client authentication, email protection. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificates renewal/revocation check/CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

In the **Certificate Inventory** > **Client Certificate** page, all the client certificates are listed. You can perform the following actions:

• Export Certificates - To export the client certificate
• Delete - To delete the client certificate
• Change Status - To change the client certificate status
• Assign Group - To assign a group to the certificate
• Unassign Group - To Unassign a group from the certificate
• Add/Modify Comments - To add/modify comments to the certificate
• Certificate Attributes - To update the certificate attributes.

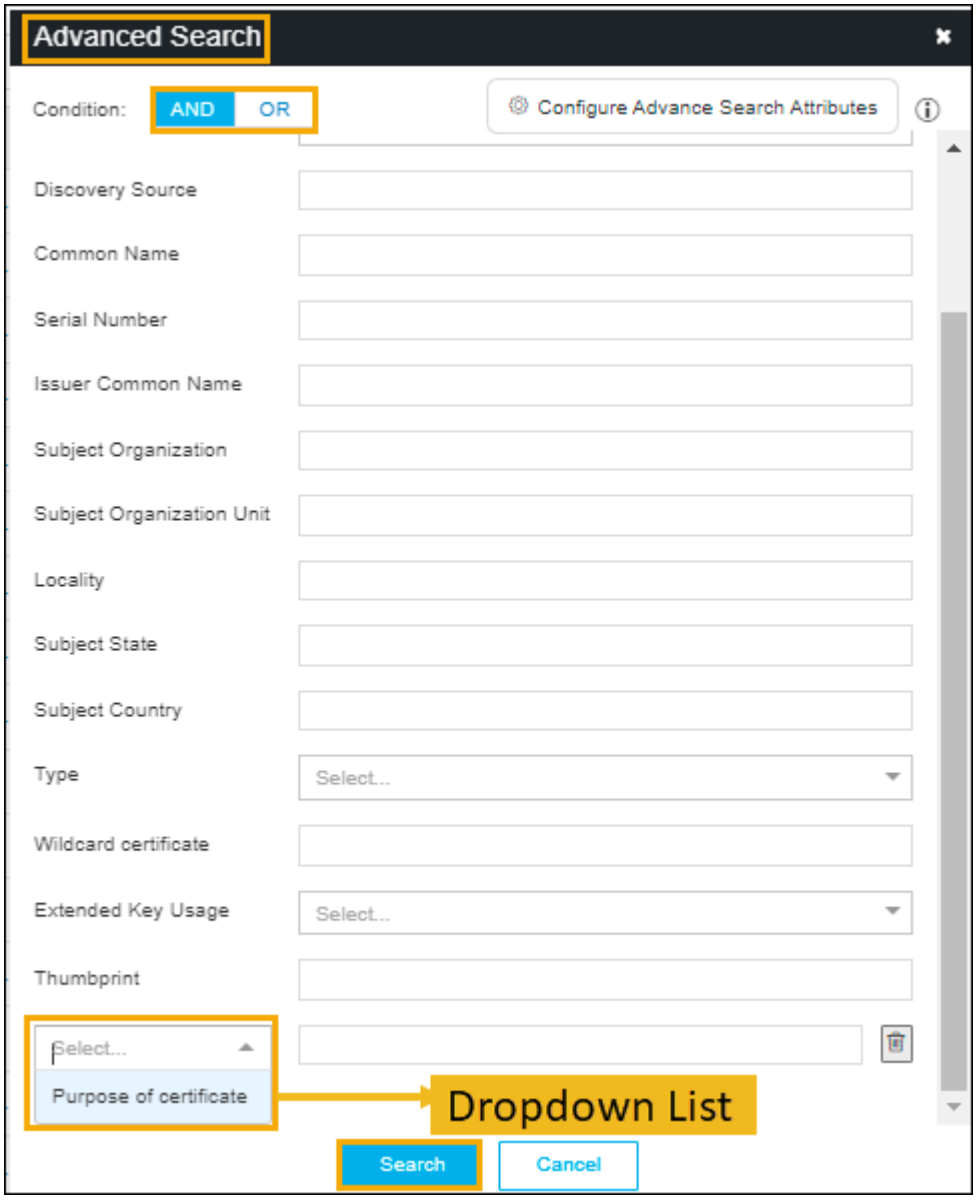


The following table describes the options available on the client certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state.

Options	Description
	
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

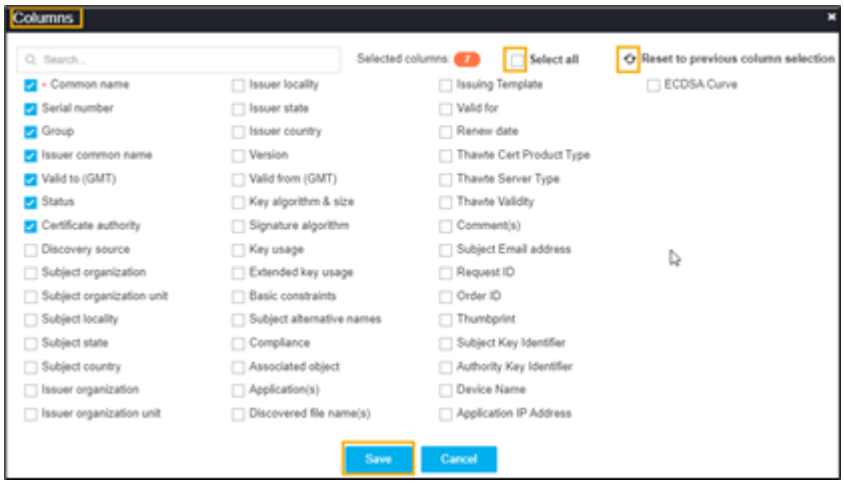


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

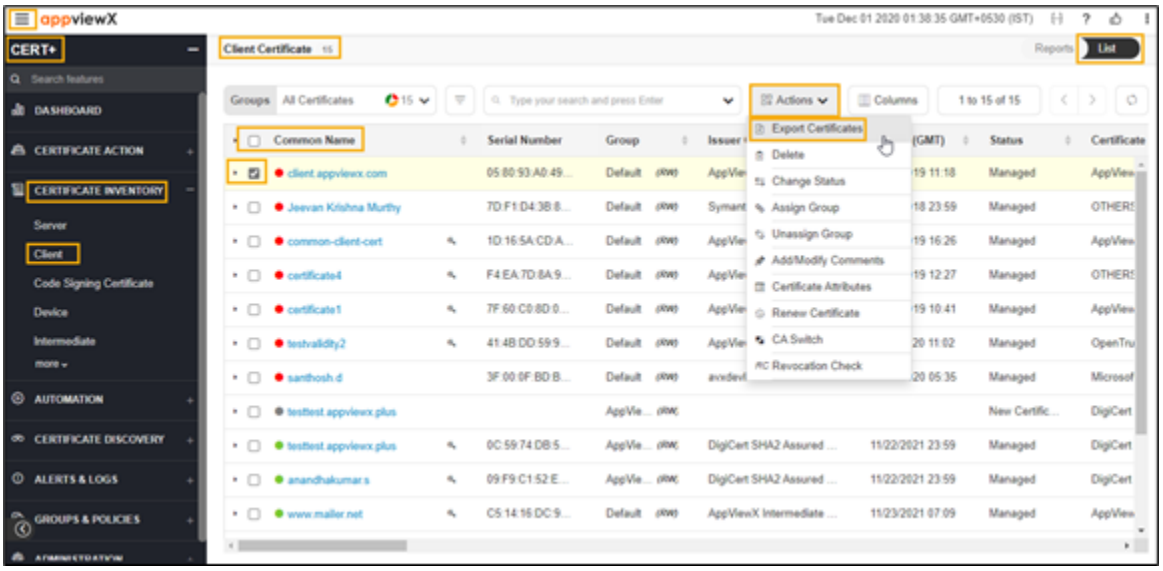
Exporting Client Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in <.xls> or <.csv> format. This can be used for reporting or creating an inventory.

To export a client certificate,

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. Click **Client**.
   The **Client Certificate** page appears.

6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate(s) that you want to export a certificate.
8. Click **Actions**, and then select **Export Certificates** from the list.

   The **Export** pop-up window appears:
9. Select the desired **Options** and **Format** in the **Export** popup window. The selected certificate is exported to your local machine.

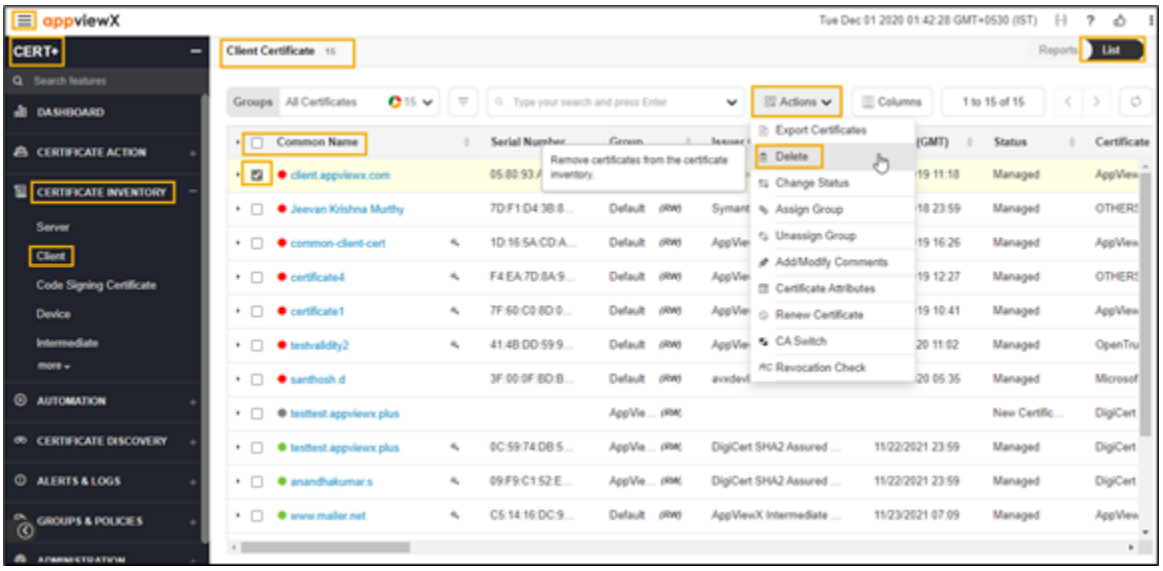
Deleting Client Certificate

Deleting client certificate feature will delete the certificate from the client certificate inventory only in AppViewX. Once the certificate gets deleted from the inventory, the same will not be shown in the reports and for alerts.

To delete a client certificate,

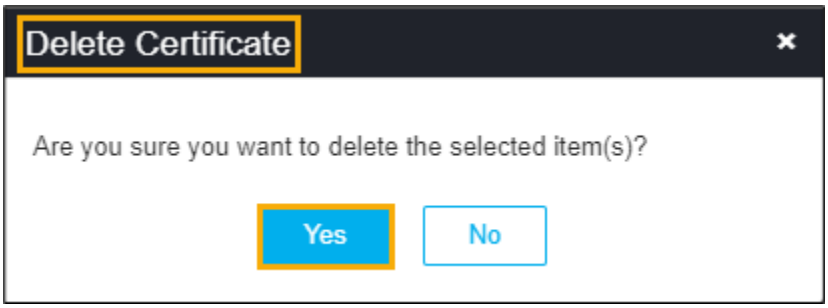
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.
   The **Client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

6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to delete.
8. Click **Actions**, and then select **Delete** from the drop-down list.

   The **Delete** pop-up window appears.



9. Click **Yes**.

   The client certificate is deleted and the pop-up message appears as "**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**".

Deleting Client Certificates via Holistic View

In the Holistic view, the user will find the entire chain of trust of the certificates along with the devices/ objects with which the certificates are associated. The primary actions that can be performed from the holistic view are Certificate creation, renewal, reissue, revoke, regenerate, install the certificates to the devices and objects. The other supported actions in the holistic view are download certificates and private keys, delete the certificate in the AppViewX certificate inventory, perform rollback action on the associated certificate and disassociate the certificate from the objects in the device.

To delete a client certificate via holistic view,

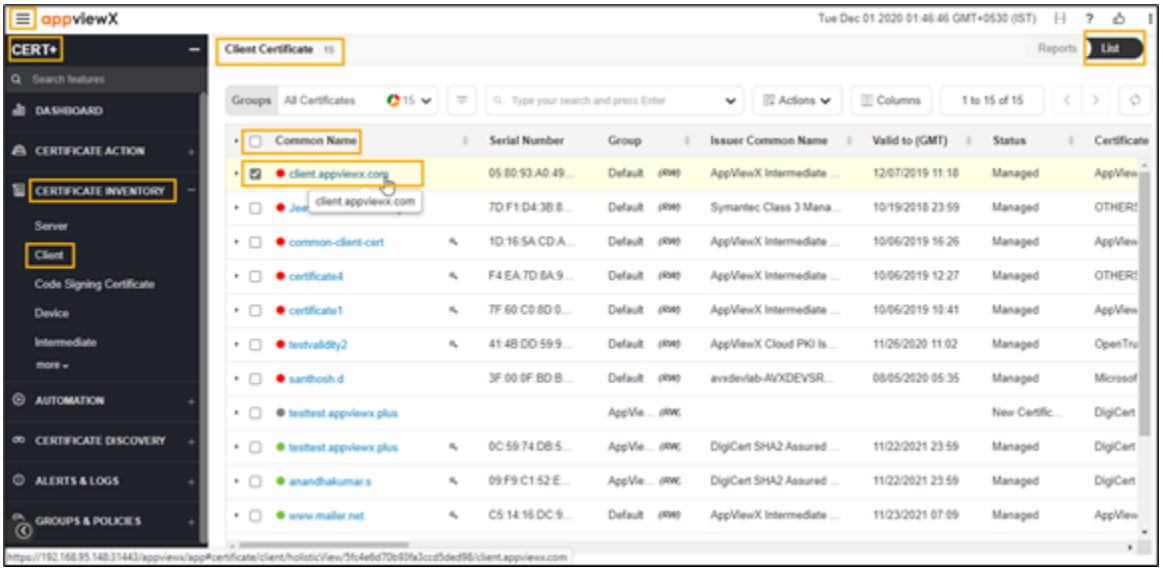
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

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

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.

   The **Client Certificate** page appears.

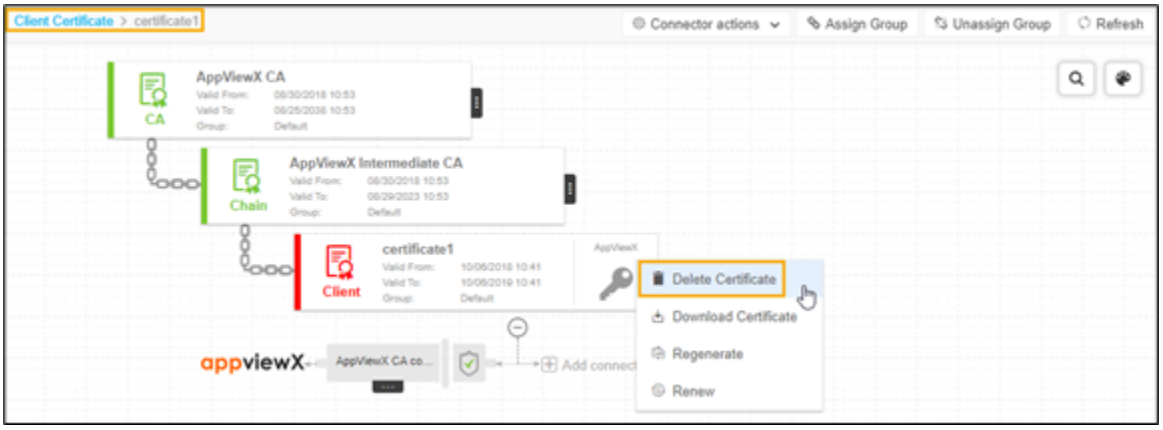
6. Click the **List** toggle button on the right top corner of the client certificate page.

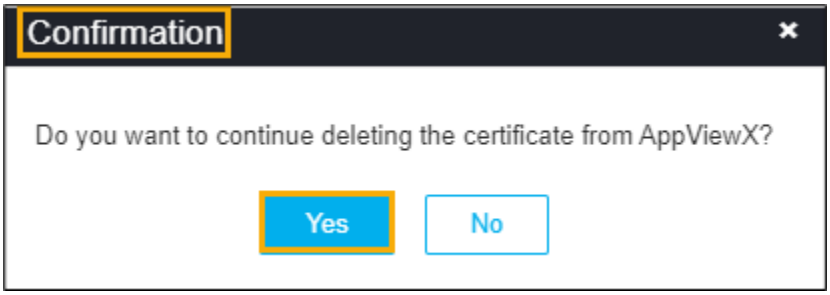


7. In the **Common Name** column certificate list, select the desired certificate that you want to delete the CA.

8. Click vertical ellipse icon in the holistic view, and then select **Delete Certificate** from the list.

   The **Delete Certificate** pop-up window appears.





9. Click **Yes**.

   The client certificate is deleted and the pop-up message appears as **Selected certificate(s) with RW permission has been deleted from AppViewX inventory**.

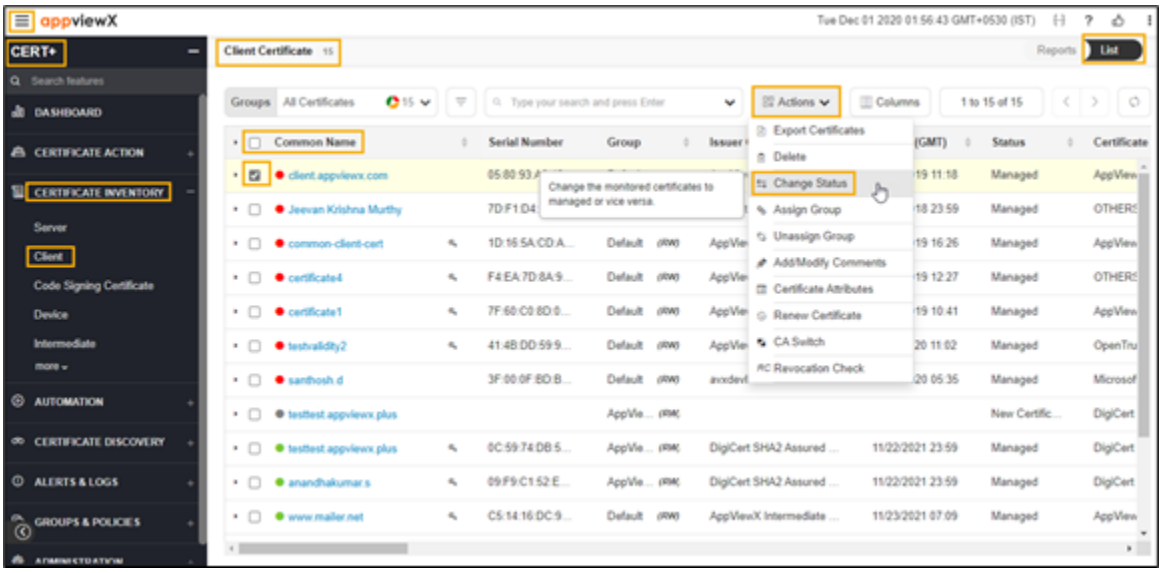
Changing Client Certificate Status

The certificate status can be set as monitored/managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, only viewing of the certificate details in terms of reports and inventory provided with alerting mechanisms can be done. When the certificates are set as Managed, the certificates-related actions along with push/bind operation can be performed along with viewing of the certificates in the reports and inventory.

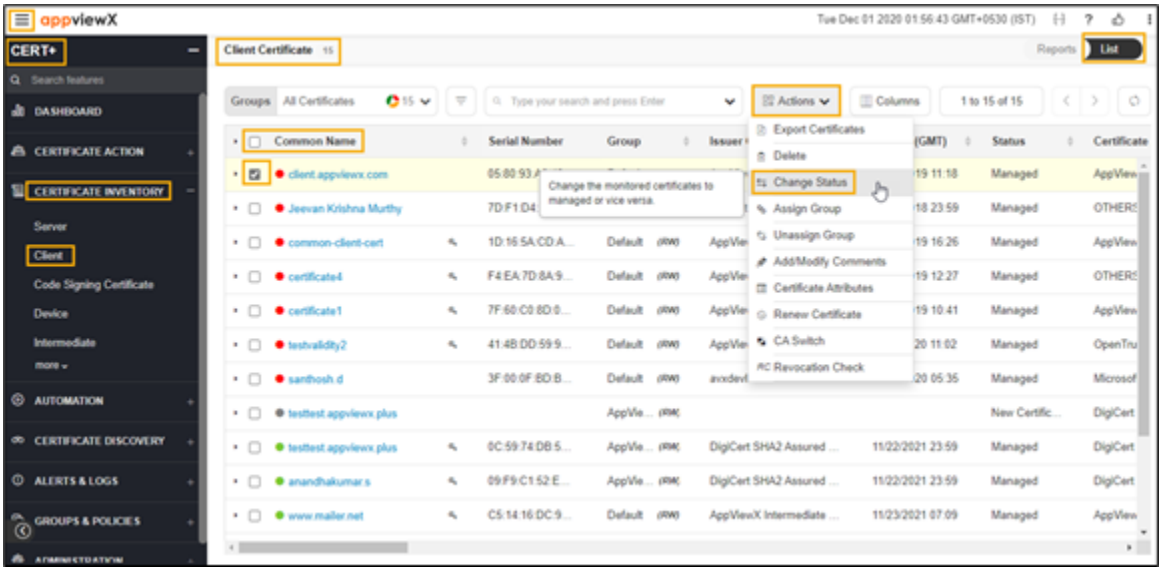
To change the Client certificate status,

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. Click **Client**.
   The **Client Certificate** page appears.

6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to change the certificate status.
8. Click **Actions**, and then select **Change Status** from the drop-down list.
   The Change Status pop-up window appears.



   a. Select the desired status from the **Change Status to** drop-down list.
   b. Enter the reason for changing the status in the description field.
   c. Click **Yes**.
9. The certificate status is changed to Managed or Monitored as selected from the drop-down list. The pop-up message appears as **Updated**.

Assigning Client Certificate Group

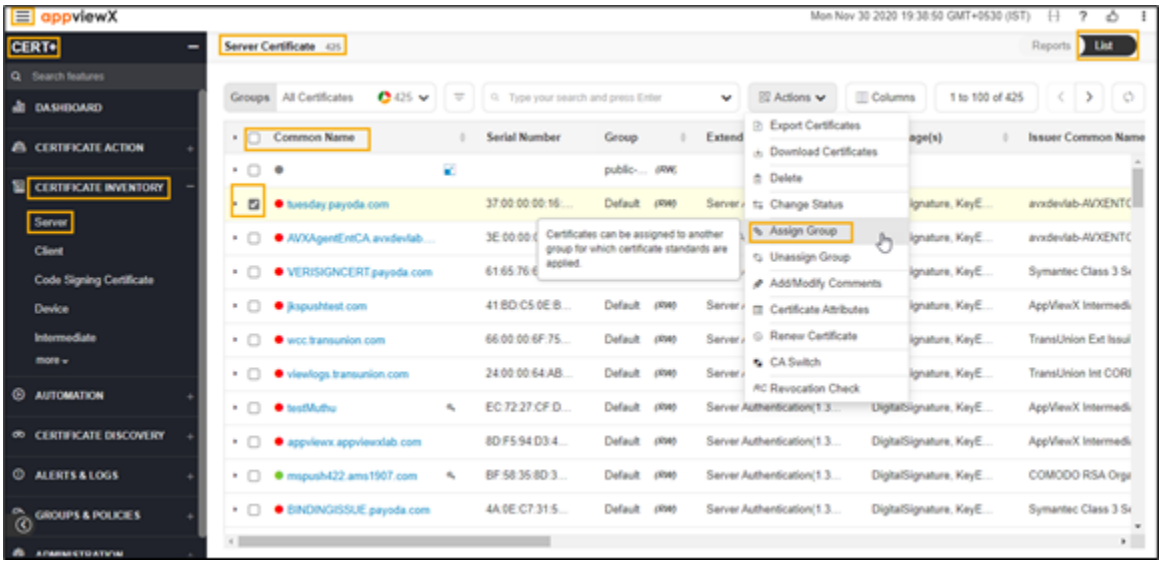
The certificates of any common criteria can be grouped together to perform compliance checks against the policy details, to enable auto-renewal and auto-push operations. The viewing of the certificates can also be done on a group basis.

To assign the client 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. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.

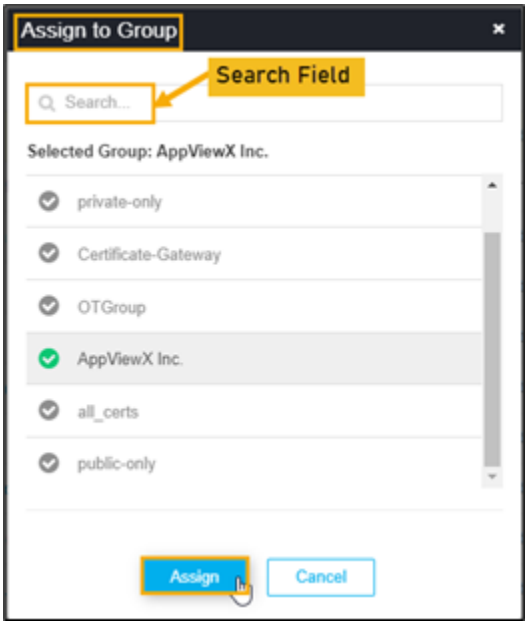
   The **Client Certificate** page appears.

6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate(s) that you want to assign the certificate group.
8. Click **Actions**, and then select **Assign Group** from the drop-down list.

   The **Assign Group** pop-up window appears.



   a. Enter keywords if you want to search for a specific group from the list.
   b. Select the desired group from the listed groups.
   c. Click **Assign**.
9. The certificate is assigned to a selected group.

   The pop-up message appears as **<certificate_name> assigned to <group_name>**.

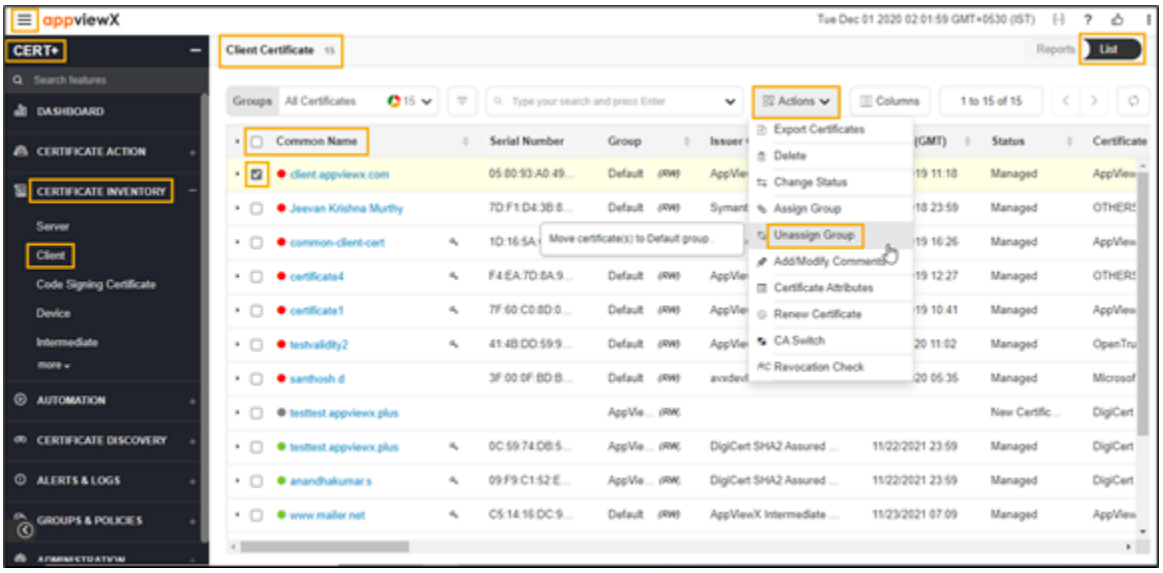
Unassigning Client Certificate Group

The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign the client 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. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.
   The **Client Certificate** page appears.

6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to unassign the certificate group.
7. Click the **List** toggle button on the right top corner of the client certificate page.



8. Click **Actions**, and then select **Unassign Group** from the drop-down list.
9. The selected certificate is assigned to the default group.

   The pop-up message appears as **<certificate_name> assign to undefined**.

Bulk Client Certificate Revoke Action

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

To revoke a server certificate:

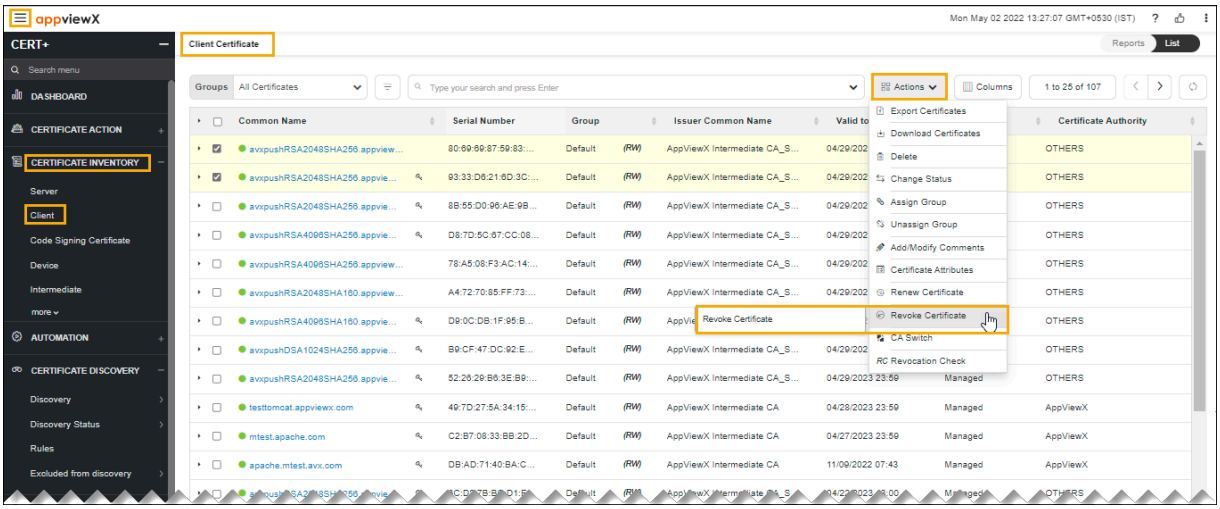
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

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

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.

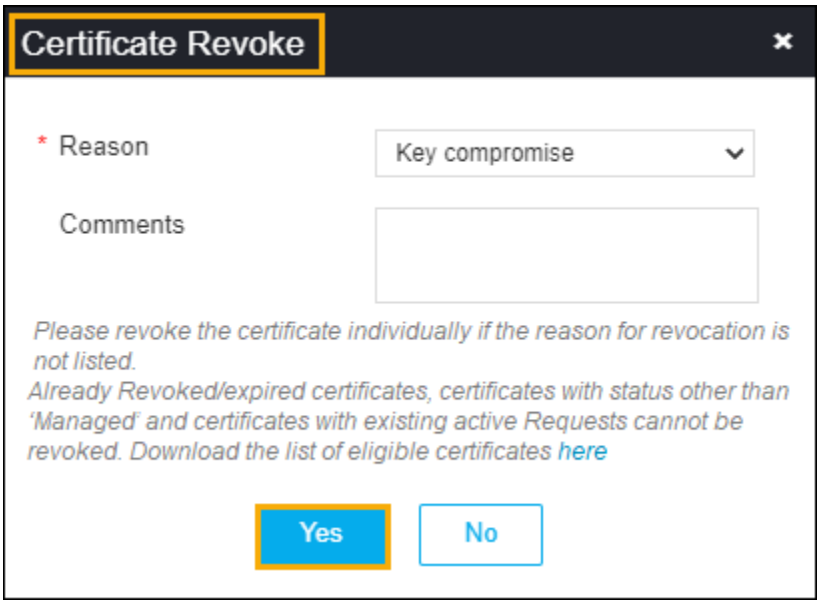
   The **Client Certificate** page appears.

6. Click the **List** toggle button on the right top corner of the server certificate page.



7. Select the required certificate check box.
8. Click **Actions**, and then select **Revoke Certificate** from the list.

   The certificate revoke window page appears.



The following table describes the options available on the revoke certificate page:

Field	Description
Reason	The required option from the dropdown list. The possible options are, • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Type the required comments.

9. Click **Yes**.

Add/Modify Comments for Client Certificate

To add/modify the comments for a client certificate,

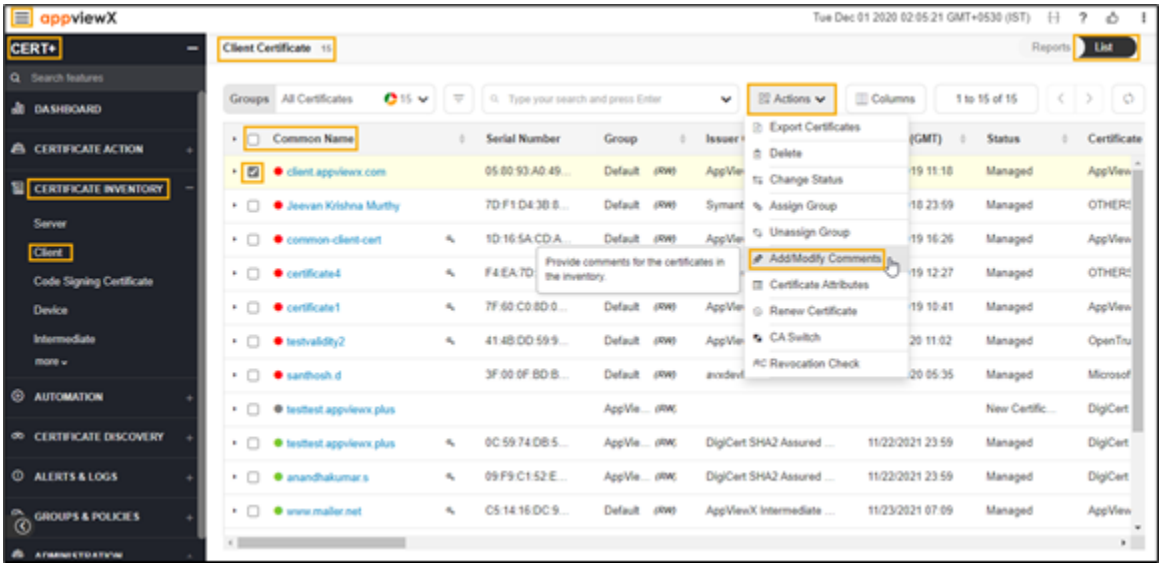
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.

3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.

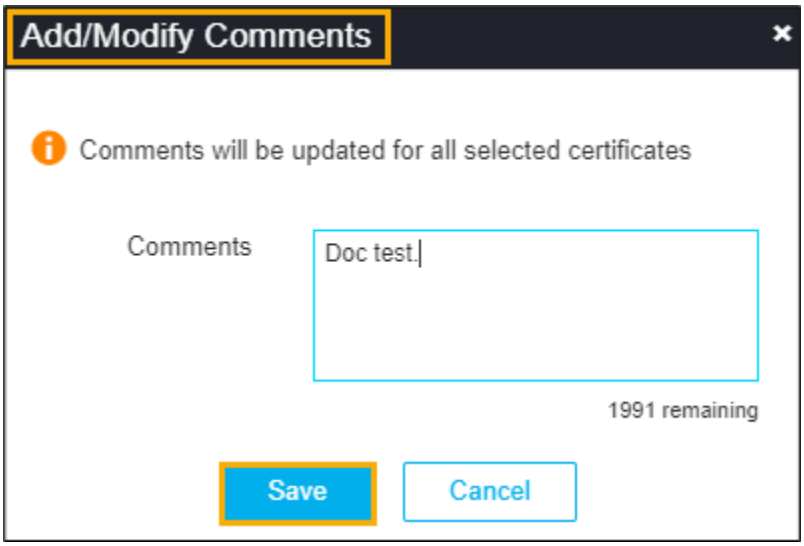
   The **Client Certificate** page appears.

6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to add/modify the certificate.
8. Click **Actions**, and then select **Add/Modify Comments** from the drop-down list.

   The **Add/Modify Comments** pop-up window appears.



a. Enter the description in the comments field.

b. Click **Save**.

The pop-up message appears as **Selected certificate(s) comment(s) uploaded**.

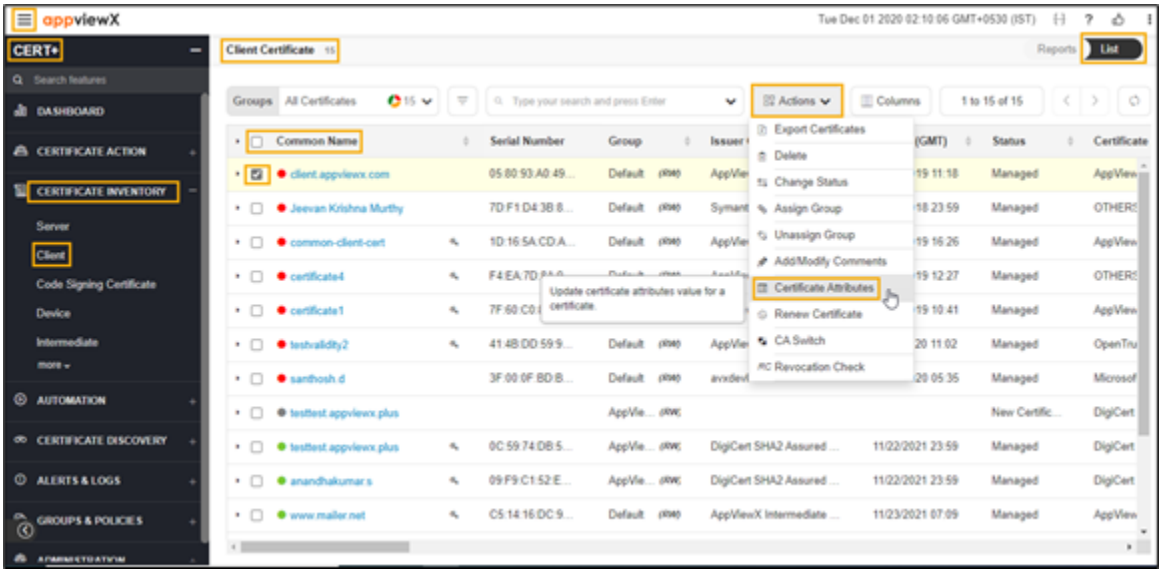
Updating Certificate Attributes for Client Certificate

Other than the fields that are defined for CSR, the customer can add organization-specific values for a certificate request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a client certificate,

1. 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. Click **Client**.
   The **Client Certificate** page appears.

6. In the **Common Name** column certificate list, select the desired certificate that you want to add attributes.
7. Click the **List** toggle button on the right top corner of the client certificate page.



8. Click **Actions**, and then select **Certificate Attributes** from the drop-down list.

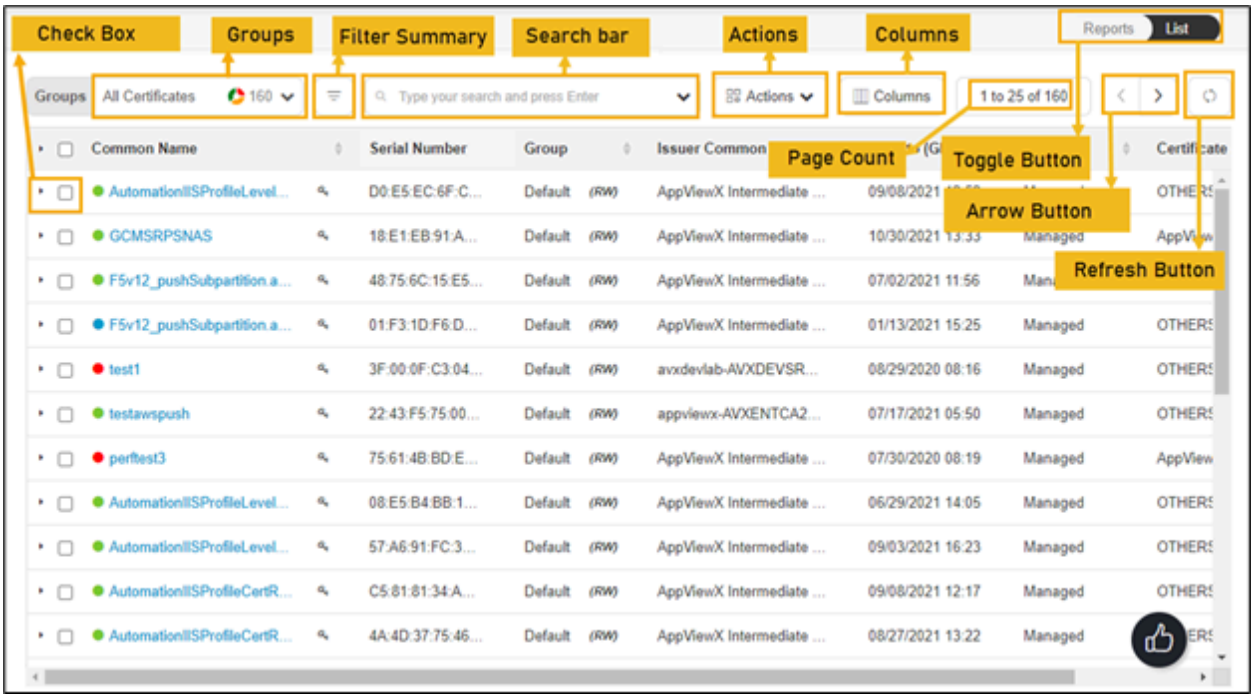
Code Signing Certificate Inventory

Overview

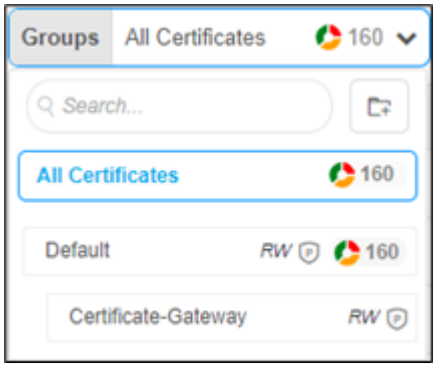
Code signing certificate inventory is where all the code certificate with the EKU(Extended/enhanced key usage) code signing will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificates revocation check, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

On the **Certificate Inventory** > **Code Signing Certificate** page, all the code signing certificates are listed. You can perform the following actions:

• Export Certificates - To export the code signing certificate
• Delete - To delete the code signing certificate
• Change Status - To change the code signing certificate status
• Assign Group - To assign a group to the certificate
• Unassign Group - To Unassign a group from the certificate
• Add/Modify Comments - To add/modify comments to the certificate
• Certificate Attributes - To update the certificate attributes.

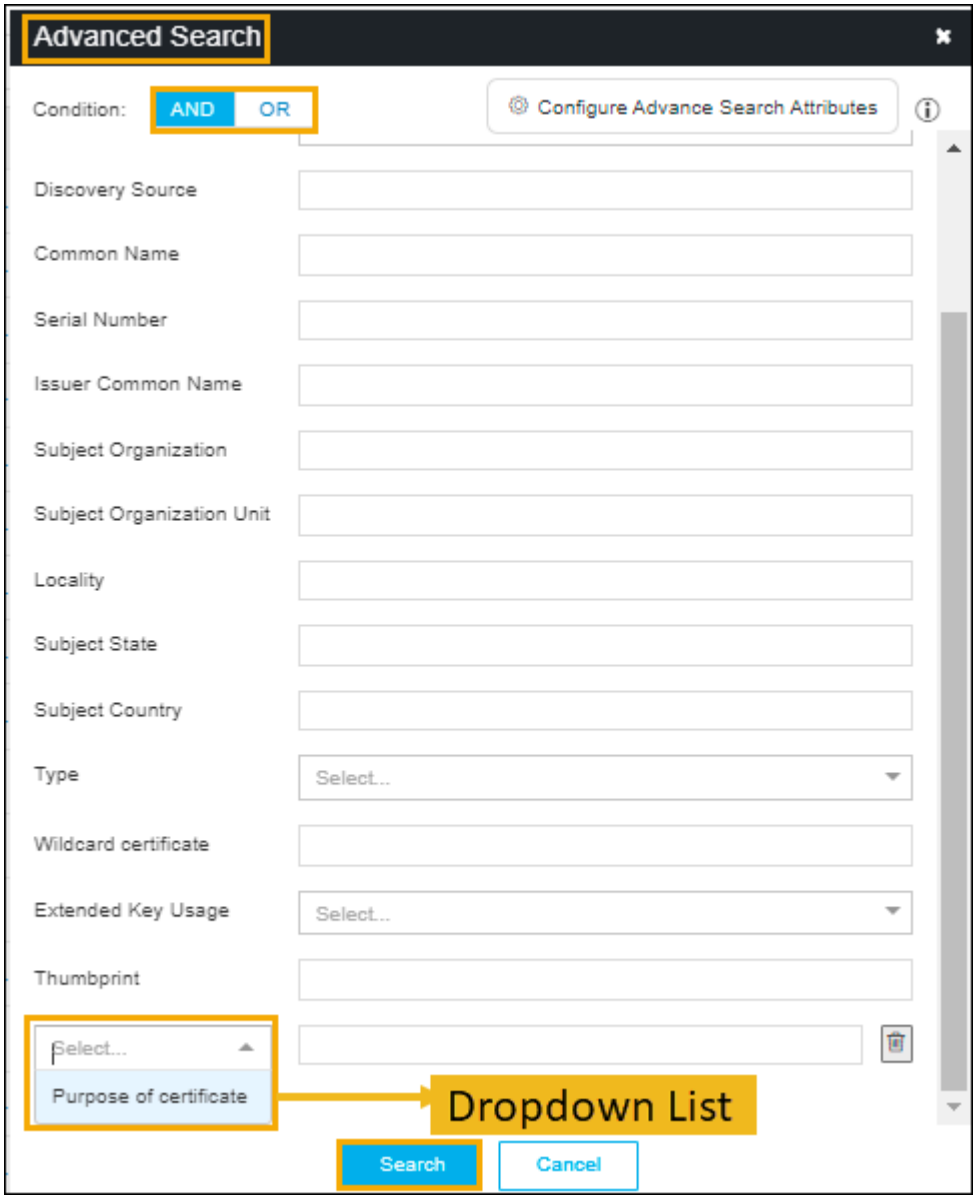


The following table describes the options available on the code signing certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state.

Options	Description
	
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

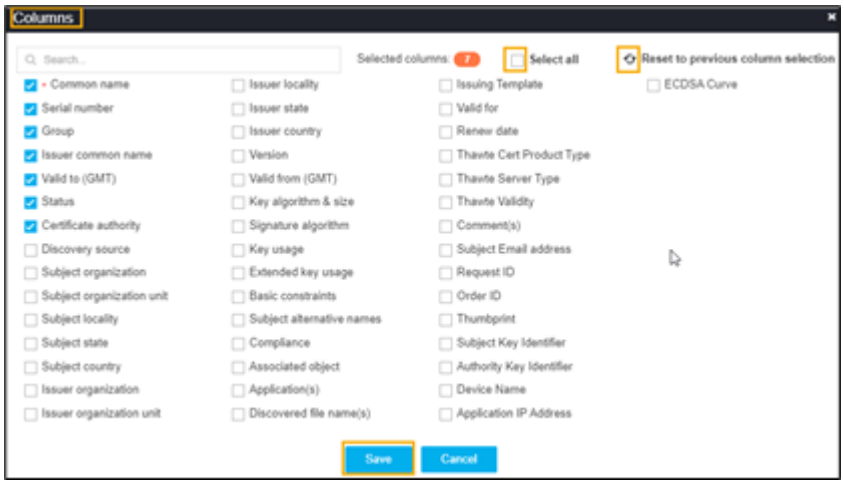


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

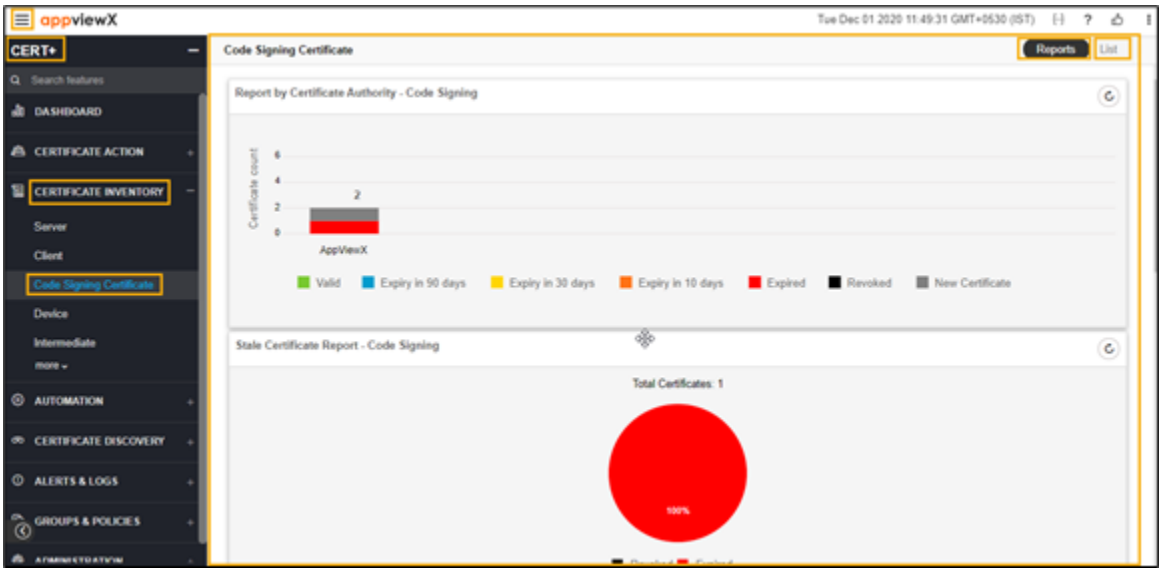
Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Exporting Code Signing Certificate

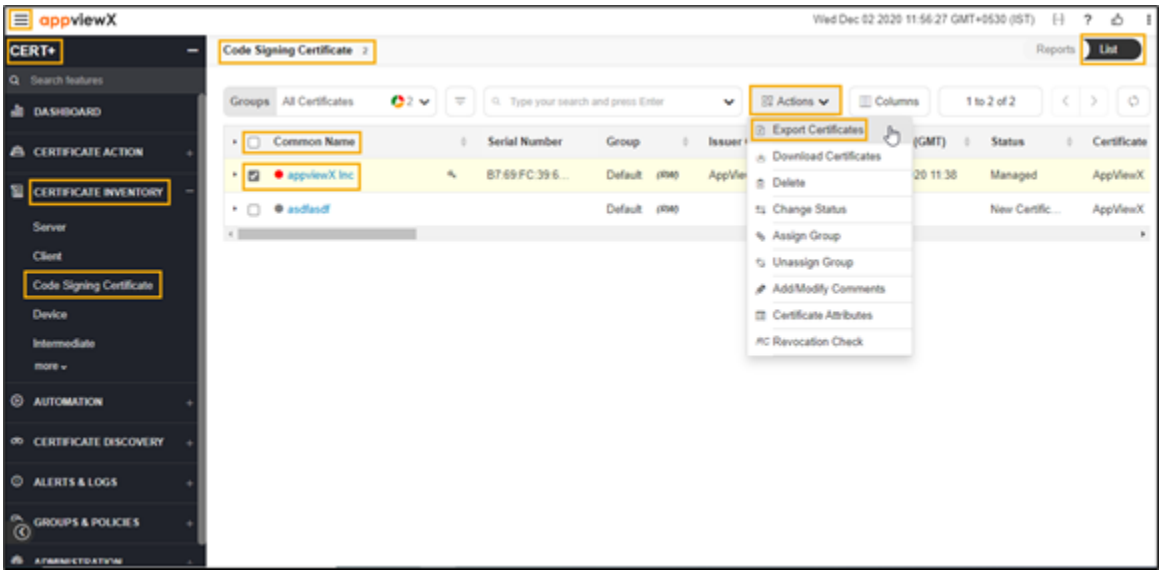
Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in <.xls> or <.csv> format. This can be used for reporting or creating another inventory.

To export code signing certificate,

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. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.

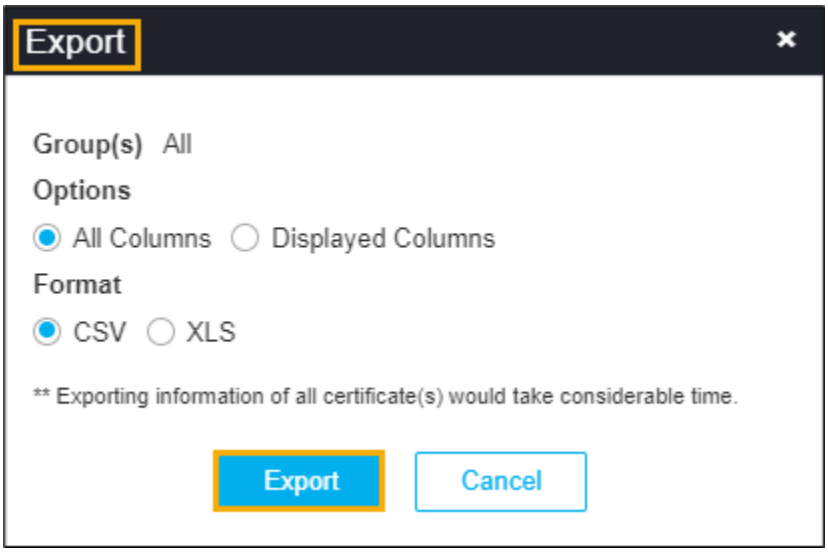


6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to export a certificate.
8. Click **Actions**, and then select **Export Certificates** from the list.

   The **Export** pop-up window appears.



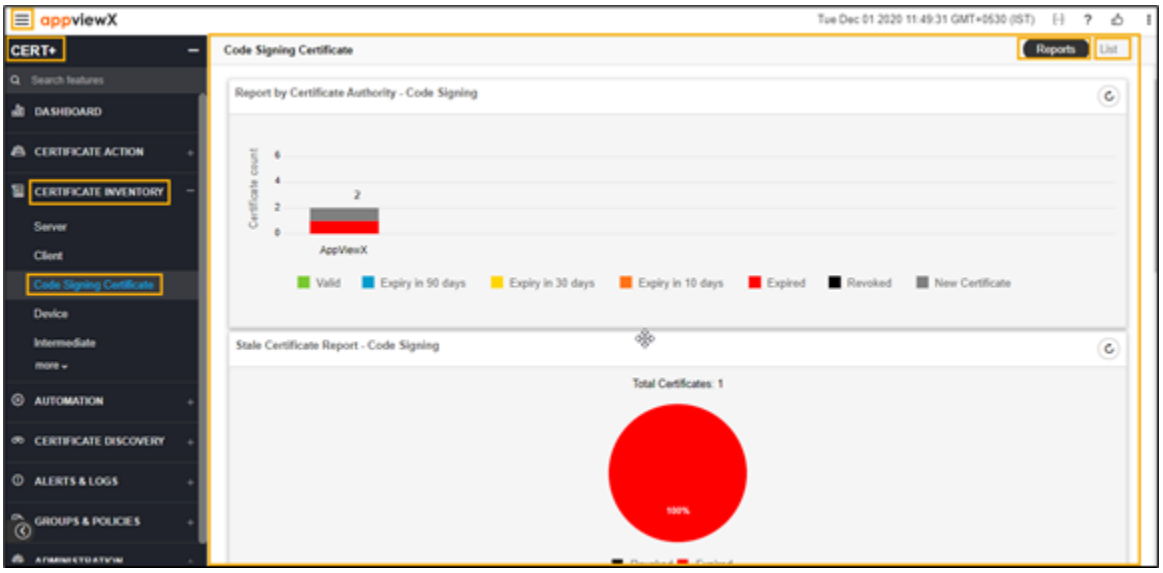
9. Select the desired **Options** and **Format** in the **Export** pop-up window.
   The selected certificate is exported to your local machine.

Deleting Code Signing Certificate

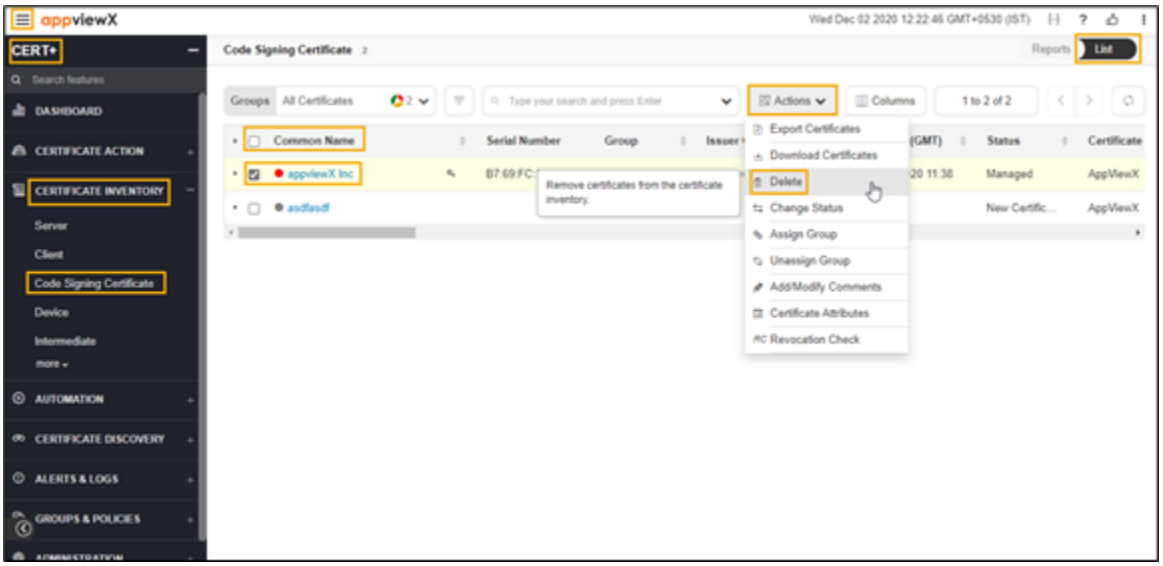
Deleting code signing certificate feature allows you to delete a certificate from the server certificate inventory only in AppViewX. Once the certificate gets deleted from the inventory, the same will not be shown in the reports and for alerts.

To delete code signing certificate,

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. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.

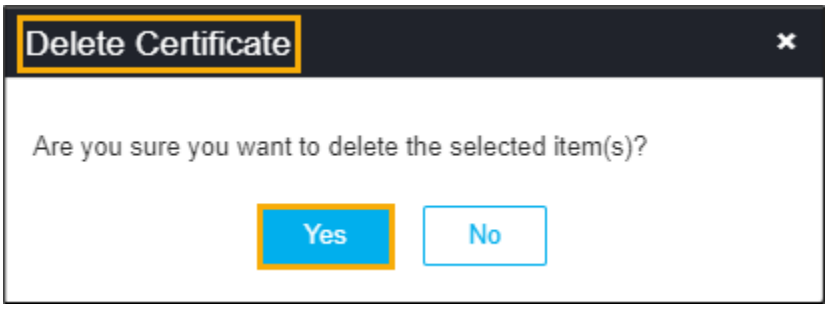


6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to delete the certificate.
8. Click **Actions**, and then select **Delete** from the drop-down list.

   The **Delete** pop-up window appears.



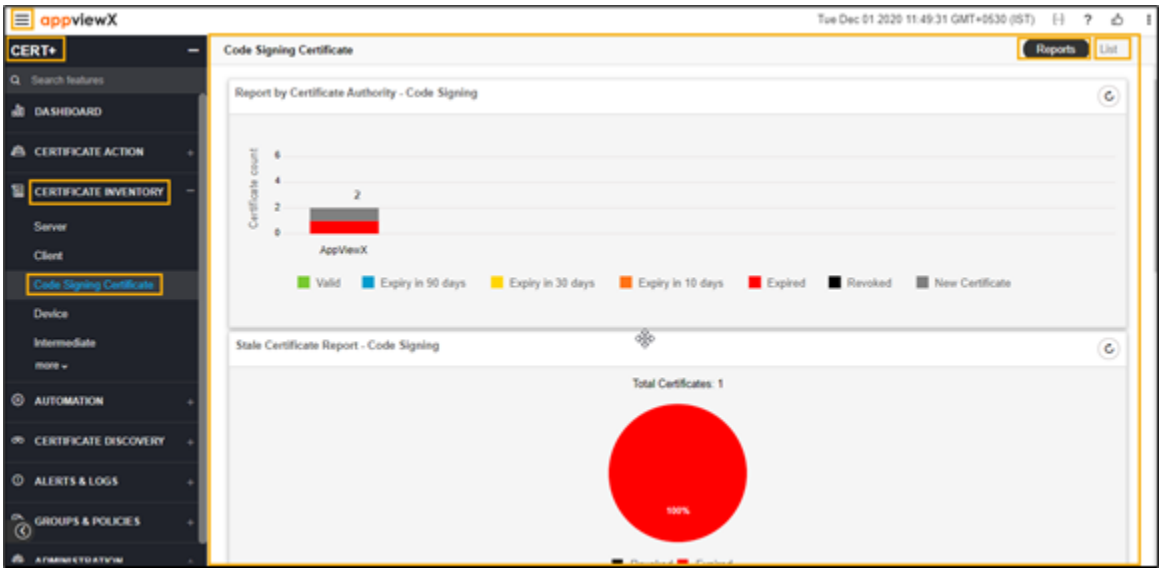
9. Click **Yes**.
   The code signing certificate is deleted and the pop-up message appears as "**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**".

Deleting Code Signing Certificates via Holistic View

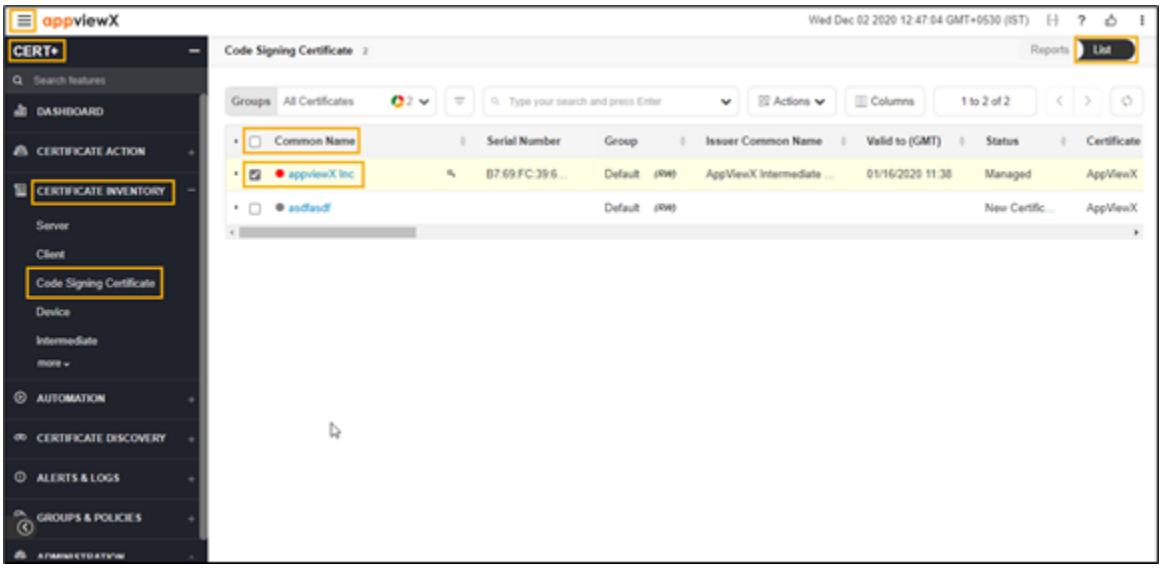
In the Holistic view, the user will find the entire chain of trust of the certificates along with the devices/ objects with which the certificates are associated. The primary actions that can be performed from the holistic view are Certificate creation, renewal, reissue, revoke, regenerate, install the certificates to the devices and objects. The other supported actions in the holistic view are download certificates and private keys, delete the certificate in the AppViewX certificate inventory, perform rollback action on the associated certificate and disassociate the certificate from the objects in the device.

To delete code signing certificate via holistic view,

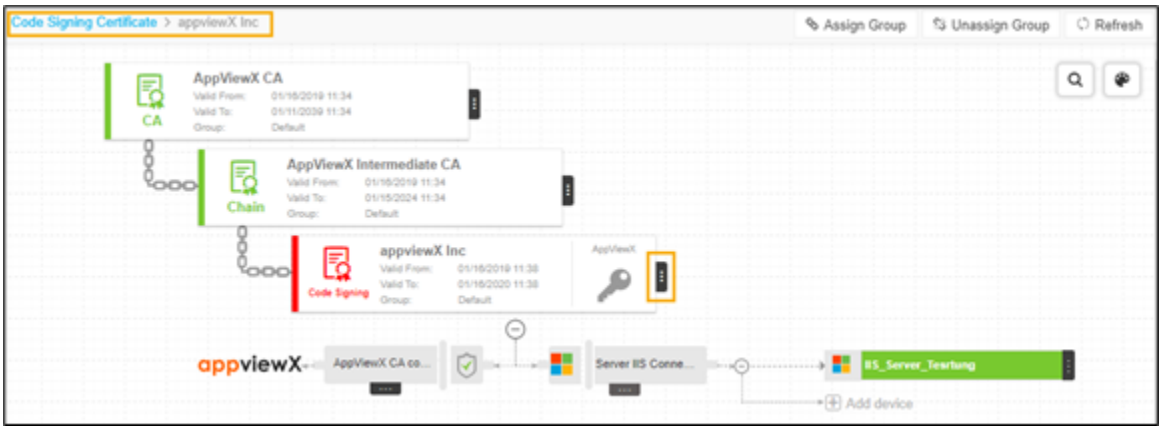
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.



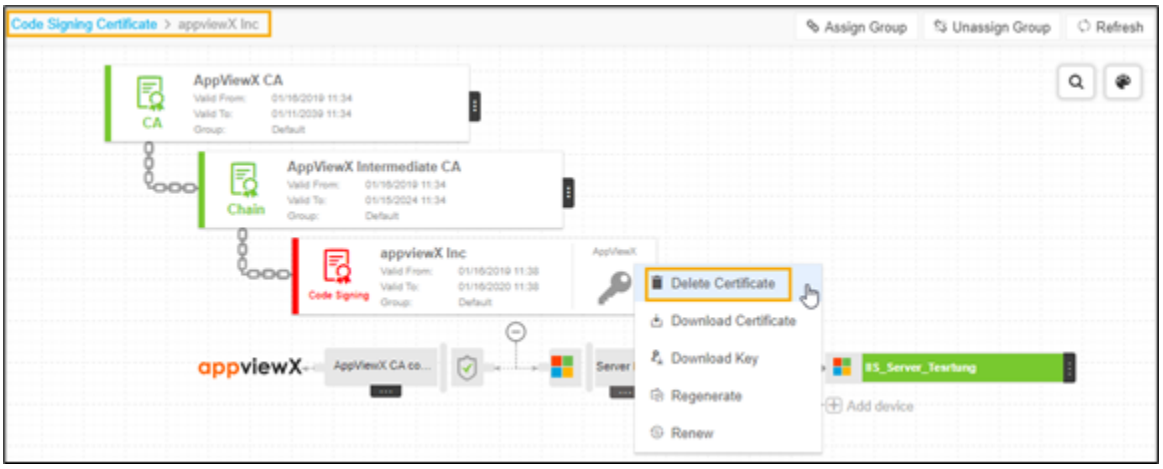
6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, click the desired certificate that you want to delete the CA.



8. Click vertical ellipse icon in the holistic view, and then select **Delete Certificate** from the list.
   The **Delete Certificate** pop-up window appears.



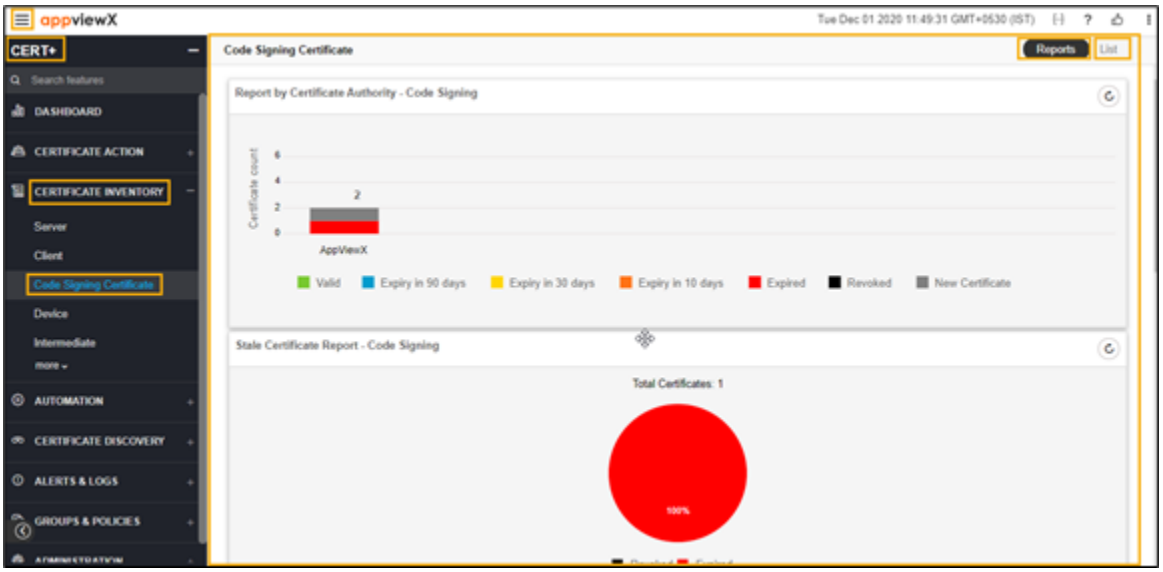
9. Click **Yes**.
   The code signing certificate is deleted and the pop-up message appears as **Selected certificate(s) with RW permission has been deleted from AppViewX inventory**.

Changing Code Signing Certificate Status

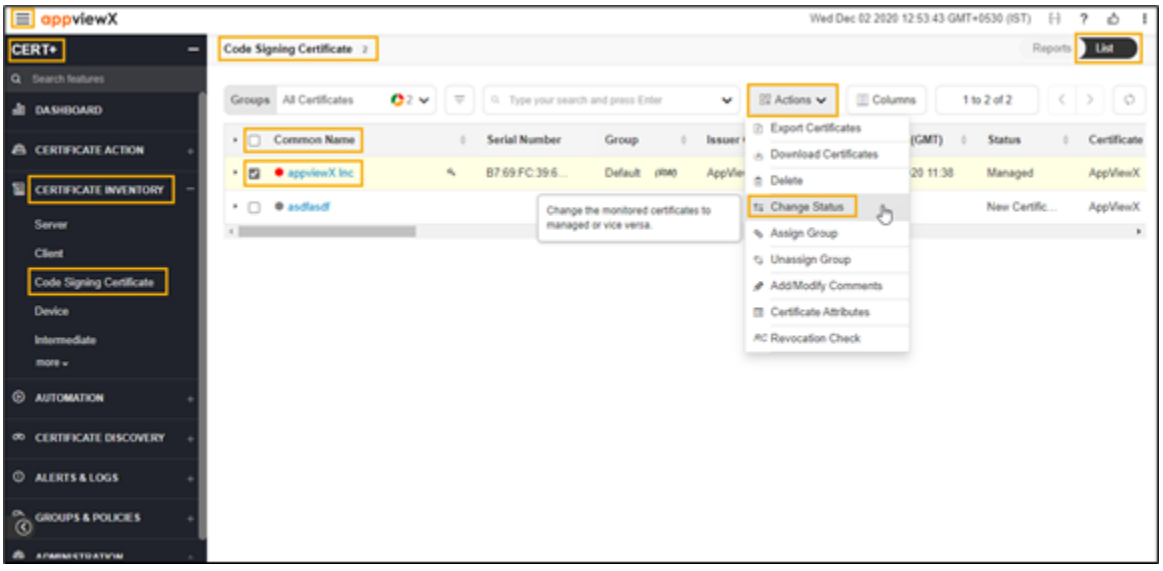
The certificate status can be set as monitored/managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, only viewing of the certificate details in terms of reports and inventory provided with alerting mechanisms can be done. When the certificates are set as Managed, the certificates-related actions along with push/bind operation can be performed along with viewing of the certificates in the reports and inventory.

To change code signing certificate status,

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. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.

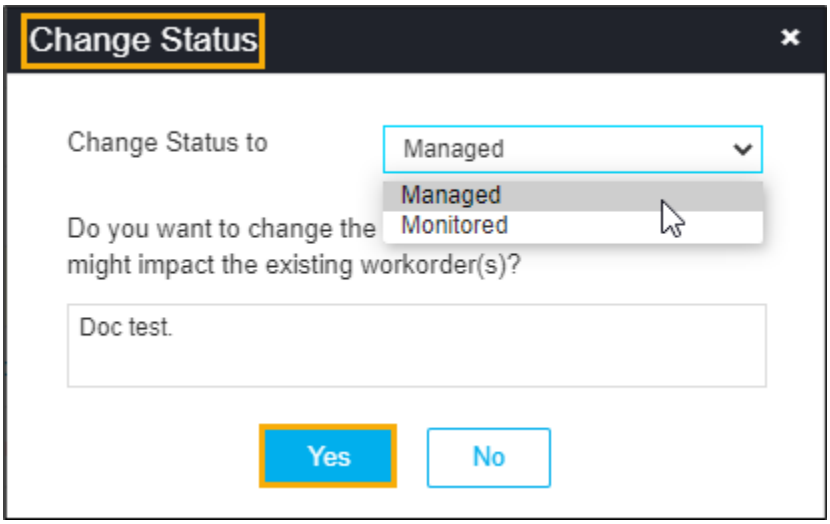


6. Click the **List** toggle button on the right top corner of the code signing certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to change the certificate status.

8. Click **Actions**, and then select **Change Status** from the drop-down list.
   The Change Status pop-up window appears.



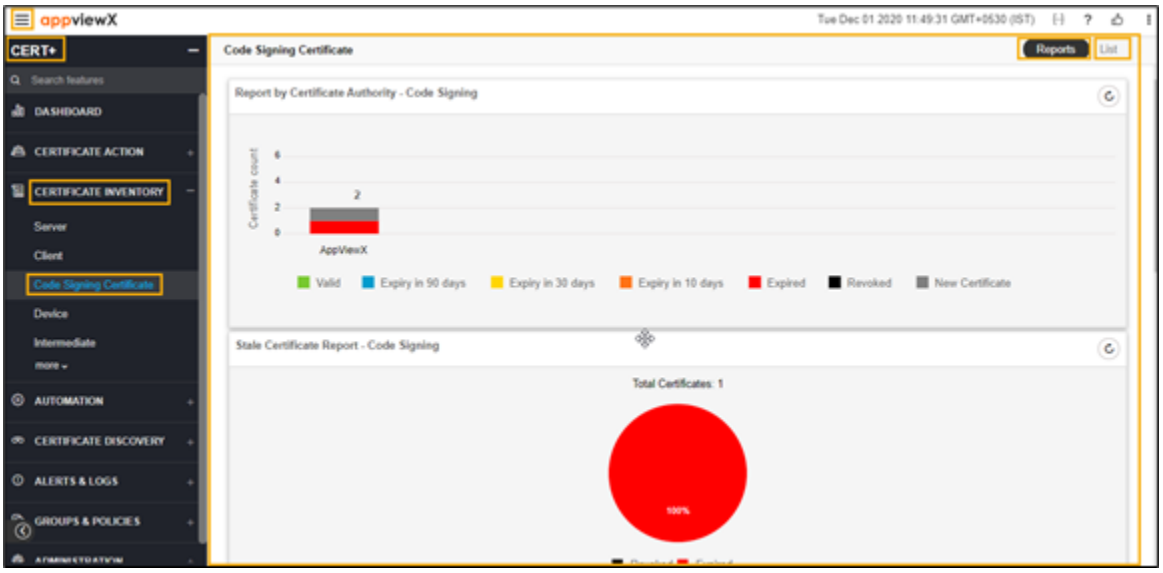
   a. Select the desired status from the **Change Status to** the drop-down list.
   b. Enter the reason for changing the status in the description field.
   c. Click **Yes**.
9. The certificate status is changed to Managed or Monitored as selected from the drop-down list.
   The pop-up message appears as **Updated**.

Assigning Code Signing Certificate Group

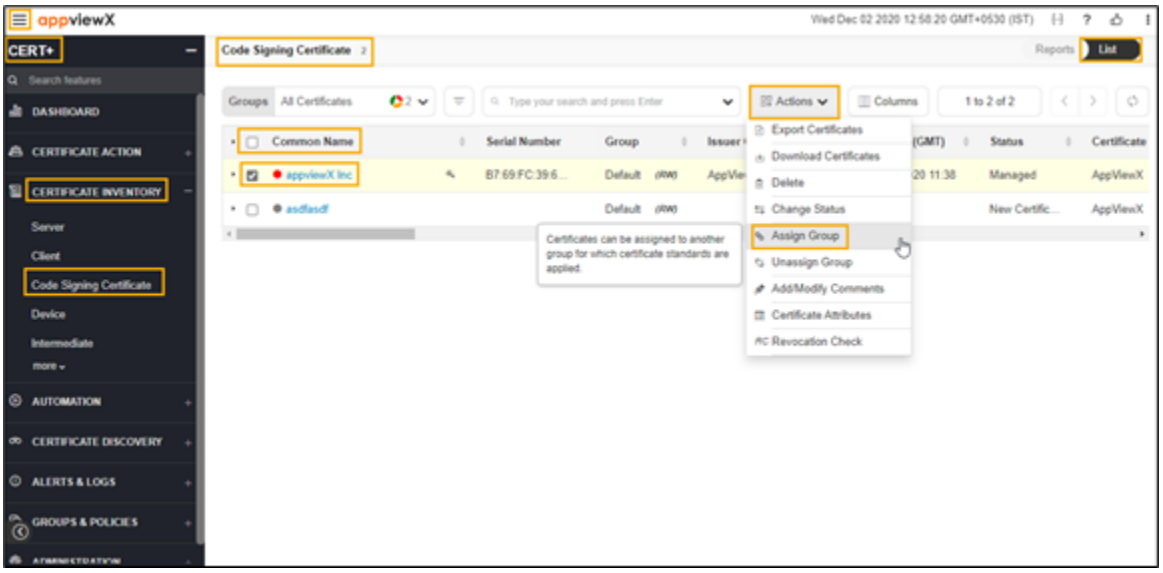
The certificates of any common criteria can be grouped together to perform compliance checks against the policy details, to enable auto-renewal and auto-push operations. The viewing of the certificates can also be done on a group basis.

To assign the code signing 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. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.

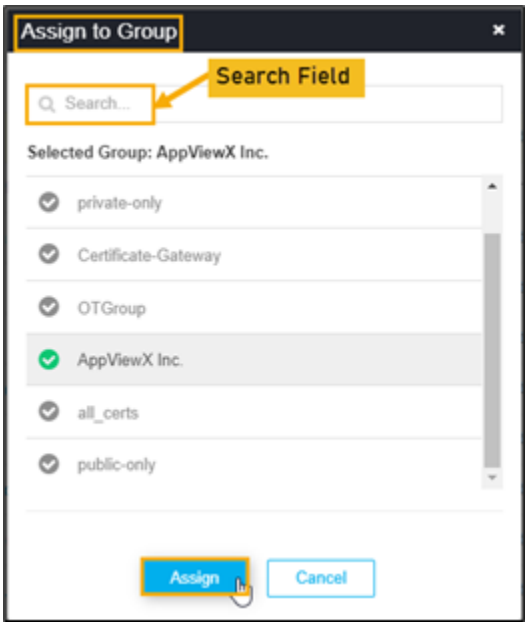


6. Click the **List** toggle button on the right top corner of the code signing certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to assign the group.
8. Click **Actions**, and then select **Assign Group** from the drop-down list.

   The **Assign Group** pop-up window appears.



a. Enter keywords if you want to search for a specific group from the list.
b. Select the desired group from the listed groups.
c. Click **Assign**.

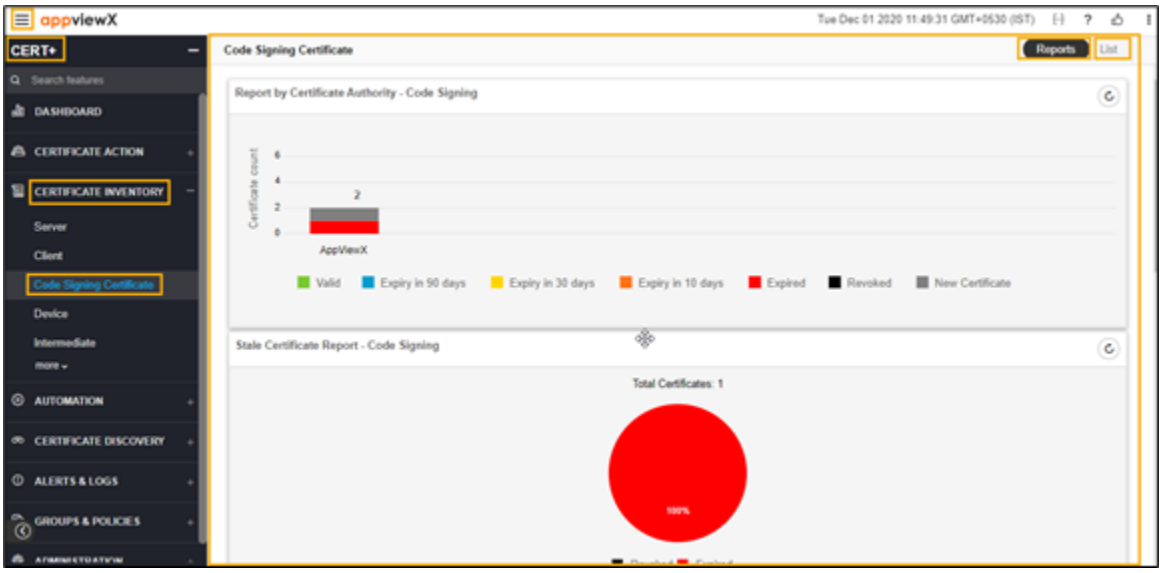
9. The certificate is assigned to a selected group.
   The pop-up message appears as **<certificate_name> assigned to <group_name>**.

Unassigning Code Signing Certificate Group

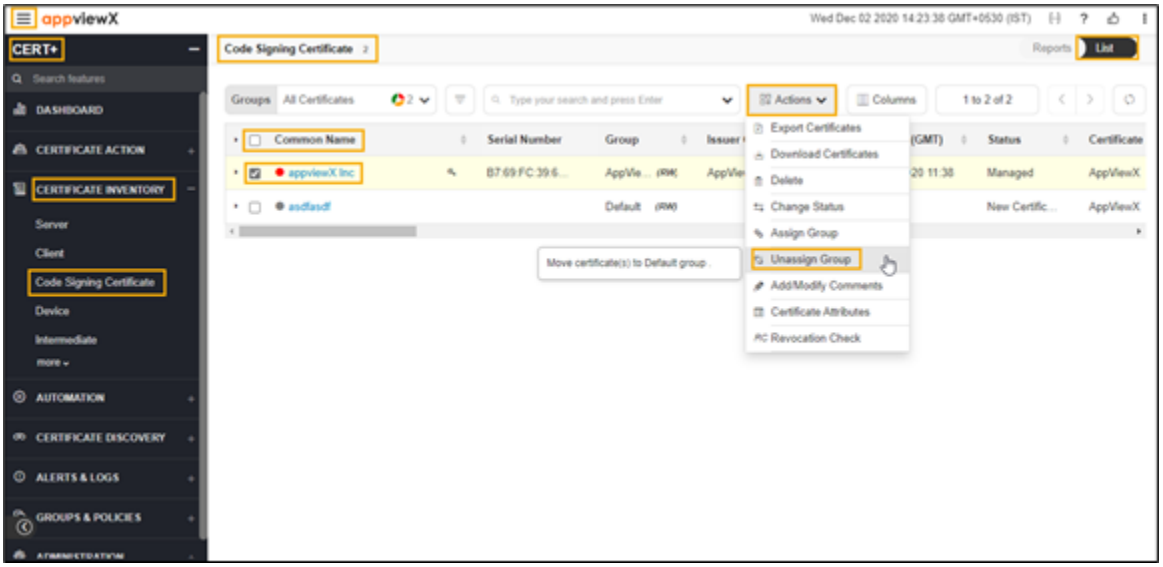
The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign the code signing 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. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.



6. Click the **List** toggle button on the right top corner of the client certificate page.

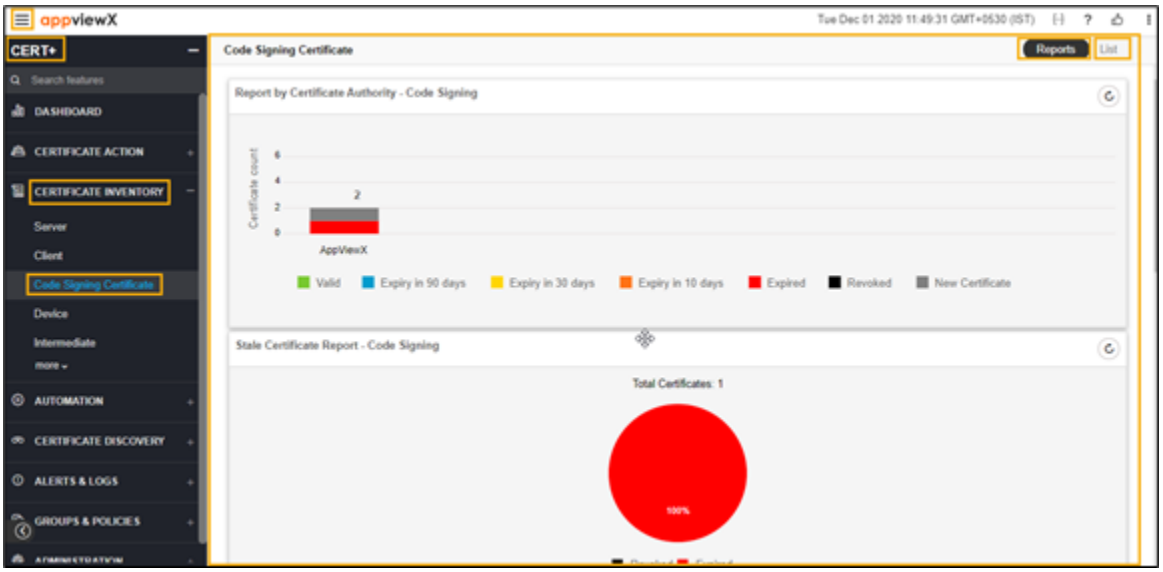


7. In the **Common Name** column certificate list, select the desired certificate that you want to unassign the group.
8. Click **Actions**, and then select **Unassign Group** from the drop-down list.
9. The selected certificate is assigned to the default group.
   The pop-up message appears as **<certificate_name> assign to undefined**.

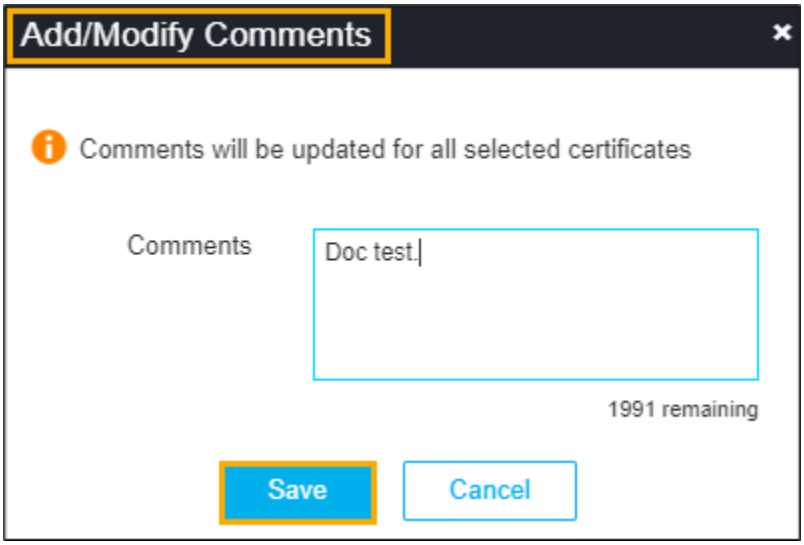
Add/Modify Comments for Code Signing Certificate

To add/modify the comments for code signing certificate,

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. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.

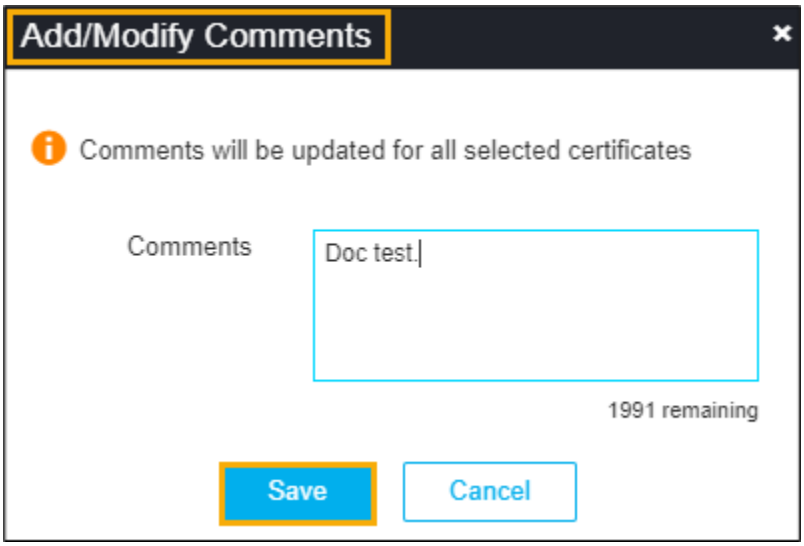


6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to add/modify the comments.

8. Click **Actions**, and then select **Add/Modify Comments** from the drop-down list.
   The **Add/Modify Comments** pop-up window appears.



   a. Enter the description in the comments field.

   b. Click **Save**.

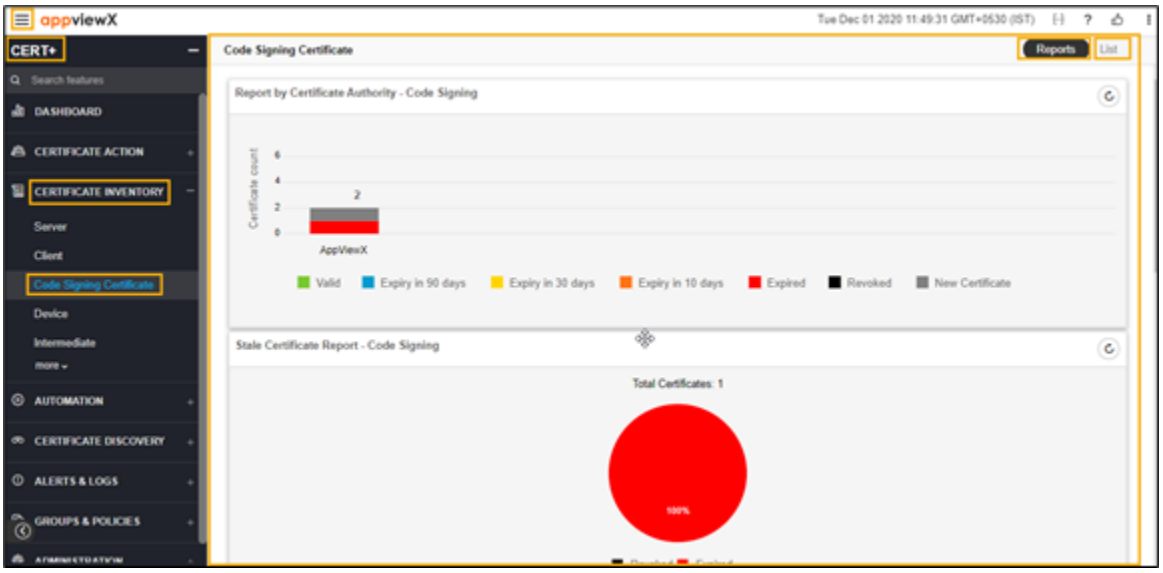
      The pop-up message appears as **Selected certificate(s) comment(s) uploaded**.

Updating Certificate Attributes for Code Signing Certificate

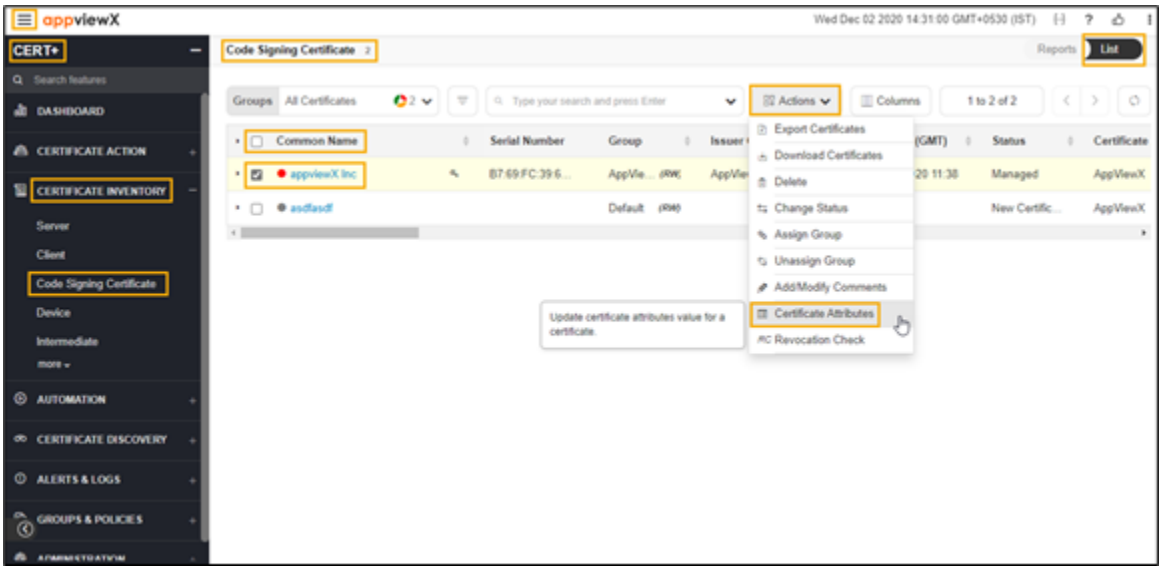
Other than the fields that are defined for CSR, the user can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update certificate attributes for code signing certificate,

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. Click **Code Signing Certificate**.
   The **Code Signing Certificate** page appears.



6. Click the **List** toggle button on the right top corner of the client certificate page.



7. In the **Common Name** column certificate list, select the desired certificate that you want to add attributes.
8. Click **Actions**, and then select **Certificate Attributes** from the drop-down list.

Device Certificate Inventory

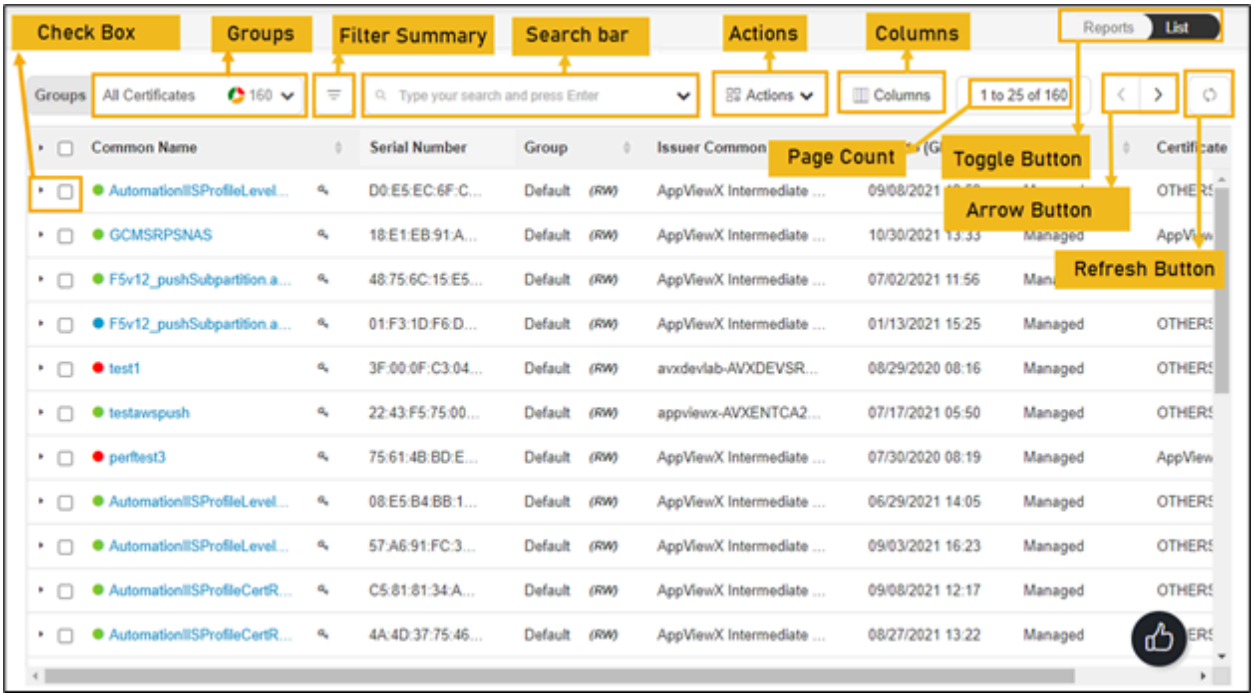
- Overview
- Exporting Device Certificate
- Deleting Device Certificate

Overview

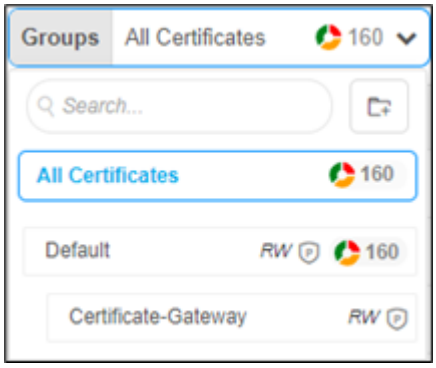
Device certificate inventory is where all the management interface certificates will be maintained. Currently, in this inventory, only F5 vendor certificates are shown.

On the **Certificate Inventory** > **Device Certificate** page, all the code signing certificates are listed. You can perform the following actions:

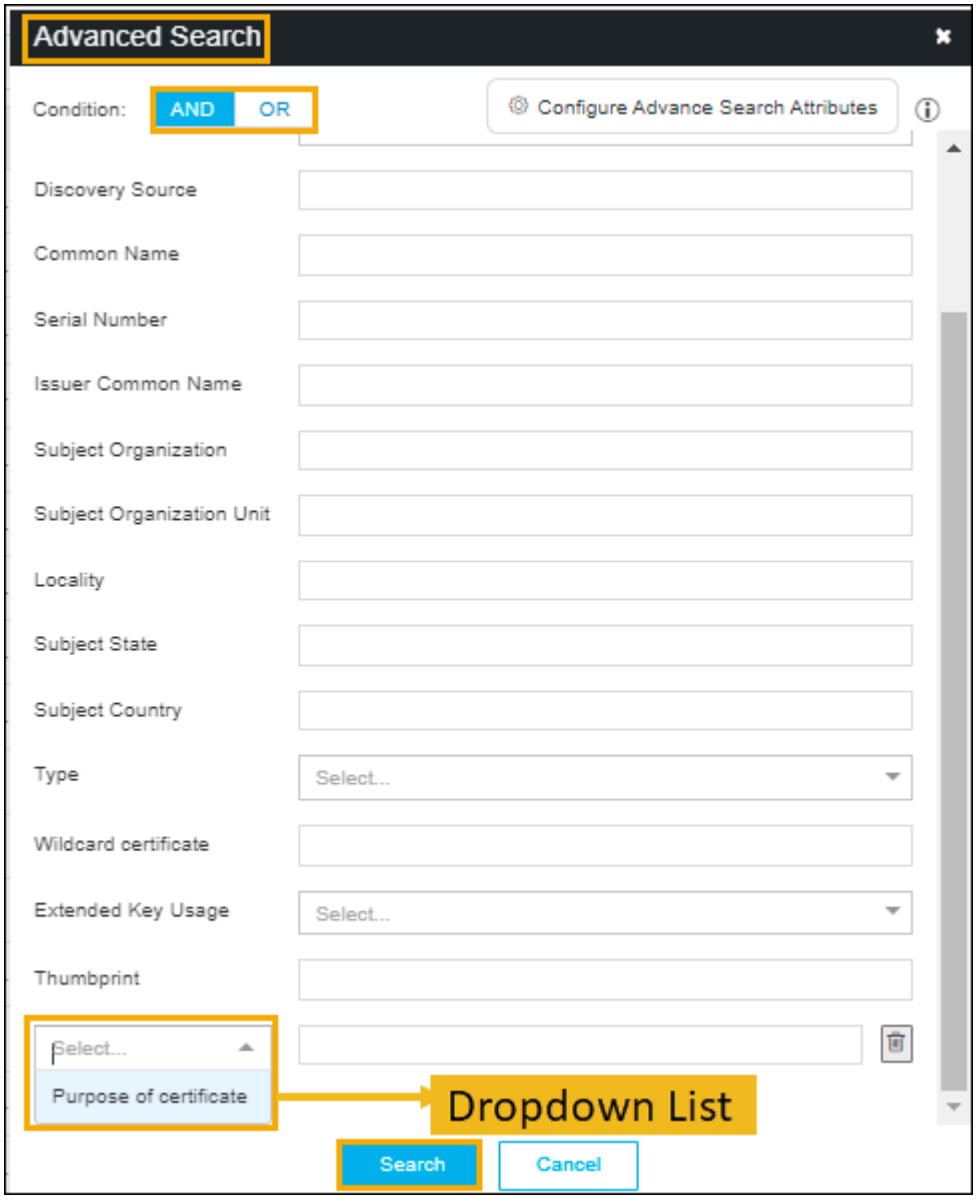
- **Export Certificates** - To export the device certificate
- **DeleteCertificates** - To delete the device certificate
- **DeleteCertificates** via Holistic View - To delete the device certificate via holistic view
- **Assign CertificateGroup** - To assign a group to the device certificate
- **Unassign CertificateGroup** - To Unassign a group from the device certificate
- **Add/Modify Comments** - To add/modify comments to the device certificate
- **Update Certificate Attribute** - To update certificate attributes for the device certificate.



The following table describes the options available on the device certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

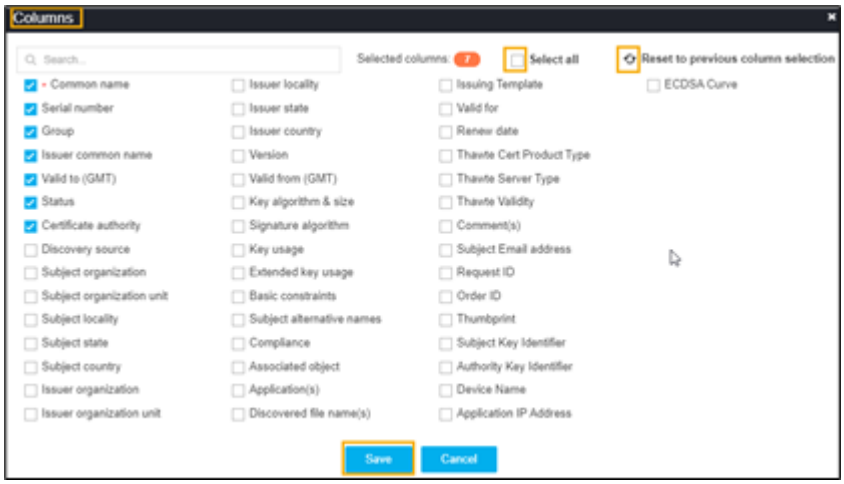


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

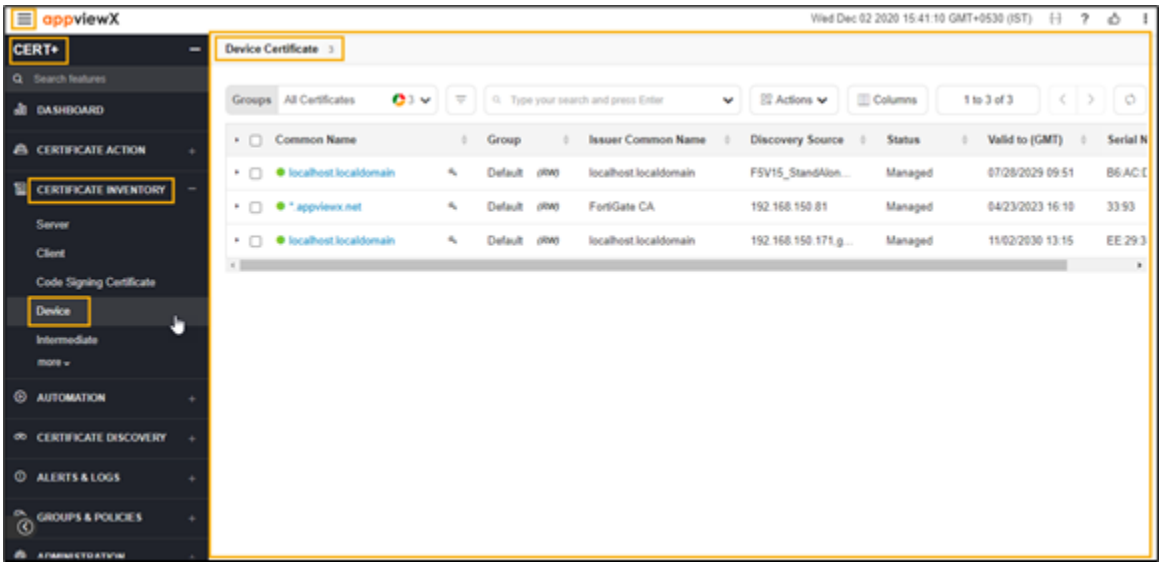
Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Exporting Device Certificate

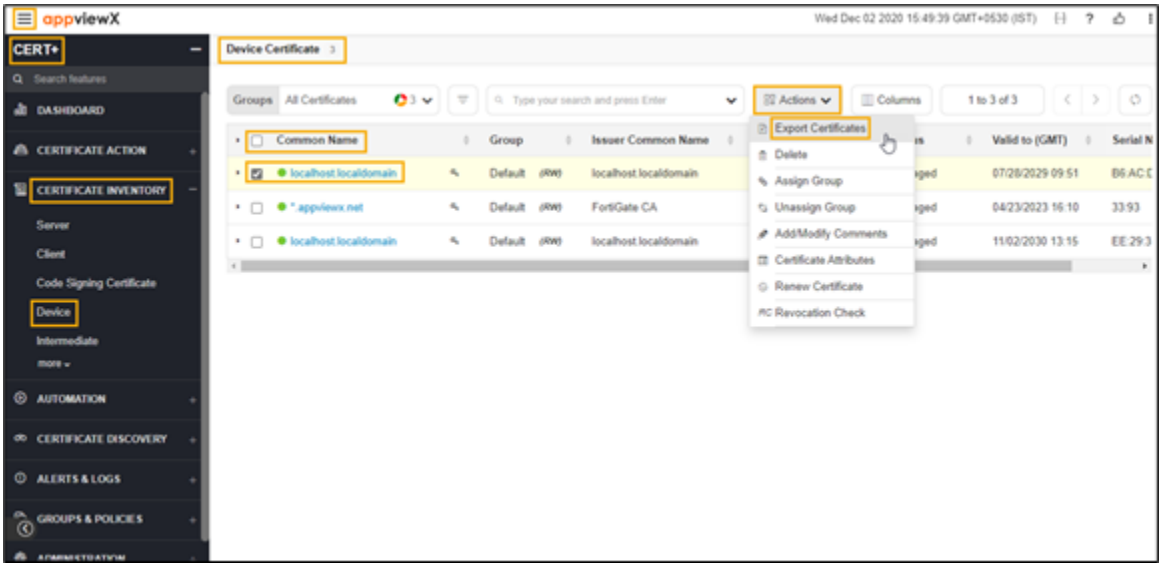
Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in <.xls> or <.csv> format. This can be used for reporting or making another inventory.

To export device certificate:

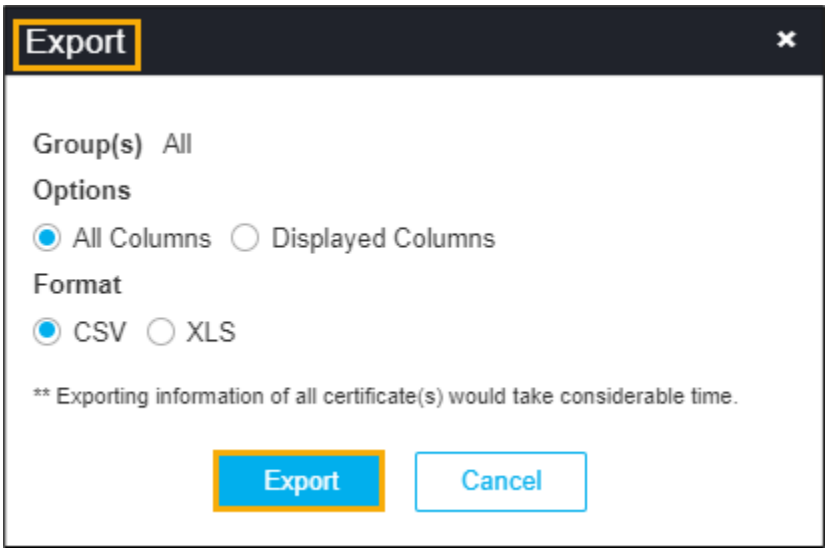
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Device**.
   The **Device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



6. In the **Common Name** column certificate list, select the desired certificate that you want to export a certificate.
7. Click **Actions**, and then select **Export Certificates** from the list.



The **Export** pop-up window appears.



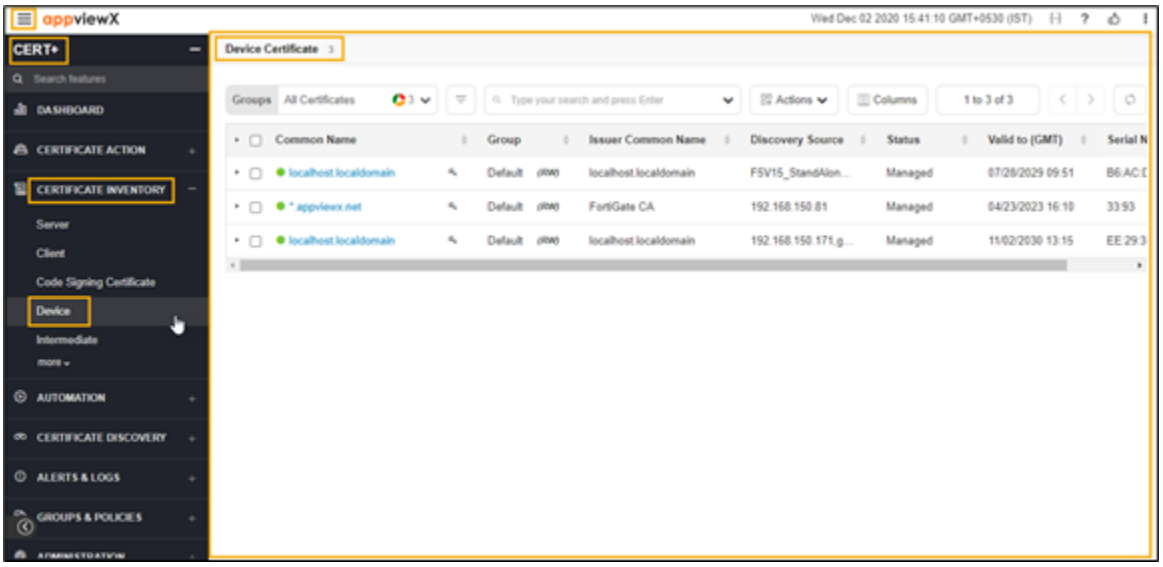
8. Select the desired **Options** and **Format** in the **Export** pop-up window.
   The selected certificate is exported to your local machine.

Deleting Device Certificate

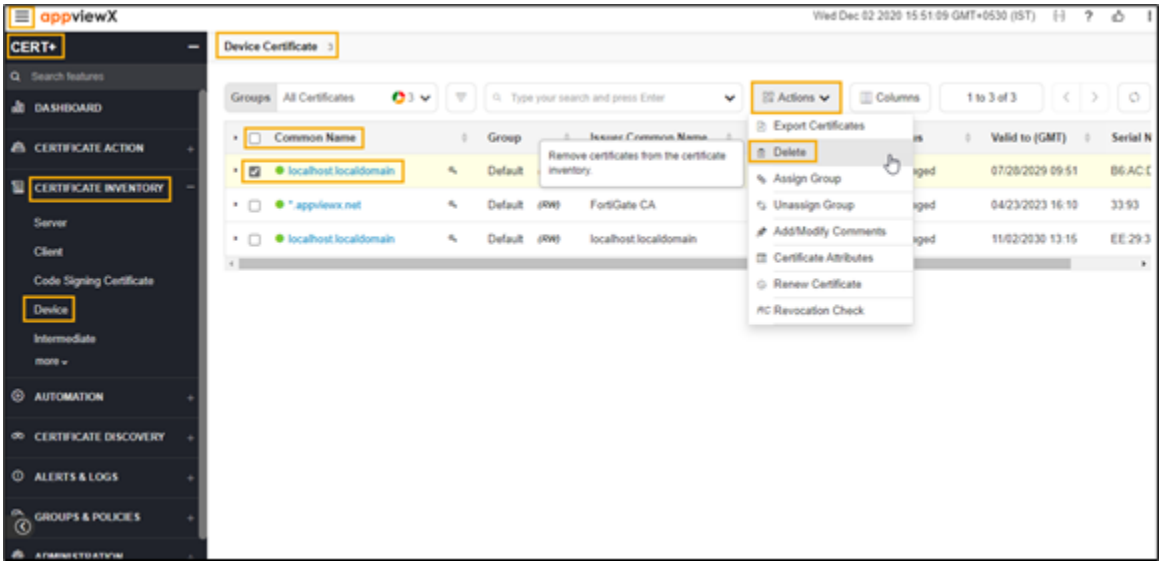
Deleting server certificate feature allows you to delete a certificate from the server certificate inventory only in AppViewX. Once the certificate gets deleted from the inventory, the same will not be shown in the reports and for alerts.

TSteps to delete device certificate,

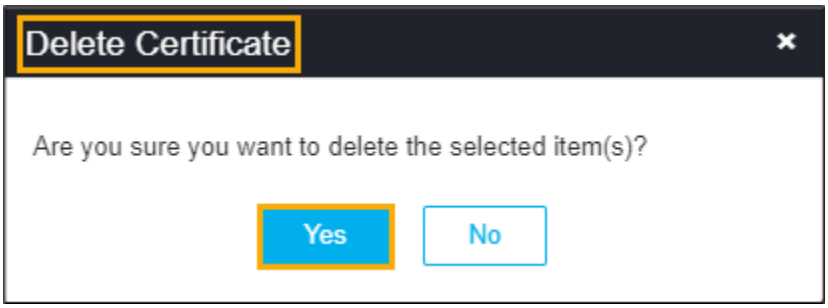
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **DeviceCertificate**.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



6. In the **Common Name** column certificate list, select the desired certificate that you want to delete.
7. Click **Actions**, and then select **Delete** from the list.



The **Delete Certificate** pop-up window appears.



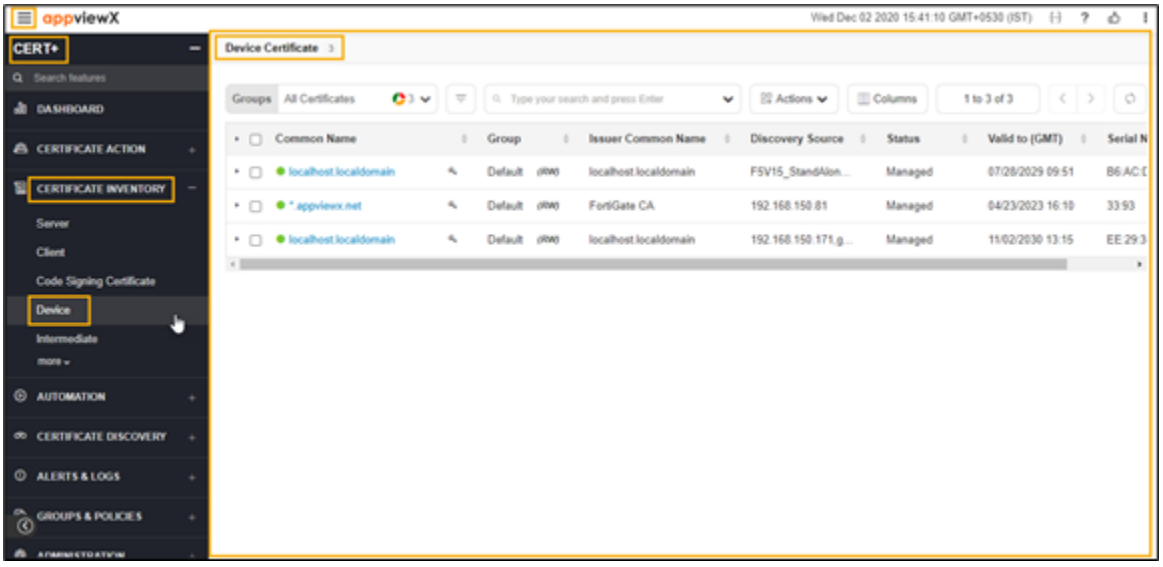
8. Click **Yes**.
   The device certificate is deleted and the pop-up message appears as "**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**".

Deleting Device Certificates via Holistic View

In the Holistic view, the user will find the entire chain of trust of the certificates along with the devices/ objects with which the certificates are associated. The primary actions that can be performed from the holistic view are Certificate creation, renewal, reissue, revoke, regenerate, install the certificates to the devices and objects. The other supported actions in the holistic view are download certificates and private keys, delete the certificate in the AppViewX certificate inventory, perform rollback action on the associated certificate and disassociate the certificate from the objects in the device.

To delete the device certificate via holistic view,

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. Click **Device Certificate**.
   The **Device Certificate** page appears.

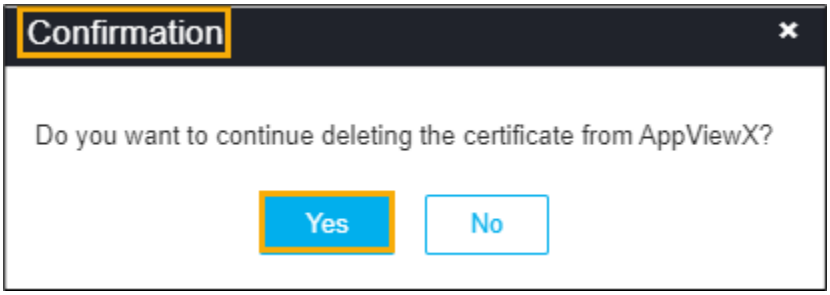


6. In the **Common Name** column certificate list, select the desired certificate that you want to delete the CA.

   The holistic view appears.

7. Click the vertical ellipse in the holistic view, and then select **Delete Certificate** from the list.

   The **Delete Certificate** pop-up window appears.



8. Click **Yes**.

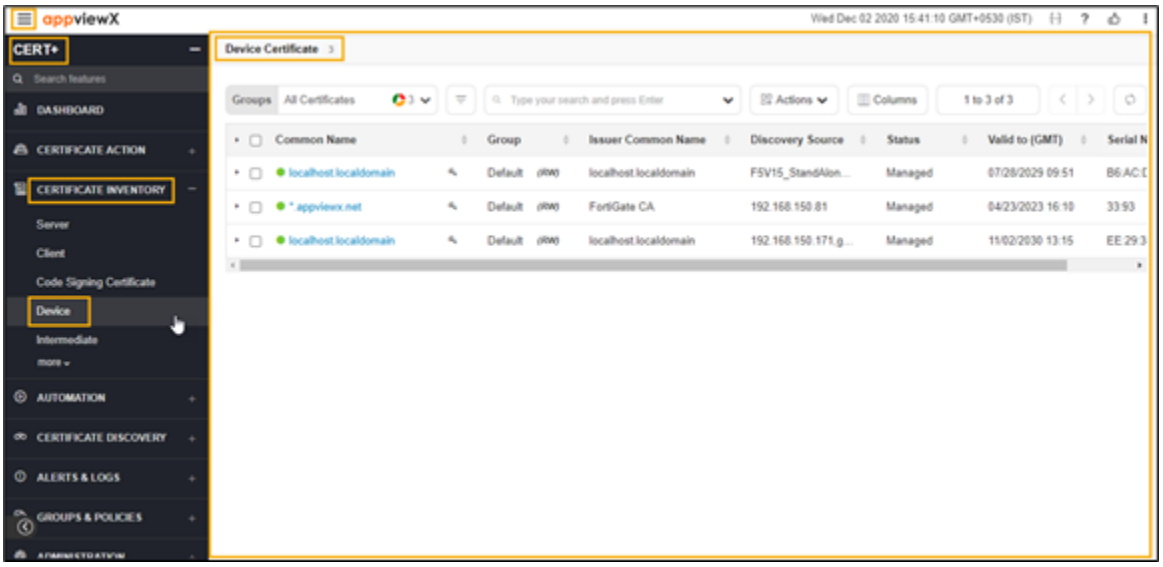
   The device certificate is deleted and the pop-up message appears as "**Selected certificate(s) with RW permission has been deleted from AppViewX inventory"**.

Assigning Device Certificate Group

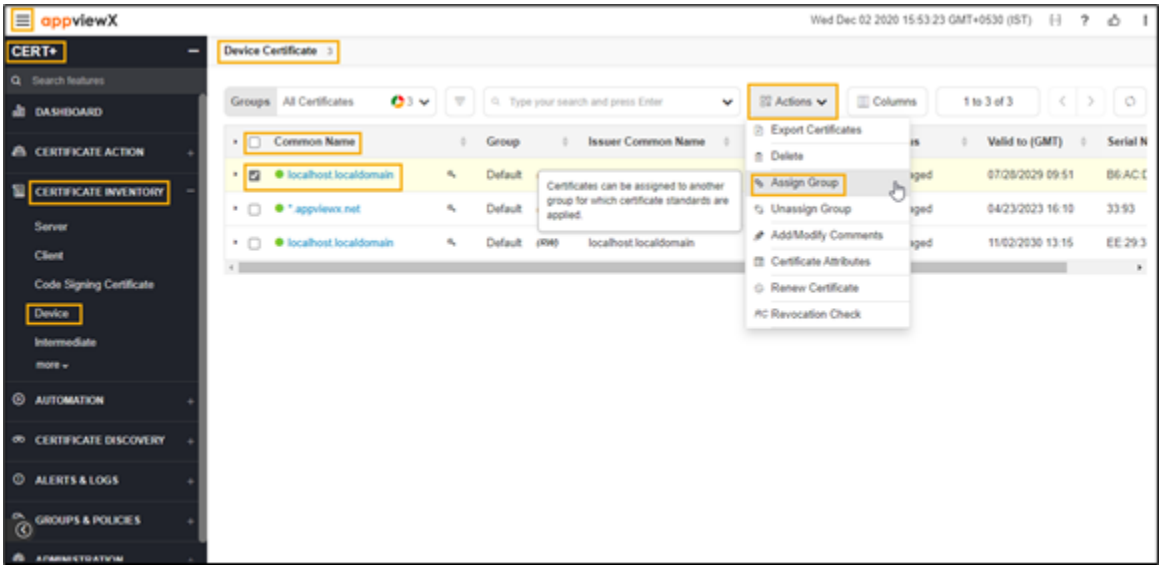
The certificates of any common criteria can be grouped together to perform compliance checks against the policy details, to enable auto-renewal and auto-push operations. The viewing of the certificates can also be done on a group basis.

To assign the device certificate group,

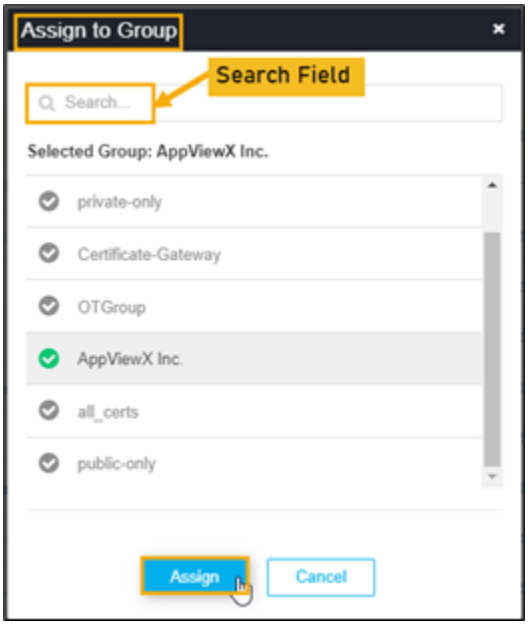
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Device Certificate**.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



6. In the **Common Name** column certificate list, select the desired certificate that you want to migrate to the CA.
7. Click **Actions**, and then select **Assign Group** from the list.



The **Assign to Group** pop-up window appears.



8. Enter keywords if you want to search for a specific group from the list.
9. Select the desired group from the listed groups.
10. Click **Assign**.

    The certificate is assigned to the selected group. The pop-up message appears as **<certificate_name> assigned to <group_name>**.

Unassigning Device Certificate Group

The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

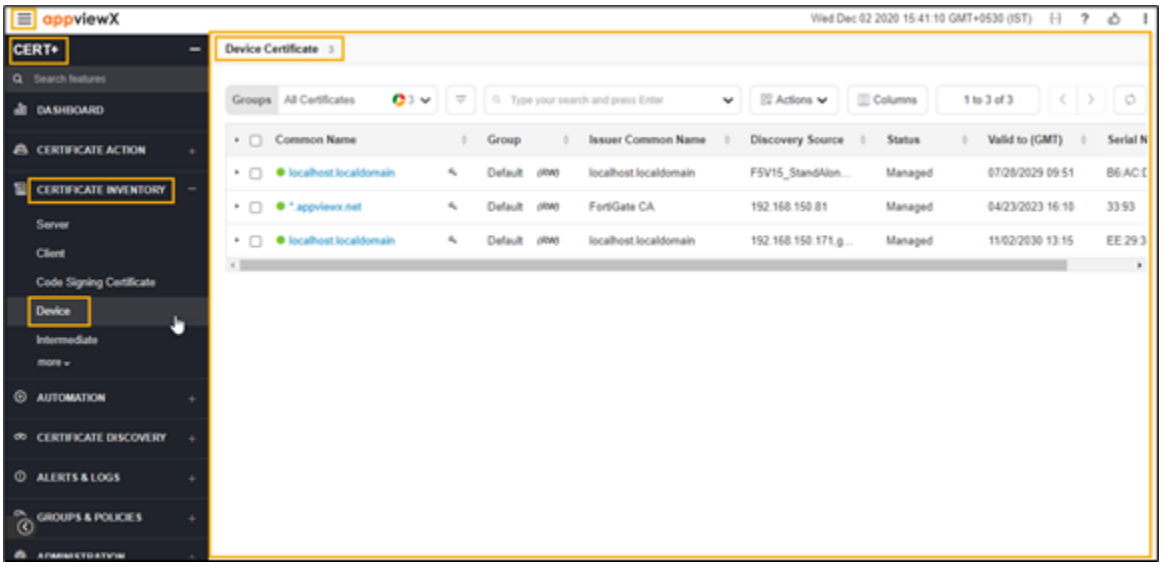
To unassign the device certificate group,

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

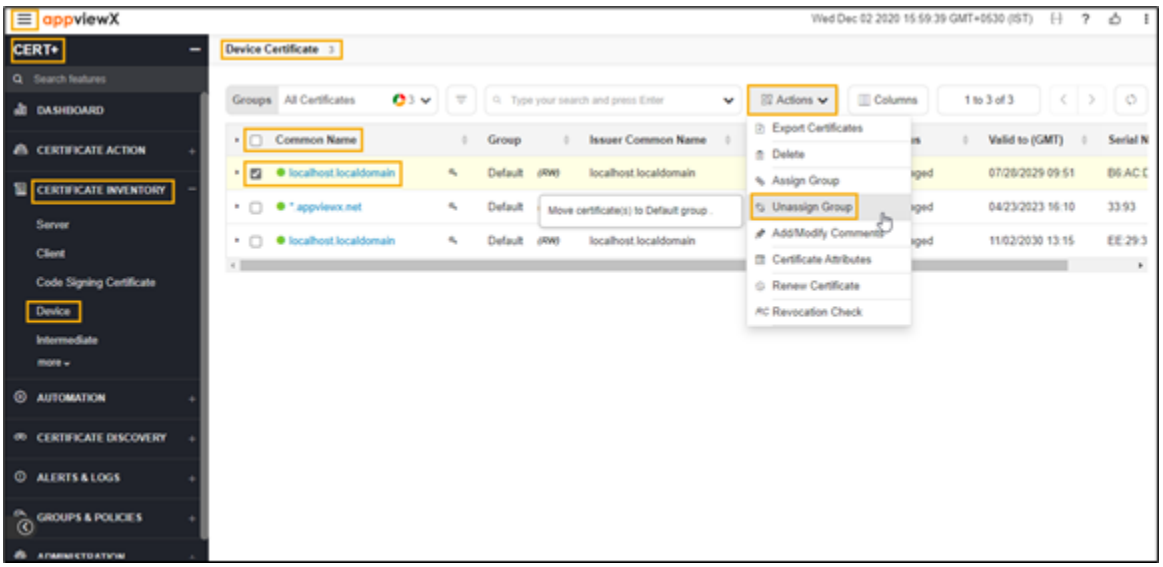
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Device Certificate**.

   The **Device Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate that you want to unassign.
7. Click **Actions**, and then select **Unassign Group** from the list.



8. The selected certificate is assigned to the default group.
   The pop-up message appears as **<certificate_name> assign to undefined**.

Add/Modify Comments for Device Certificate

To add/modify the comments for device certificate,

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.

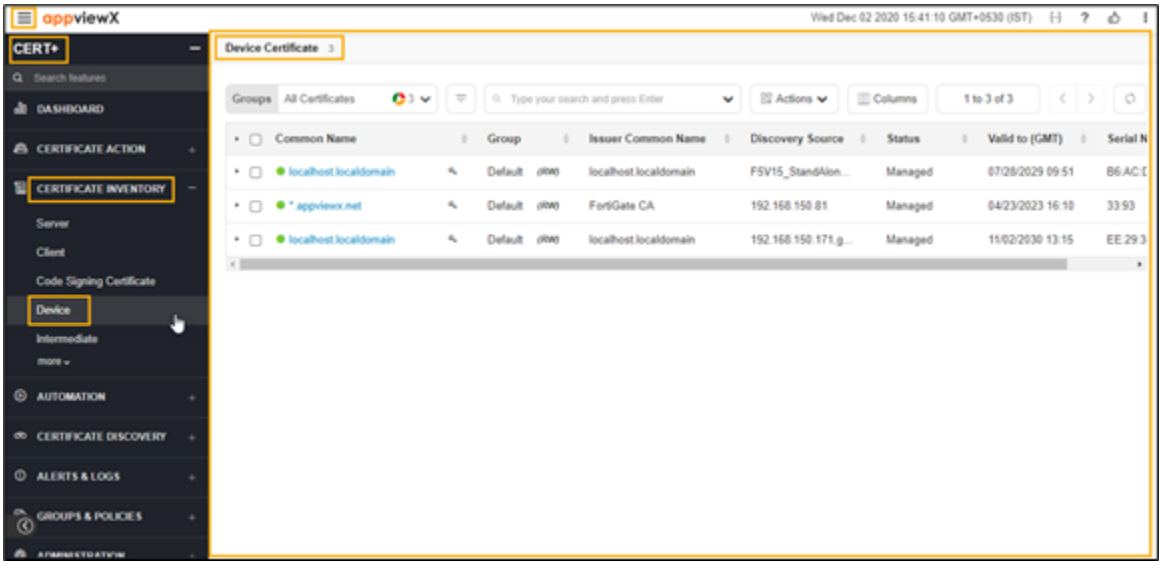
3. Click **CERT+**.

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

4. Expand **CERTIFICATE INVENTORY**.

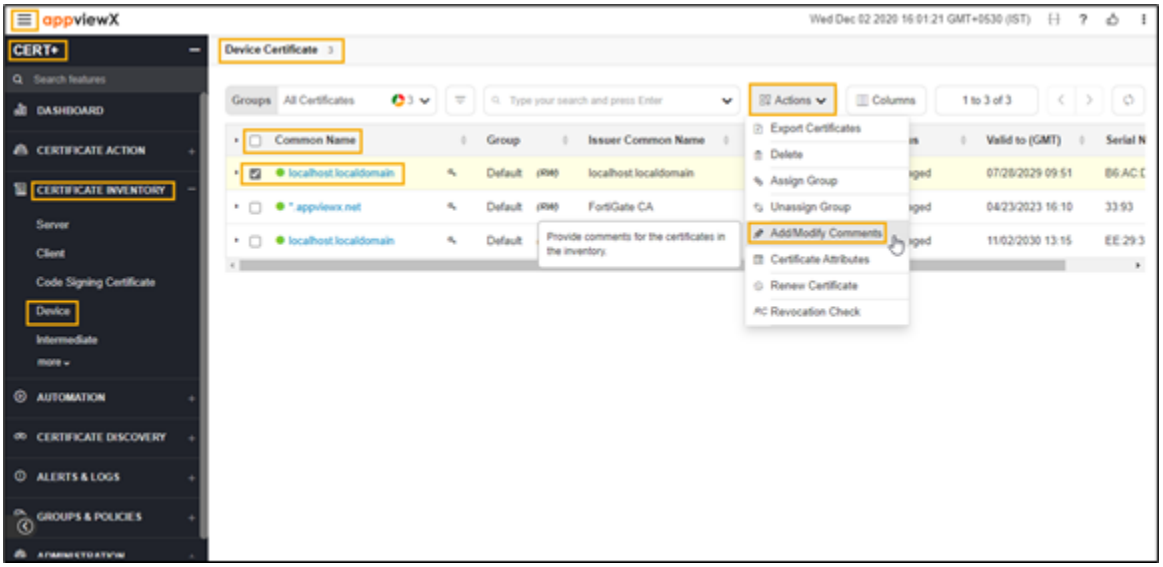
5. Click **Device Certificate**.

   The **Device Certificate** page appears.

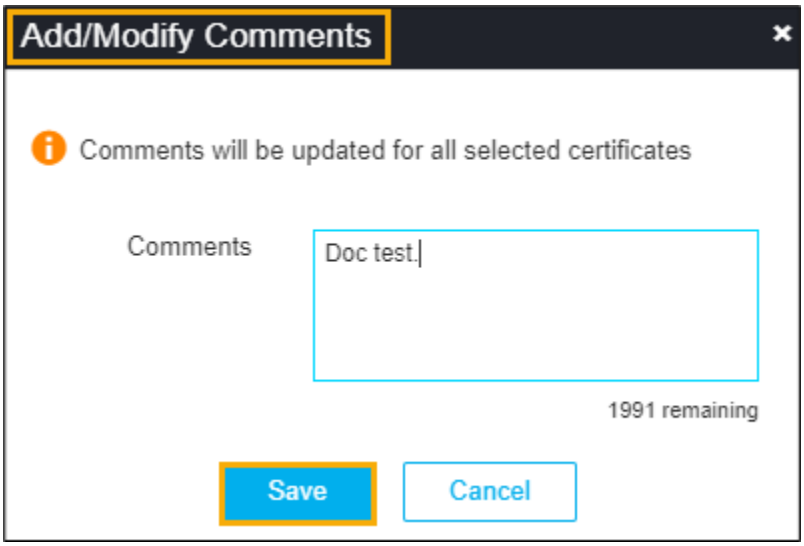


6. In the **Common Name** column certificate list, select the desired certificate that you want to add/modify the comments.

7. Click **Actions**, and then select **Add/Modify Comments** from the list.



8. The **Add/Modify Comments** pop-up window appears.



9. Enter the description in the **Comments** field.
10. Click **Save**.

    The pop-up message appears as "**Selected certificate(s) comment(s) uploaded**".

Updating Certificate Attributes for Device Certificate

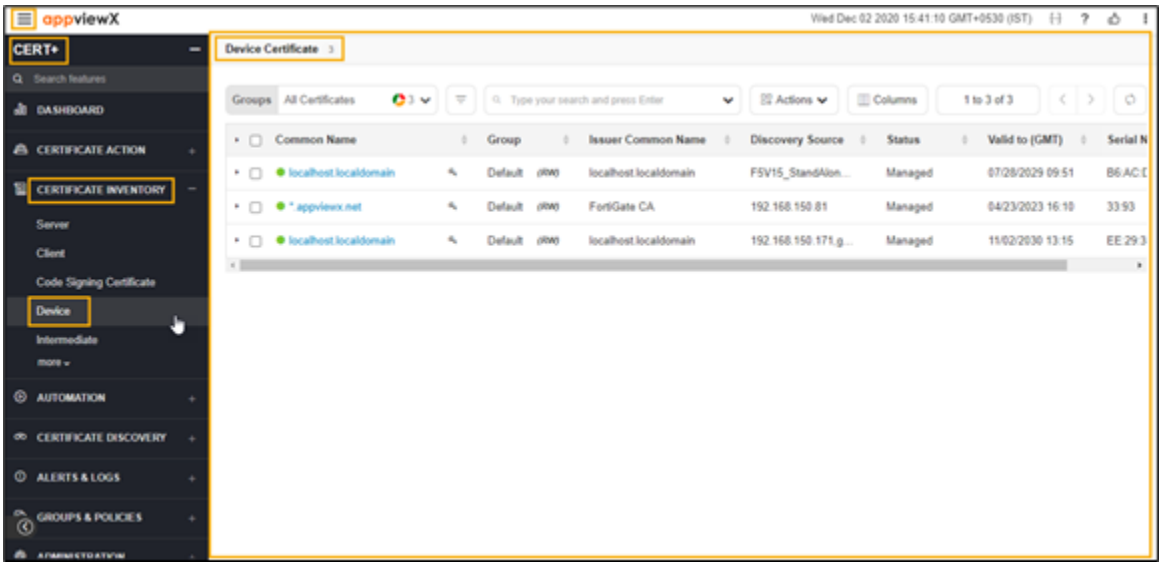
To view the attributes for a device certificate,

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

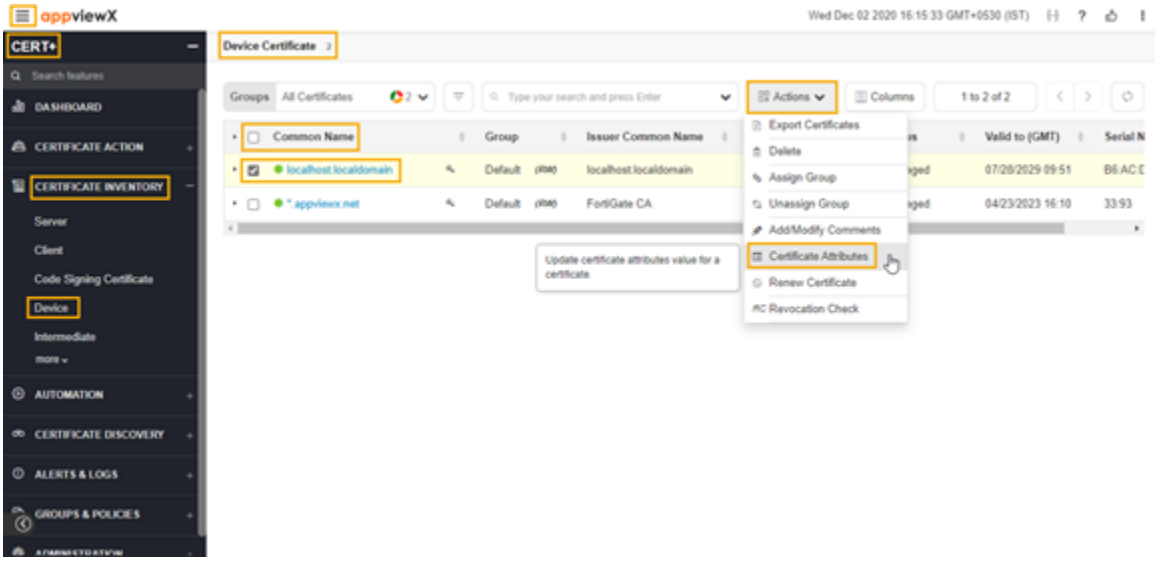
   The left navigation pane appears.
3. Click **CERT+**.

   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Device Certificate**.

   The **Device Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate that you want to add attributes.
7. Click **Actions**, and then select **Certificate Attributes** from the list.



Intermediate Certificate Inventory

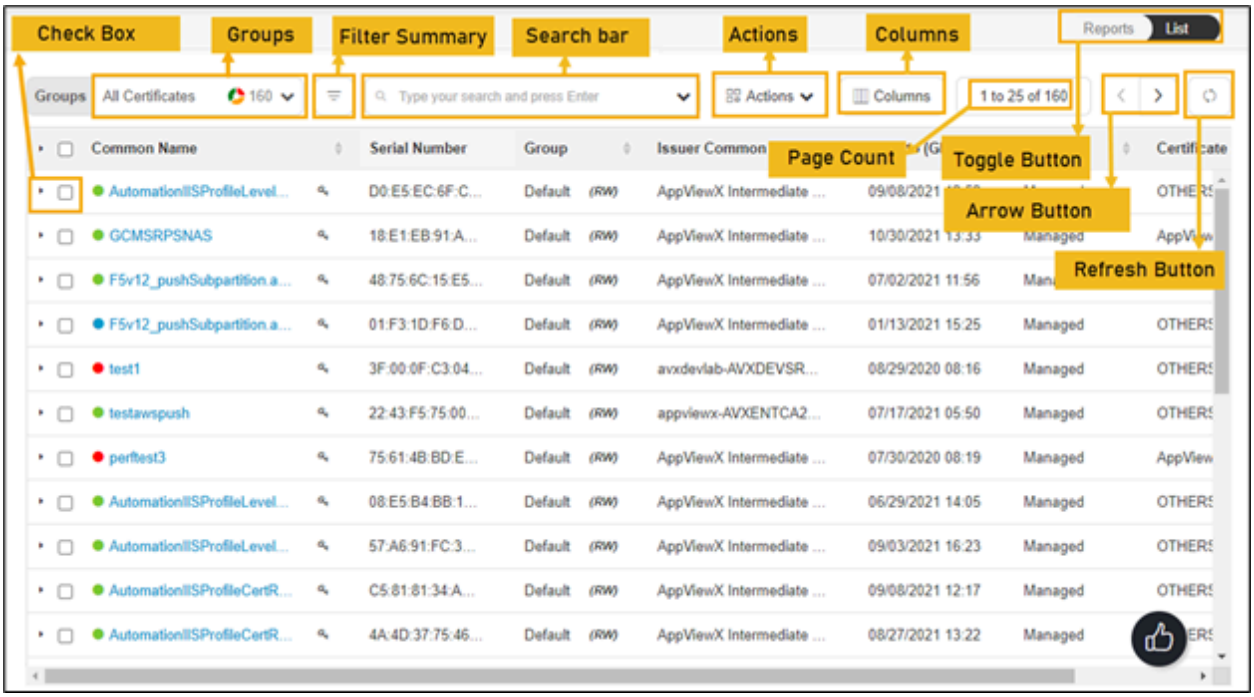
- Overview
- Deleting Intermediate Certificate
- Downloading Intermediate Certificate via Holistic View

Overview

Intermediate certificate inventory is where the issuer certificates apart from the root certificate will be displayed. In the chain of trust, if there is more than one layer of the intermediate certificate (excluding root and end certificate), all those certificates will be shown in this inventory. From this inventory, the user can get into the holistic view where the user can perform the push operation of the intermediate and its root certificates.

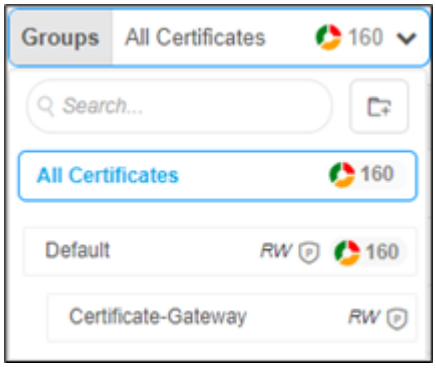
In the **Certificate Inventory** > **Intermediate Certificate** page, all the intermediate certificates are listed. You can perform the following actions:

- **Delete Certificate** - To revoke the device certificate
- **Download Certificate** - To regenerate the device certificate.

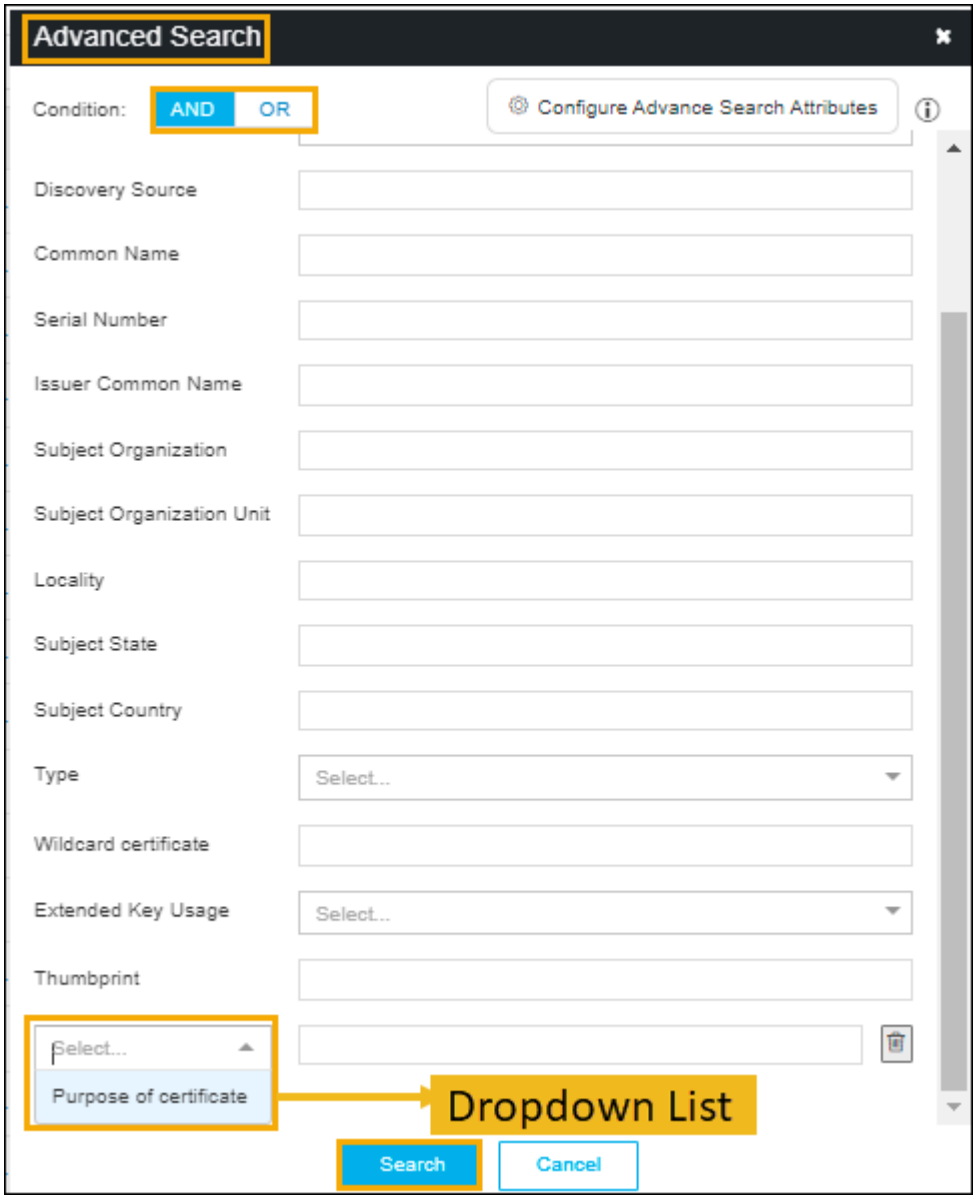


The following table describes the options available on the intermediate certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected.

Options	Description
	
Filter Summary	Displays number of certificates in which state. 
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

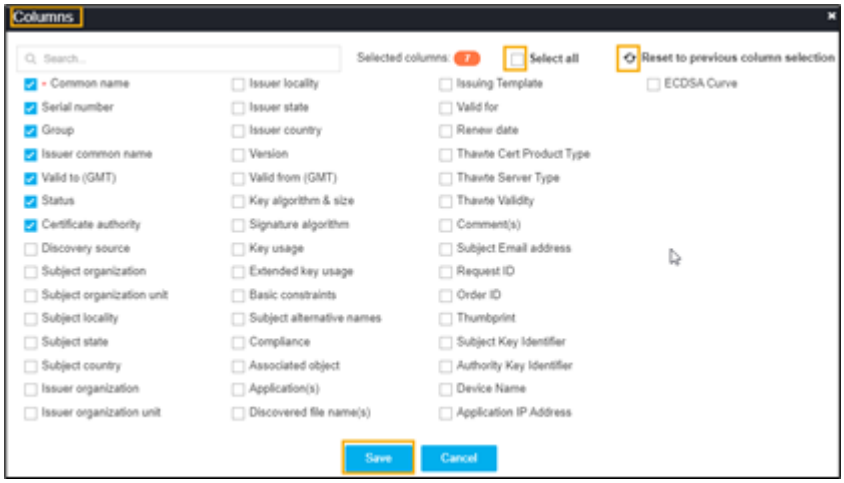


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

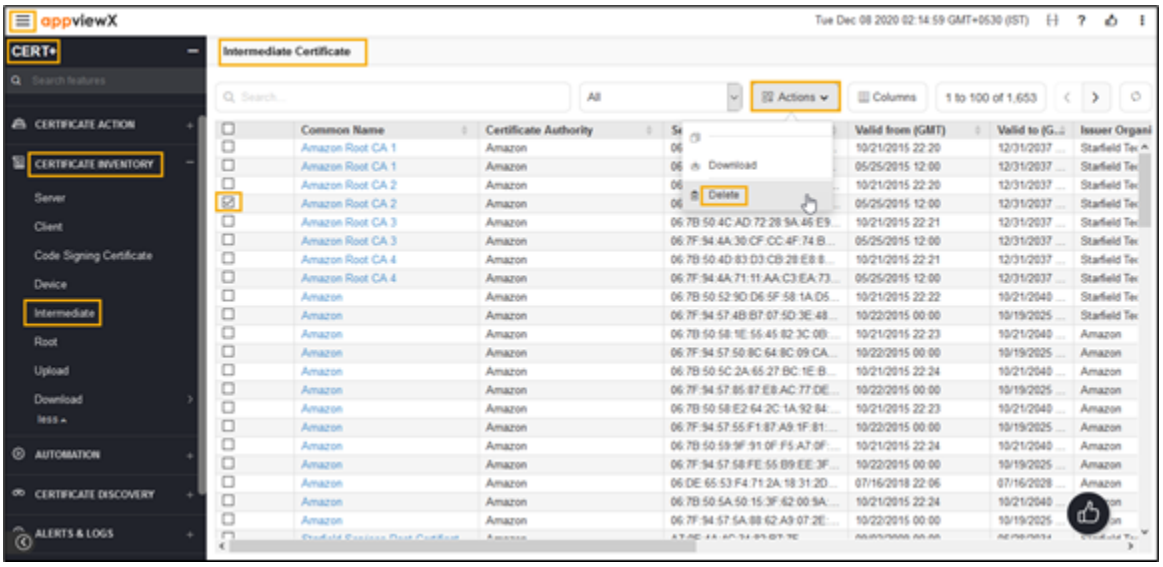
Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

Deleting Intermediate Certificate

Deleting intermediate certificate will delete the certificate from the intermediate certificate inventory only in AppViewX. Once the certificate gets deleted from the inventory, the same will not be shown in the reports and for alerts.

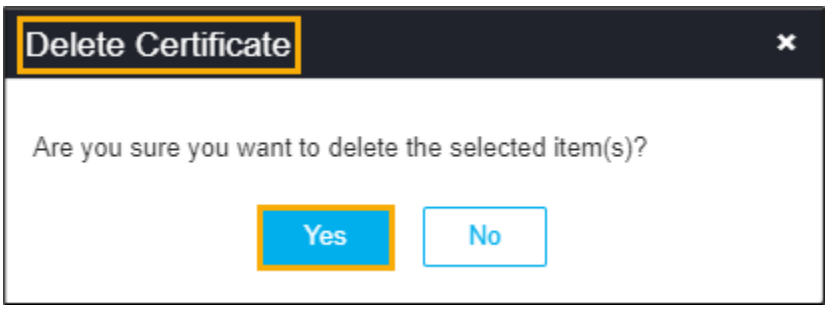
To delete the intermediate certificate,

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. Click **Intermediate**.
   The **Intermediate Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to delete.
7. Click **Actions**, and then select **Delete**.

   The **Delete Certificate** pop-up window appears.



8. Click **Yes**.

   The client certificate is deleted and the pop-up message appears as “**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**”.

Downloading Intermediate Certificate via Holistic View

Download intermediate certificate can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download intermediate certificate via holistic view,

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.

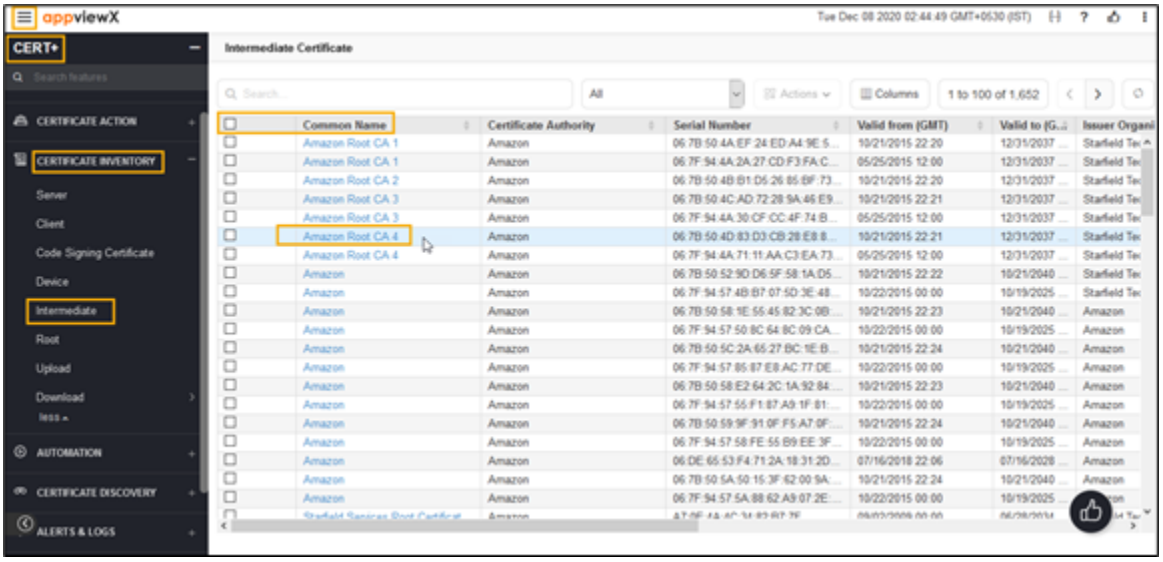
3. Click **CERT+**.

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

4. Expand **CERTIFICATE INVENTORY**.

5. Click **Intermediate**.

   The **Intermediate Certificate** page appears.

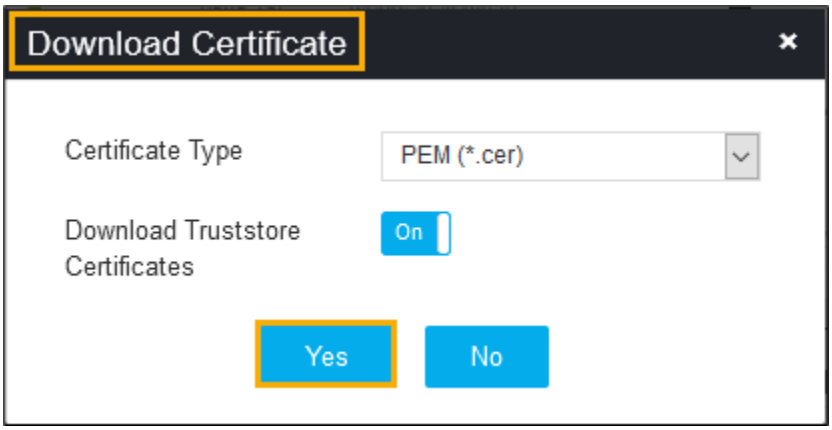


6. In the **Common Name** column certificate list, select the desired certificate that you want to download the CA.

   The holistic view appears.

7. Click vertical ellipse in the holistic view, and then select **Download Certificate** from the list.

   The **Download Certificate** pop-up window appears.



a. Select the file format from the **Certificate Type** list.
b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.

8. Click **Yes**.
   The certificate is downloaded to your local machine.

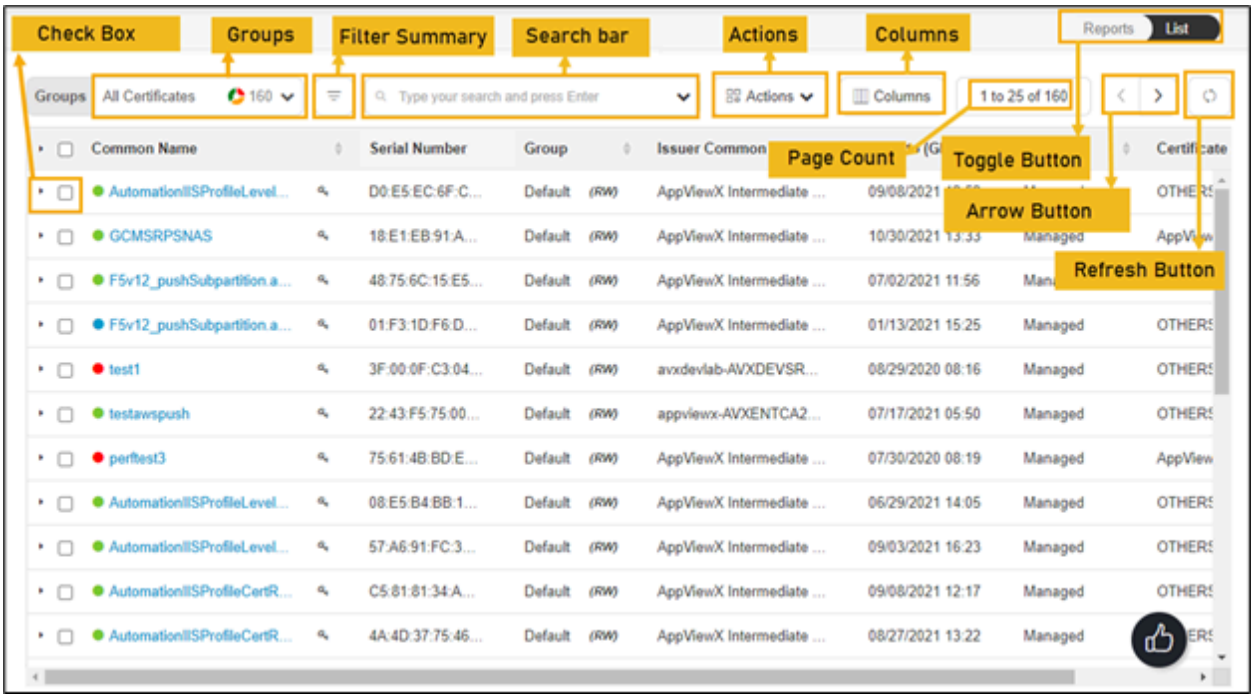
Root Certificate Inventory

Overview

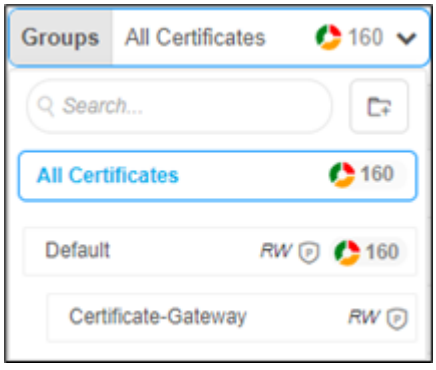
Root certificate inventory is where the root certificate of all the issuer certificates will be maintained. For any chain of trust certificates, there can be only one root certificate. From this inventory, the user can get into the holistic view where the user can perform the push operation of the root certificate only.

In the **Certificate Inventory** > **Root Certificate** page, all the root certificates are listed. You can perform the following actions:

• **Delete Certificate** - To revoke the device certificate
• **Download Certificate** - To regenerate the device certificate.

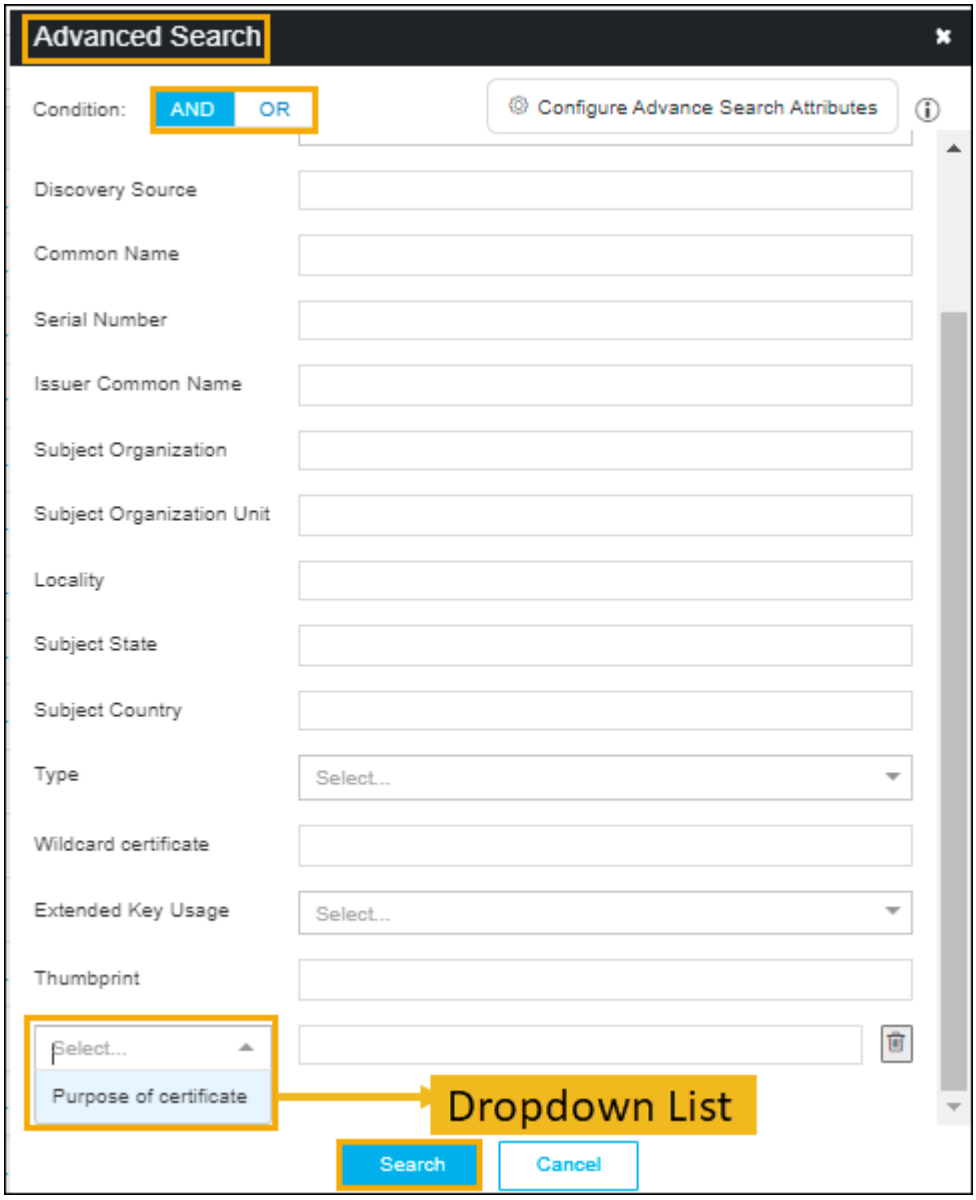


The following table describes the options available on the root certificate inventory page:

Options	Description
Check Box	Select the check box of the certificate that needs to be renewed.
Groups	Displays the group of certificates that needs to be displayed as selected. 
Filter Summary	Displays number of certificates in which state.

Options	Description
	
Search Bar (Basic/ Advanced)	Searches for the given keyword in the field and results in the feature that matches the search keyword. Basic Search - Searches in the given keyword in the field and results from the feature that matches the search keyword. Advanced Search - The advanced search is used to perform quick searches of the data. If a more specific needs to be composed, the advanced search bar is a readily available option. To activate the advanced search bar, click the Chevron icon in the search field. The advanced search page appears.

Options	Description

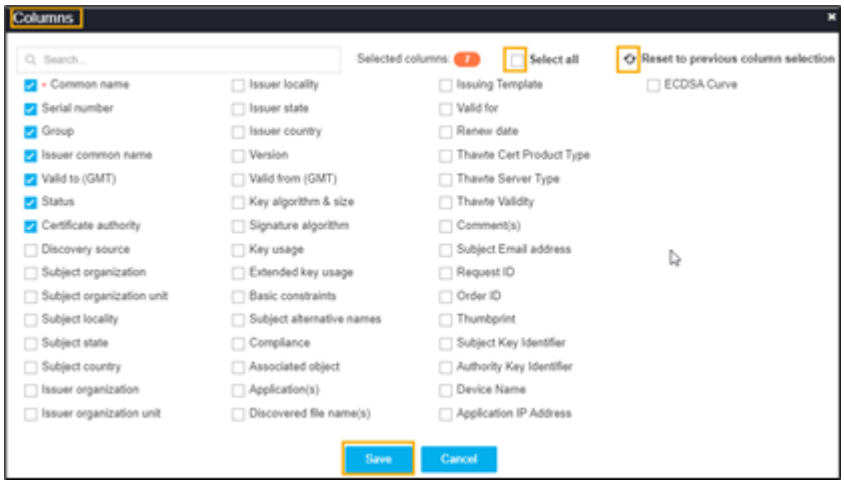


The following table describes the options available in the Advanced Search feature:

Options	Description
Condition	Displays the type of the desired search on the page. The possible options are, • AND • OR.

Options	Description

Options	Description
Certificate Authority	Allows you to select the desired CA from the dropdown list.
Status	Allows you to select the desired status certificate. The possible options are, • Manage • Monitor • New certificate.
Discovery Source	Enter the source of the discovery.
Common Name	Enter the common name of the certificate.
Serial Number	Enter the serial number of the certificate.
Issuer Common Name	Enter the name of the certificate issuer.
Subject Organization	Enter the subject of the organization.
Subject Organization Unit	Enter the subject of the organization’s unit.
Locality	Enter the specific locality.
Subject State	State Enter the state of the certificate’s subject.
Subject Country	Country of the subject.
Type	Type of the certificate.
Wildcard certificate	Enter the wildcard certificates.
Extended Key Usage	Allows you to select the EKU from the dropdown list.
Thumbprint	Enter the thumbprint value that you get it from the certificate details page.
Dropdown List	Select the custom attributes from the dropdown list.
Search	Click the Search button to get the results from the search.

Options	Description
Actions	Displays the list of actions. The possible actions are, • Export Certificates • Download Certificates • Delete • Change Status • Assign Group • Unassign Group • Add/Modify Comments • Certificate Attributes • Renew Certificate • Revoke Certificate • CA Switch • Revocation Check.
Columns	Allows you to select the number of desired columns to show on the certificate page.  • Search bar - Used to search the available options. • Click Select all check box if all parameters required to be displayed. • Click the refresh icon if you want to reset the previous columns. • Click Save.

Options	Description
Page Count	Displays the number of certificates listed on the page.
Toggle Button	Displays the desired dashboard report on the page. The available options are, • Reports • List.
Arrow Button	Allows you to move next page.
Refresh Button	Allow you to refresh the current page.

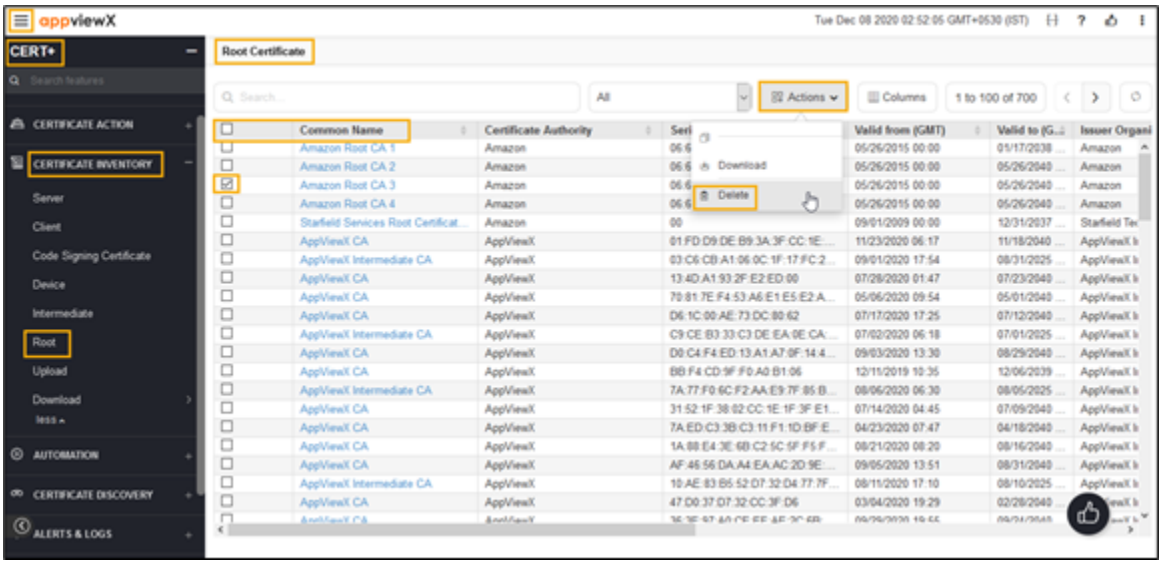
Deleting Root Certificates

During download of the root certificate from both inventory and holistic view, the certificate gets downloaded in PEM <.*crt*> format

in the inventory, the user can select one or more certificates and download them in .crt format. From the holistic view, only one certificate can be downloaded at a time.

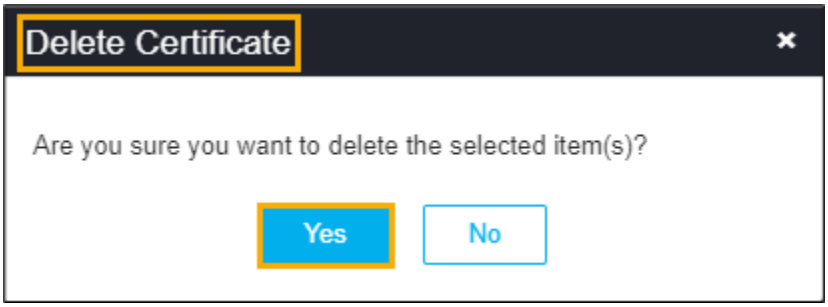
To delete the root certificate,

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. Click **Root**.
   The **Root Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate that you want to delete.
7. Click **Actions**, and then select **Delete** from the list.

   The **Delete** pop-up window appears.



8. Click **Yes**.

   The client certificate is deleted and the pop-up message appears as “**Selected certificate(s) with RW permission has been deleted from AppViewX inventory**”.

Downloading Root Certificates via Holistic View

Download root certificate is the action to download root certificate in PEM format with or without its trust store certificates.

To download the root certificate via holistic view,

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.

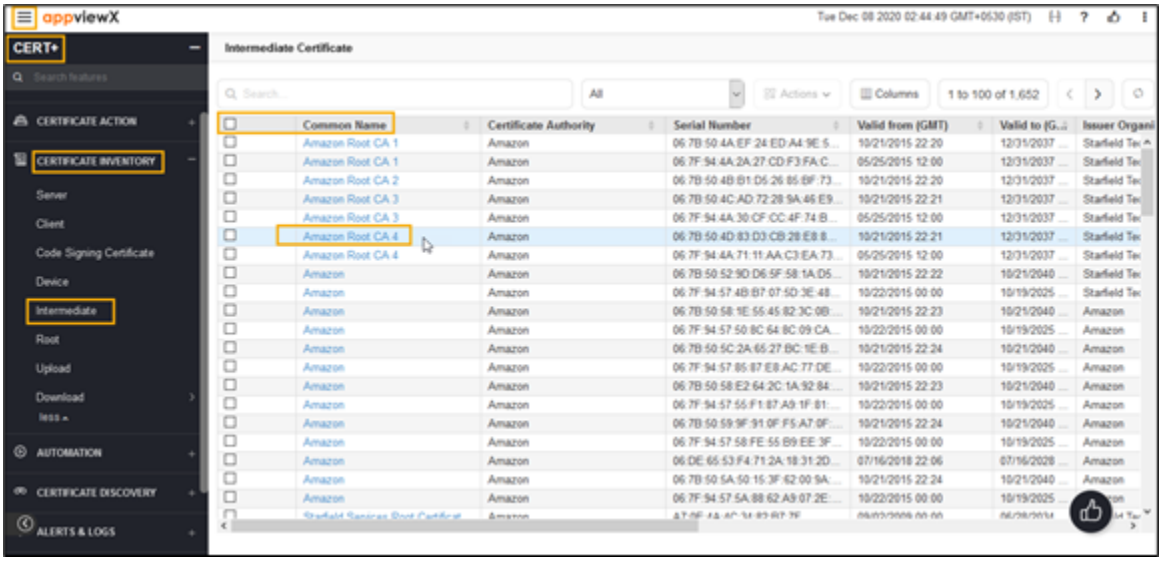
3. Click **CERT+**.

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

4. Expand **CERTIFICATE INVENTORY**.

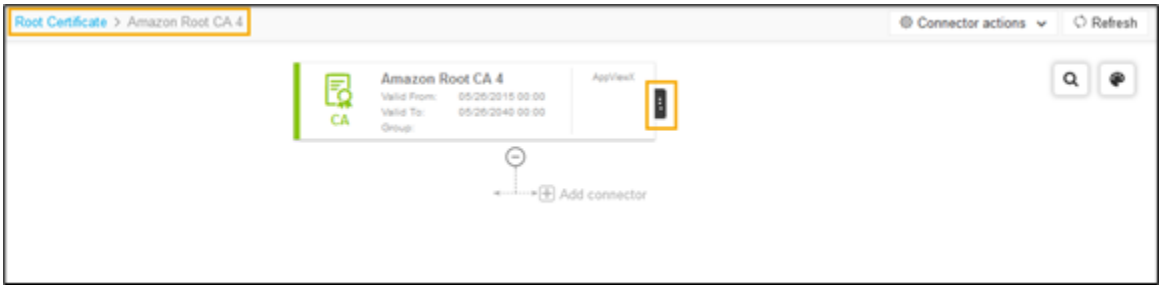
5. Click **Root**.

   The **Root Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate that you want to download the CA.

   The holistic view appears.



7. Click vertical eclipse in the holistic view, and then select **Download Certificate** from the list.

   The **Download Certificate** pop-up window appears.

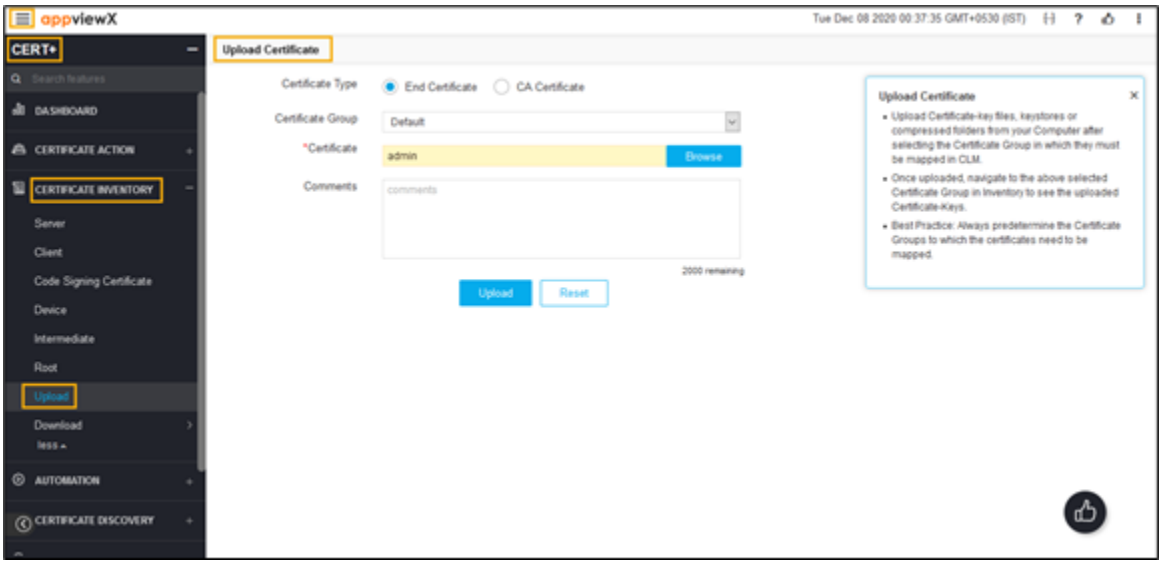
8. Select the file format from the **Certificate type** list.
9. Click **Yes**.
   The certificate is downloaded to your local machine.

Uploading Certificate

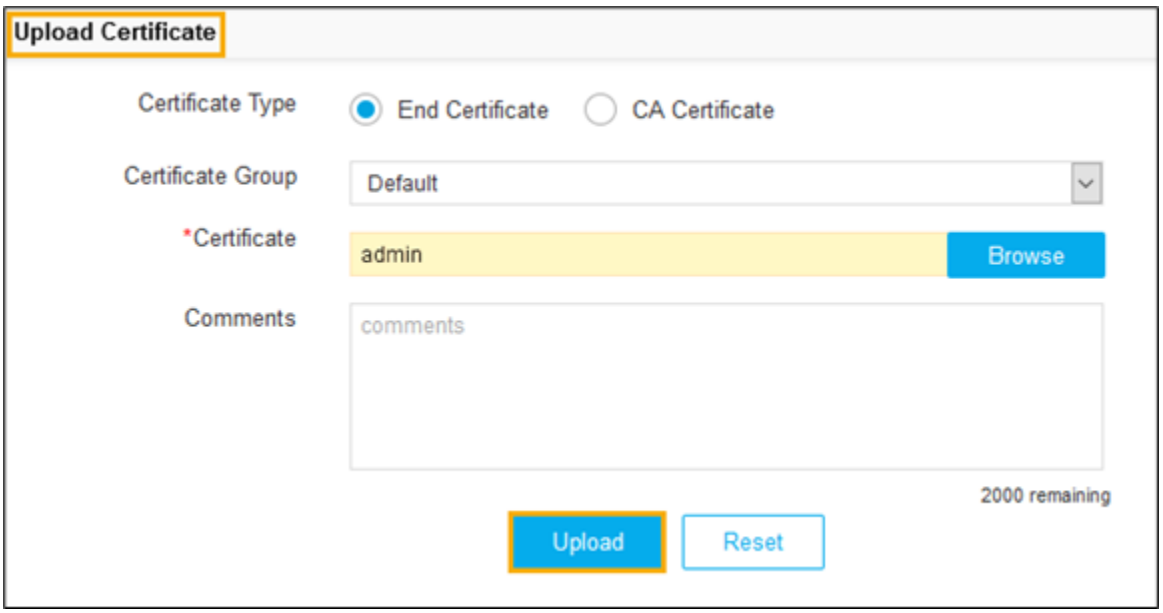
Upload certificate is the action to upload either the end certificate or trust store certificates in the certificate inventory. Once uploaded, the certificate will be applied by the policy based on the associated certificate group.

To upload a certificate,

1. 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. Click **Upload**.
   The **Upload Certificate** page appears.



6. In the **Upload Certificate** page, select/enter the details as follows:



The following table describes the options available on the upload certificate page:

Field	Description
Certificate Type	Click the check box to select the desired certificate type. The possible types are: • End Certificate • CA Certificate.
Certificate Group	Select the desired group from the dropdown list.

Field	Description
***Certificate**	Click **Browse** to upload the certificate-key files from your computer.
Comments	Enter a description in this field. **Note:** You can enter a maximum of 2000 words in the field.

7. Click **Upload**.
8. Make sure that the uploaded Certificate-Keys file is stored in the Certificate Group.

Downloading Certificates

Downloading Server Certificates

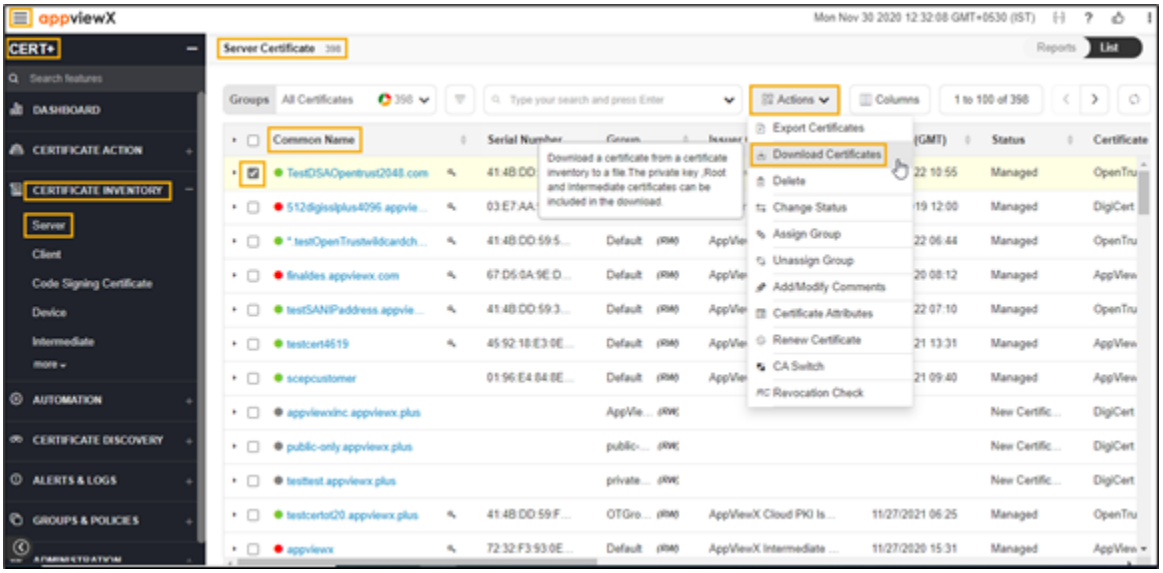
Server certificates can be downloaded from the server inventory as well as in the holistic view. In the server inventory, the user can select one or more certificates and download them in <.*crt*> format with/ without private keys and also with/without their respective trust store certificates.

To download a server certificate,

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.

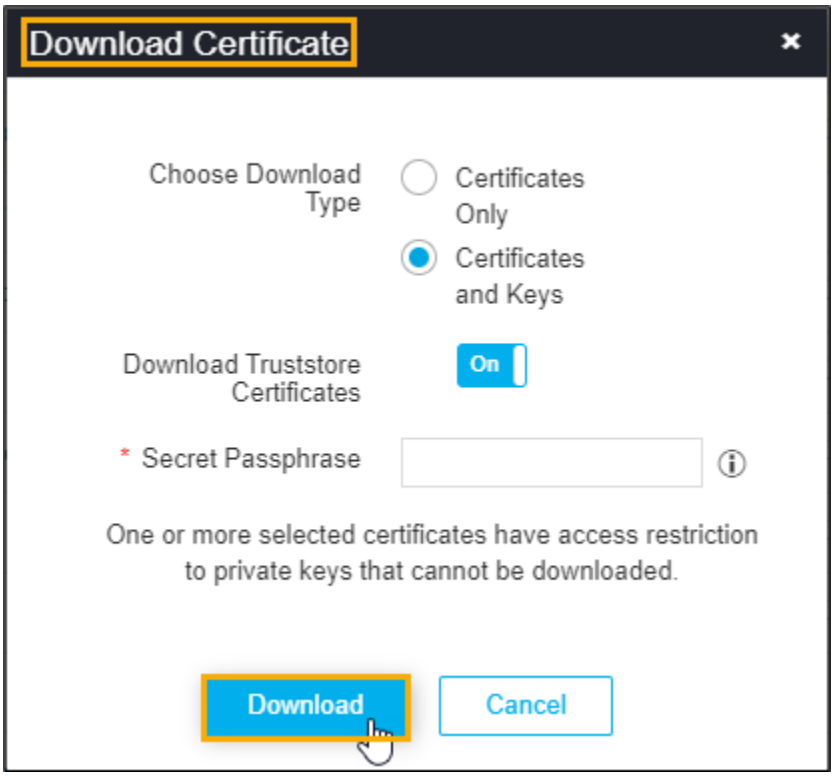
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Server**.

   The **Server Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
7. Click **Actions**, and then select **Download Certificates** from the list.

   The **Download Certificates** popup window appears.



a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.

b. You can also enable/disable **the Download Truststore Certificates** option along with the end certificates.

> **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

c. The system enables the **Secret Passphrase** field when you select **Certificates and Keys**. Enter a passphrase to encrypt the contents into a <.zip> file.

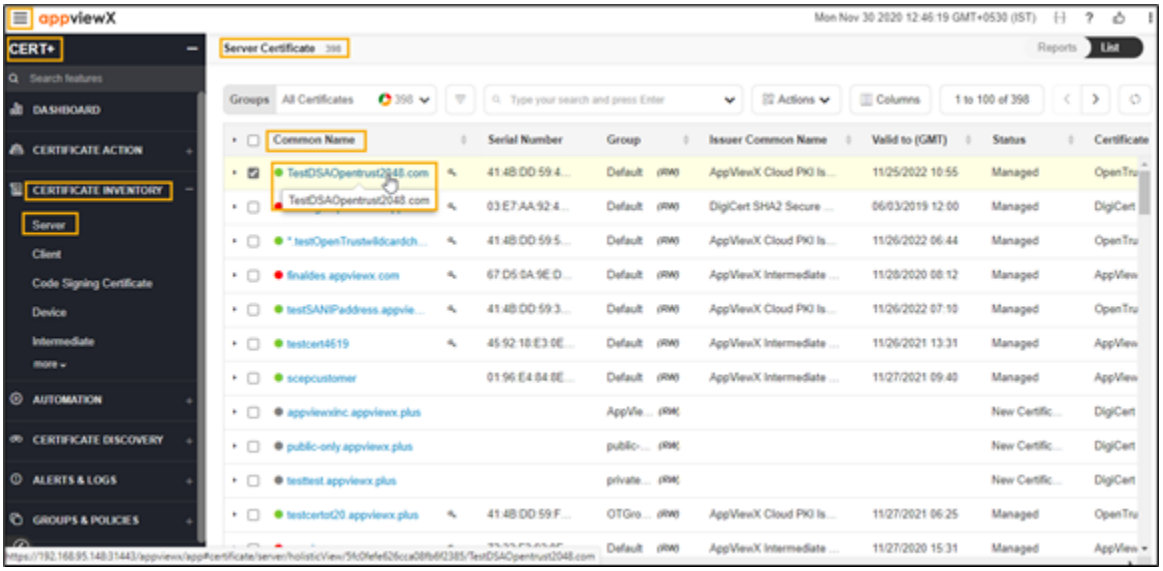
8. Click **Download**.
   The certificate is downloaded to your local machine.
9. To view details of the certificate, unzip the file and open the security certificate file.
10. Click **Details**.

Downloading Server Certificates Via Holistic View

Server certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

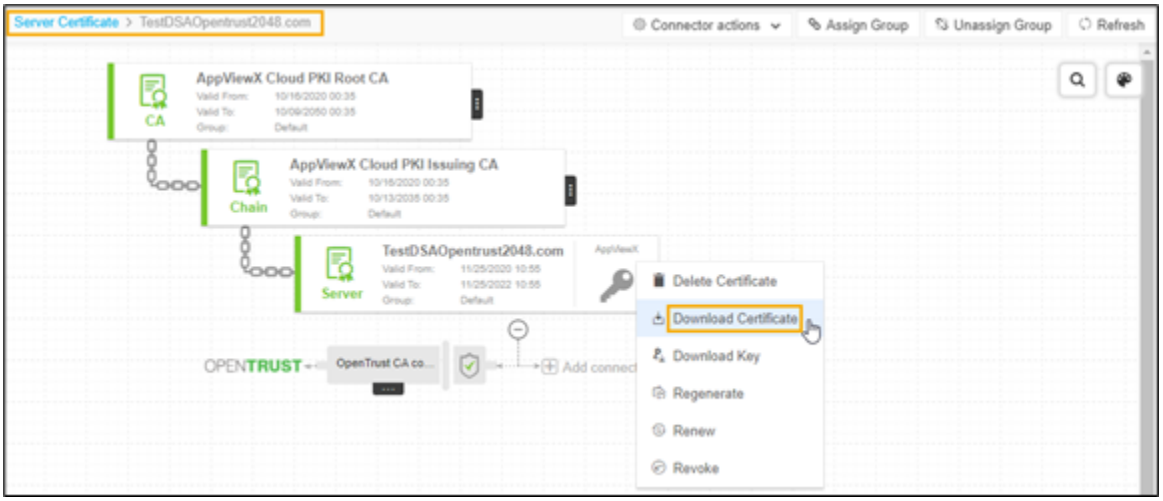
Steps to download server certificate,

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. Click **Server**.
   The **Server Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download the CA.
   The holistic view appears.

7. Click the vertical ellipse icon in the holistic view, and then select Download Certificate from the list. The Download Certificate pop-up window appears.



a. Select the file format from the Certificate type dropdown list.

b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.

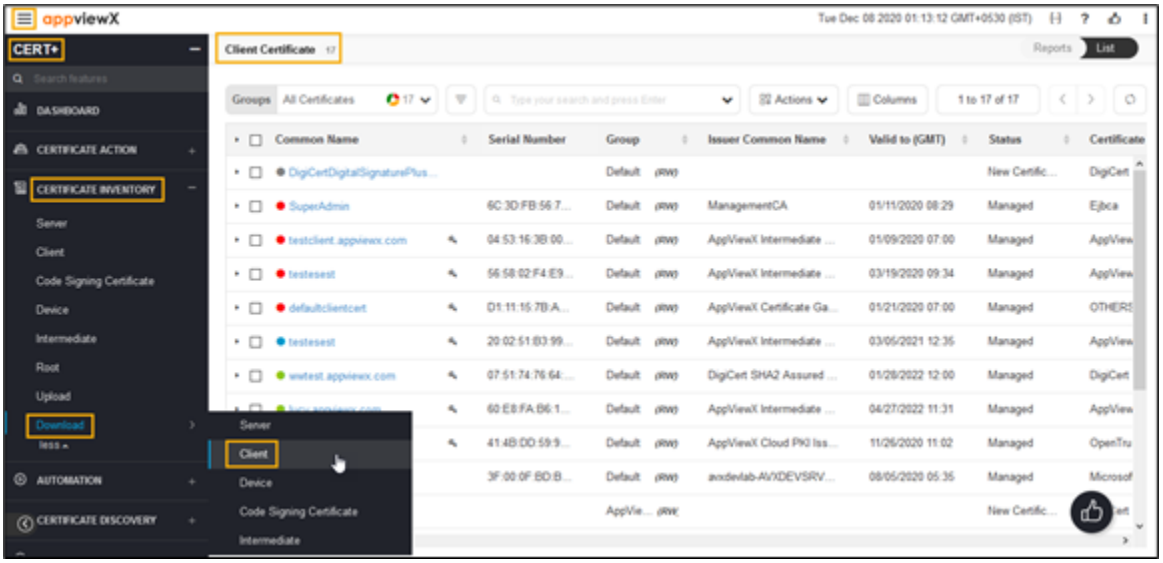
8. Click **Yes**.
   The certificate(s) is downloaded to your local machine.

Downloading Client Certificates Via Holistic View

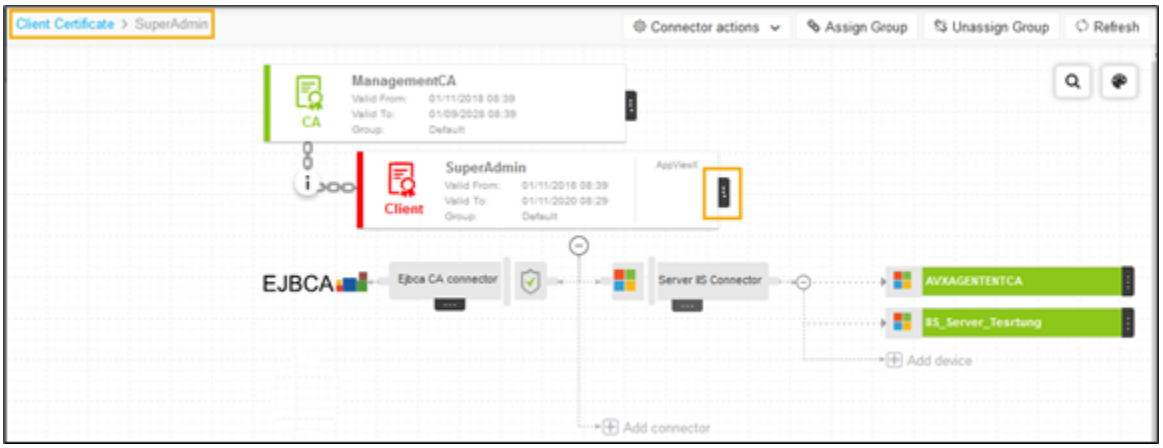
Client certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

Steps to download client certificate,

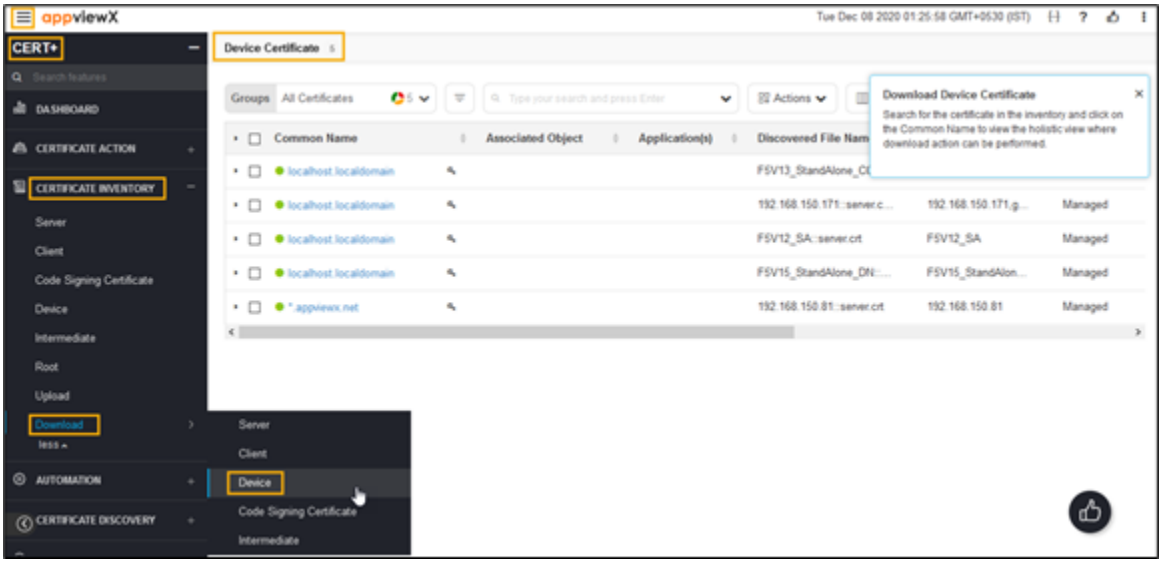
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Client**.
   The **Client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



6. In the Common Name column certificate list, select the desired certificate(s) that you want to download the CA.
   The holistic view appears.



7. Click vertical ellipse in the holistic view, and then select **Download Certificate** from the list.
   The **Download Certificate** pop-up window appears.



   a. Select the file format from the **Certificate Type** list.
   b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.
8. Click **Yes**.
   The certificate(s) is downloaded to your local machine.

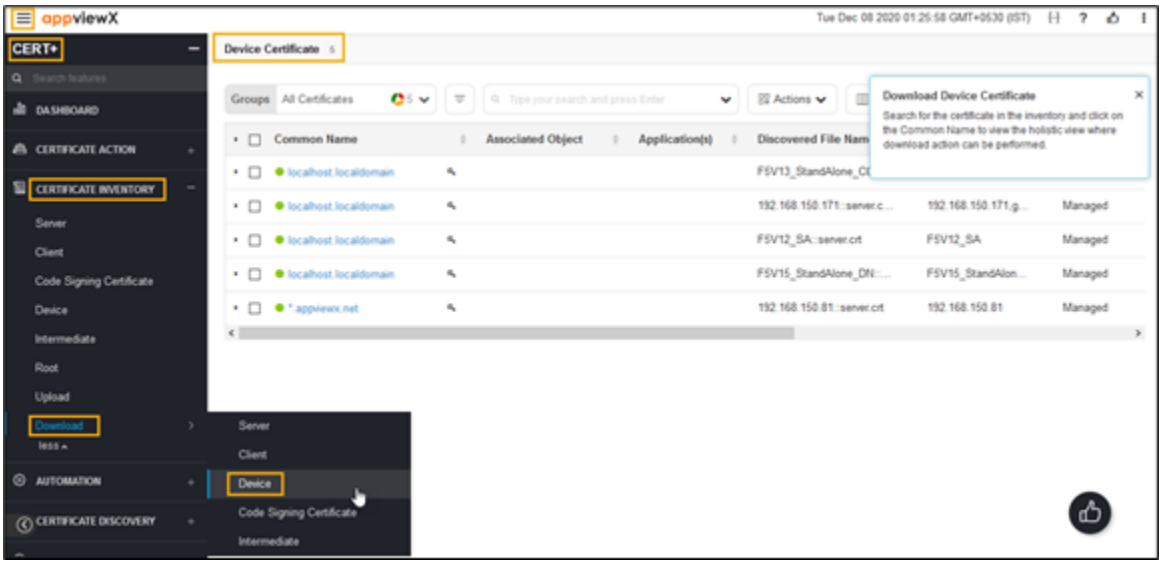
Downloading Device Certificates Via Holistic View

Device certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

Steps to download device certificate,

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. Click **Device**.

   The **Device Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
   The holistic view appears.

7. Click vertical ellipse in the holistic view, and then select **Download Certificate** from the list.
   The **Download Certificate** pop-up window appears.

8. Select the file format from the **Certificate type** list.
9. Click **Yes**.
   The certificate(s) is downloaded to your local machine.

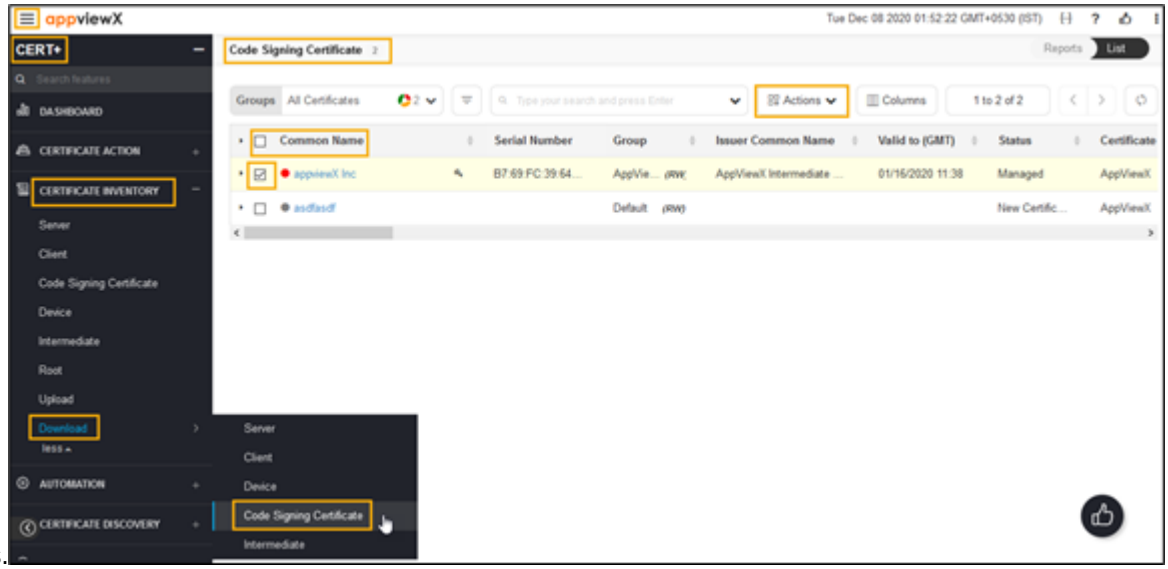
Downloading Code Signing Certificate

Code Signing certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download code signing certificate,

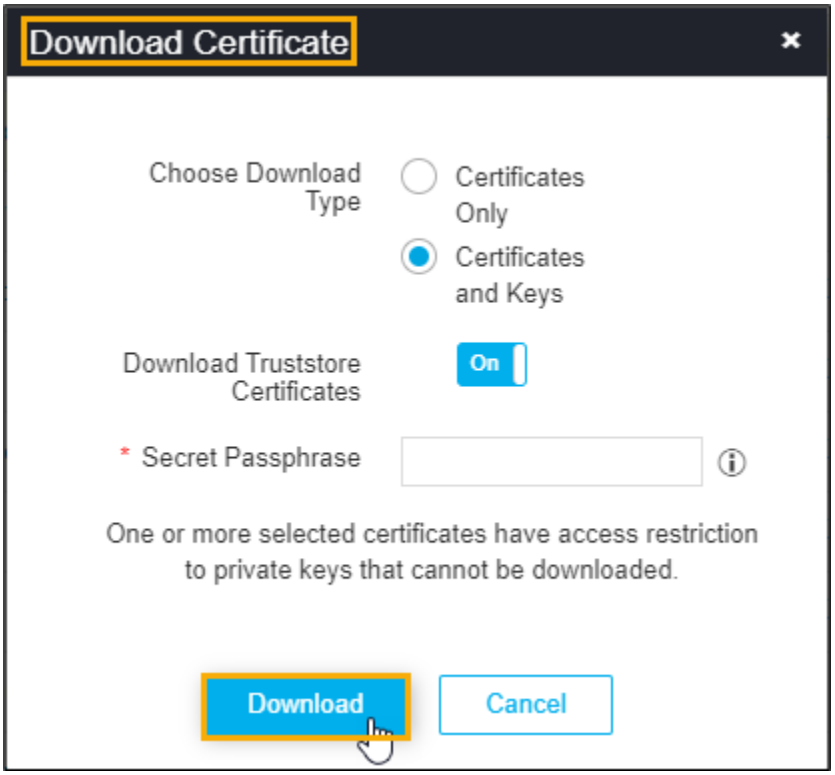
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Expand **CERTIFICATE INVENTORY**.
5. Click **Code Signing Certificate**.

The **Code Signing Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
7. Click **Actions**, and then select **Download Certificates** from the list.

   The **Download Certificates** popup window appears.



a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
b. You can also enable/disable **Download Truststore Certificates** option along with the end certificates.

> **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

c. The system enables the **Secret Passphrase** field when you select the **Certificates and Keys** option. Enter a passphrase to encrypt the contents into a `<.ZIP>` file.

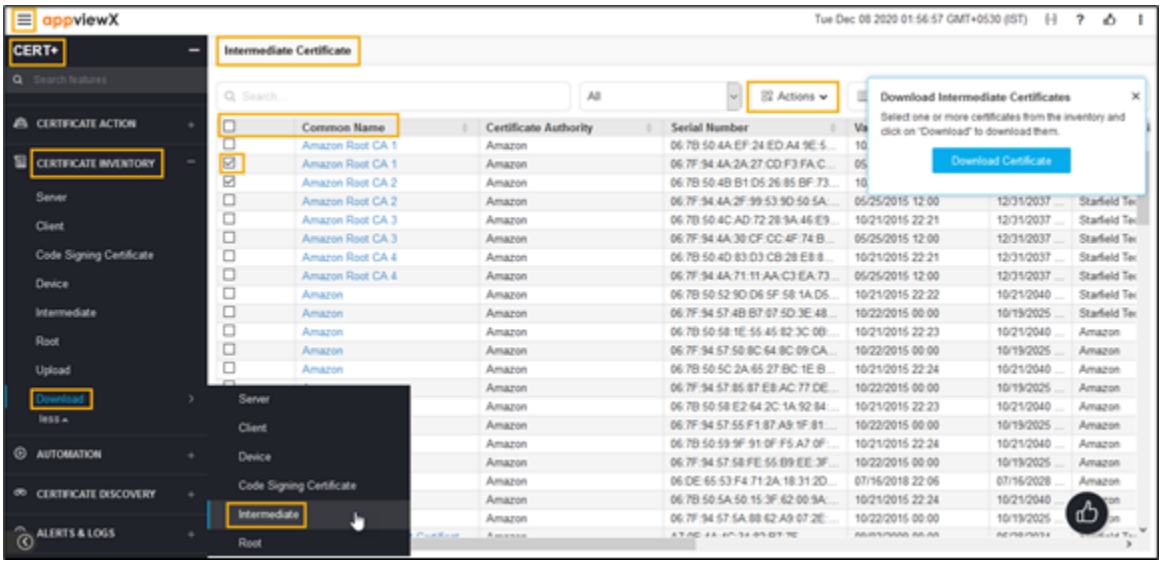
8. Click **Download**.
9. To view details of the certificate, unzip the file and open the security certificate file.
10. Click **Details**.

Downloading Intermediate Certificate

Download intermediate certificate is the action to download intermediate certificate in PEM format with or without its trust store certificates.

To download intermediate certificate,

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. Click **Intermediate**.
   The **Intermediate Certificate** page appears.



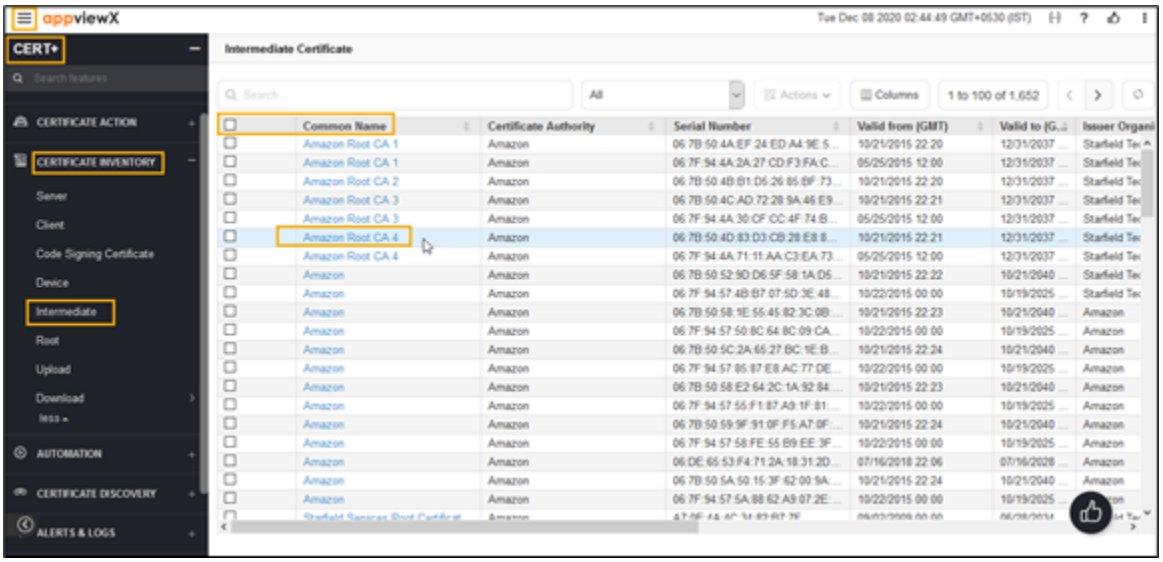
6. In the **Common Name** column certificate list, select the desired certificate that you want to download.
7. Click **Actions**, and then select **Download Certificates** from the list.
8. To view details of the certificate, unzip the file and open the security certificate file.
9. Click **Details**.

Downloading Intermediate Certificate via Holistic View

Download intermediate certificate can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download intermediate certificate via holistic view,

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. Click **Intermediate**.
   The **Intermediate Certificate** page appears.

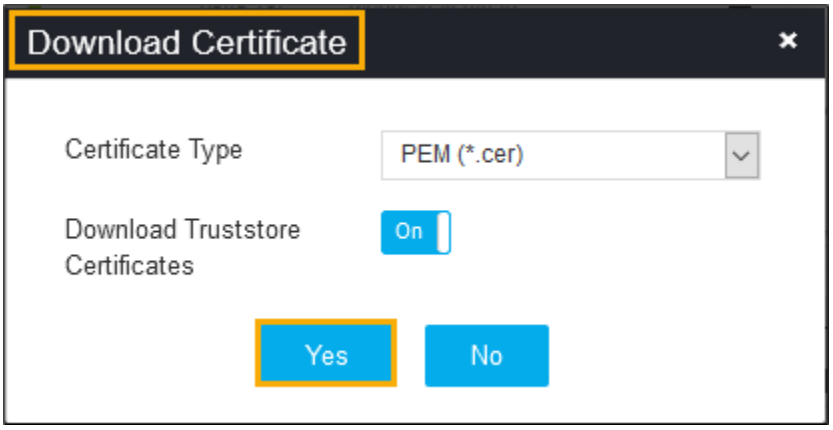


6. In the **Common Name** column certificate list, select the desired certificate that you want to download the CA.

   The holistic view appears.

7. Click vertical ellipse in the holistic view, and then select **Download Certificate** from the list.

   The **Download Certificate** pop-up window appears.



a. Select the file format from the **Certificate Type** list.
b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.

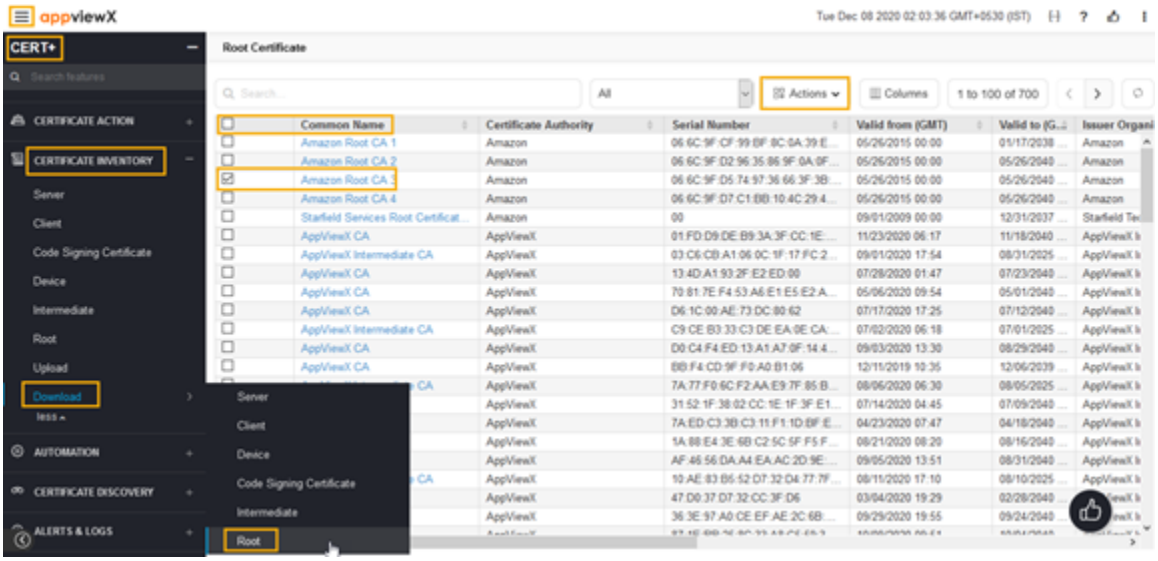
8. Click **Yes**.
   The certificate is downloaded to your local machine.

Downloading Root Certificate

Download root certificate is the action to download root certificate, the certificate get downloaded in PEM <.*crt> format from the inventory.

To download root certificate,

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. Click **Root**.
   The **Root Certificate** page appears.



6. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
7. Click **Actions**, and then select **Download Certificates** from the list.

8. To view details of the certificate, unzip the file and open the security certificate file.
9. Click **Details**.

Chapter 6: Certificate Reporting and Monitoring

Overview

Certificate Reports give you visibility over all certificates and host information in the CERT+ inventory through different modes of discovery. With the available data, you can validate whether these certificates fall under the organization's security policy. CERT+ reports give insights on all important aspects of the product.

All these reports are categorized and available as multiple dashboards as default in AppViewX. Provided with that, custom dashboards with custom reports can also be created.

Certificate Reporting and Monitoring

Once the certificates in the infrastructure are discovered in AppViewX, they can be monitored as the reports in the Dashboards. In the dashboards, the user can track the certificates expiry, compliance, security details as the reports in the dashboard.

Overview

Reporting and monitoring the certificates are essential for an administrator to get complete visibility of all the certificates across multiple vendors and data centers in one single window pane. Certificates have a finite life span and are set to expire at different dates and times. Due to advancements in cryptography, there are high chances that the infrastructure will carry the weaker algorithm certificates which will be

vulnerable to several attacks which will cause business outages. Using the dashboards and reports, the administrator can continuously monitor the status of the certificates in terms of expiry, security, compliance and so on.

Viewing Dashboard

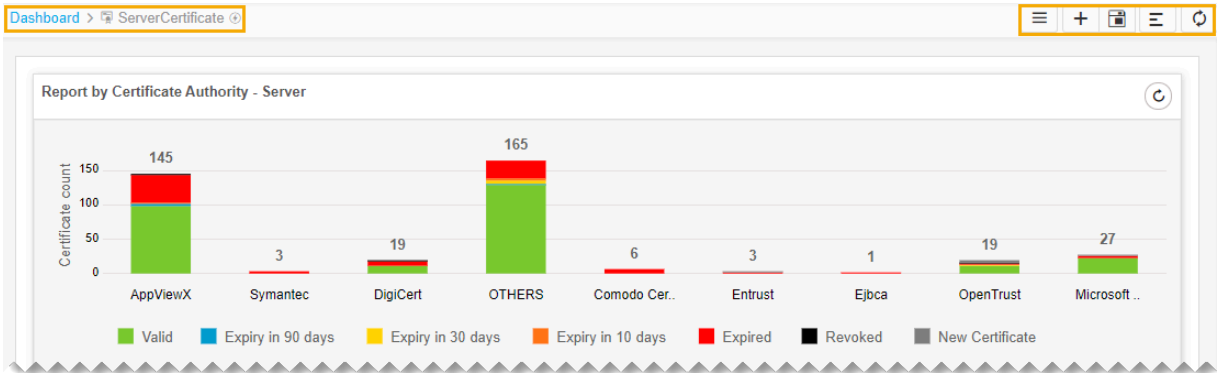
To view a dashboard,

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 **Dashboard** in the left navigation pane.

   The list of dashboards is displayed.
4. Click the desired Dashboard name.

   The dashboard page appears:



The following table describes the options available on the dashboard view page:

Options	Descriptions
Dashboard inventory 	Go to Dashboard page where all the Dashboards are listed.
Create	Create a dashboard/widget.

Options	Descriptions
	
Save widget 	Save the widget changes.
Align 	Align the widgets within the dashboard.
Refresh 	Refresh a dashboard.

5. Click the **Save Widget** button in the command bar located at the upper right of the screen.

Searching for Dashboard, Object, or Widget

To search for a dashboard,

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 **Dashboard** in the left navigation pane.
4. Enter the search keyword in the search field, and then click the **Search** icon.

   The dashboards, objects, or widgets that match with the keyword are displayed.

Creating Dashboard

To create a dashboard,

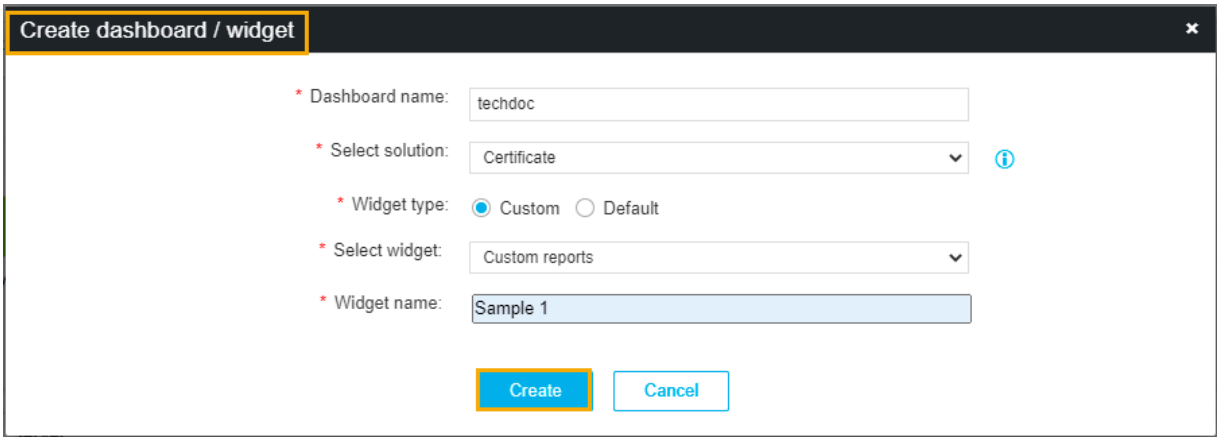
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.

3. Click **Dashboard** in the left navigation pane.
4. Click the **add** button in the command bar.

   The **Create dashboard/widget** pop-up window appears.

5. Enter or select the field information in the **Create dashboard/widget** pop-up window.



The following table provides the field description to create a Dashboard:

Field	Description
***Dashboard name**	Name of the Dashboard.
***Select solution**	ADC is the select solution.
***Widget type**	Type of the Widget. The possible Widget types are: • **Custom** - choose this option to create a customized Widget. By default, this option is selected. • **Default**- choose this option to select the default Widget.

Field	Description
	
***Select widget**	Customized widgets appear in the drop-down menu. Select the appropriate widget.
***Widget name**	Name of the Widget.

Note: The asterisk (*) symbol indicates mandatory fields.

6. To create a Dashboard/Widget, click **Create**.

Note: To discard the changes, click **Cancel**.

Exporting Dashboard Information

You can export the dashboards in <.csv> or <.json> format. The dashboards that are exported in the <.json> format can be imported to another build of the AppViewX platform.

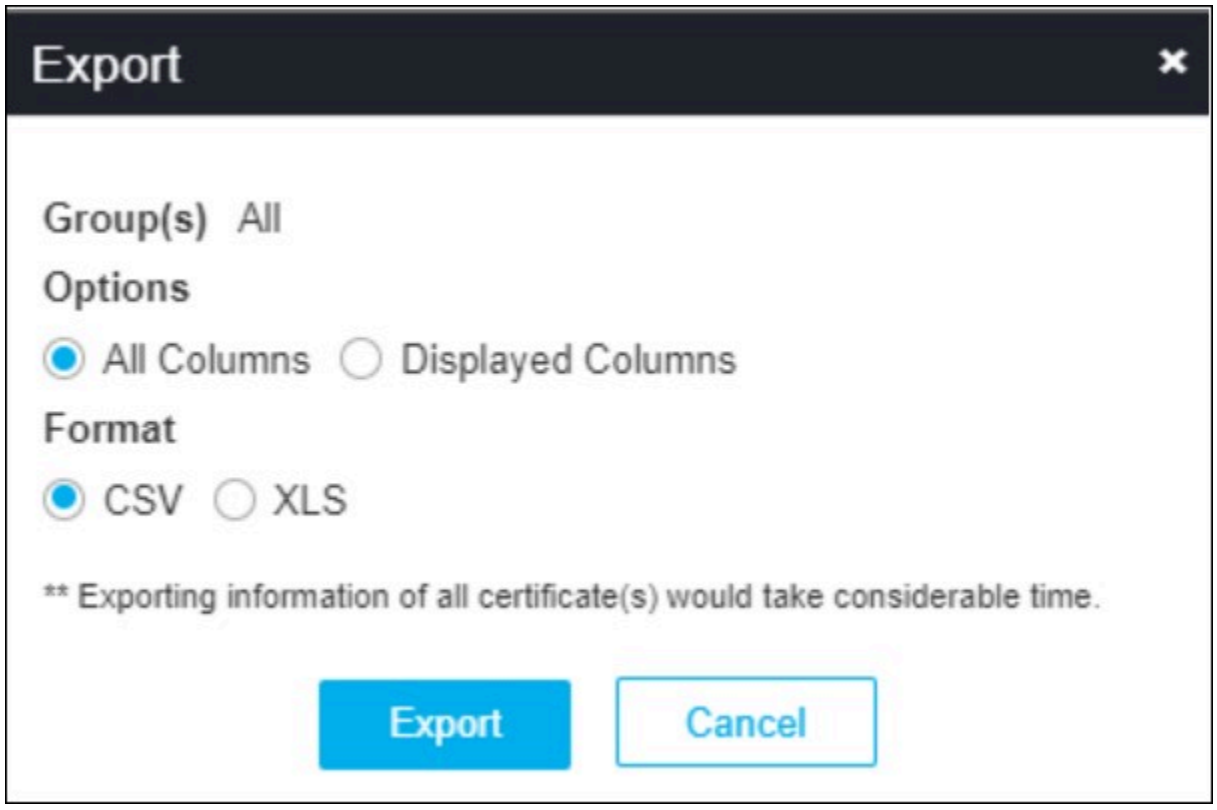
To export dashboard information,

1. 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 **Dashboard** in the left navigation pane.

   The list of dashboards is displayed.
4. Select the desired dashboards from the list.
5. Click the export button in the command bar located at the upper right of the screen.

   The **Export** pop-up window appears:



6. Select the desired **Options** and **Format** in the **Export** popup window.

   The selected dashboards are exported to your local machine.

Importing Dashboard

You can import the list of dashboards, which has the **Application View** widget. The import file must be in the <.text> and/or <.json> format and zipped.

To import a dashboard:

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

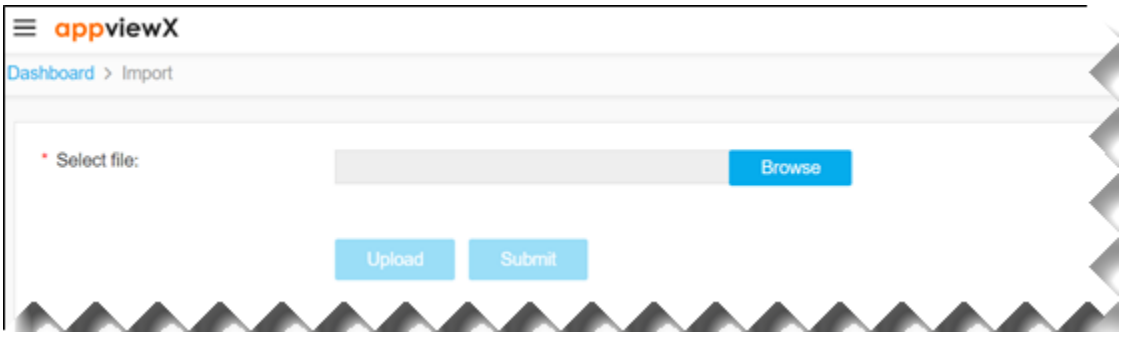
   The left navigation pane appears.

3. Click **Dashboard** in the left navigation pane.

   The list of dashboards is displayed.

4. Click the Import button in the command bar located at the upper right of the screen.

The **Import** page appears:



5. Browse and open the dashboard import file in <.zip> format.
6. Click the **Upload** button.
7. Once the file is uploaded, click the **Submit** button.

   The list of dashboards is imported to AppViewX platform.

Deleting Dashboard

The default dashboard cannot be deleted from the AppViewX platform. Only the customized dashboard can be deleted and deleting the dashboard includes the deletion of all the widgets on the dashboard also.

To delete a dashboard,

1. 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 **Dashboard** in the left navigation pane.

   The list of dashboards is displayed.

4. Select the desired Dashboard to be deleted.
5. Click the **delete** button in the command bar located at the upper right of the screen

   The delete pop-up window appears.

6. Click the **Delete** button to delete the desired dashboard.

Overview

Certificate Reports give you visibility over all certificates and host information in the CERT+ inventory through different modes of discovery. With the available data, you can validate whether these certificates fall under the organization's security policy. CERT+ reports give insights on all important aspects of the product.

All these reports are categorized and available as multiple dashboards as default in AppViewX. Provided with that, custom dashboards with custom reports can also be created.

Certificate Reporting

View Certificate Reports

To view certificate reports:

1. Click **Certificate Inventory** and click the type of certificate for which you want to view the report.
2. The **Reports** page is selected.

Although each certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Client Certificate** screen:

- **Report by Certificate Authority -** A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month -** A bar chart that shows the total number of certificates expiring each month.
- **Policy Compliance -** A pie chart that shows the number of compliant and non-compliant certificates in the system, with each sector in the chart representing a different kind of policy such as Strict or Suggestive. You can also export the report details from the Policy Compliance Report widget.
- **Stale Certificate -** A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary -** A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the

Report by Certificate Authority widget. You can also configure the report settings from the Certificate Summary Report widget.

- **Count by Issuer -** A doughnut chart that shows the total number of certificates managed by the issuer such as Root CA or the Intermediate CA. You can also configure the report settings from the Count by Issuer widget.

Default Reports

AppViewX CERT+ has a few in-built reports (recommended) that are available as default reports. These reports can be triggered directly to take necessary actions. The primary risk to be addressed is to enforce security compliance. Compliance reports that are provided as in-built reports can be used to categorize certificates based on the non-compliant parameter. This information (value addition) can be used to enforce the application team to onboard for automation.

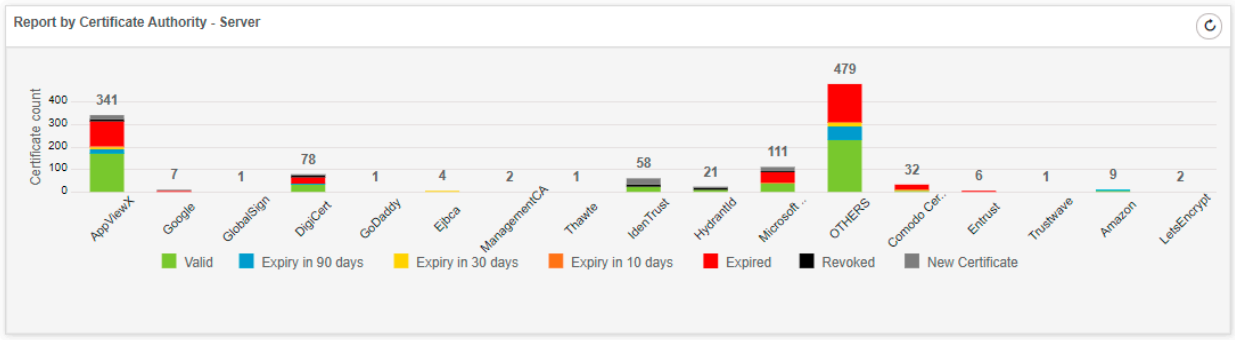
Server Certificate Dashboard

Server Certificate Dashboard

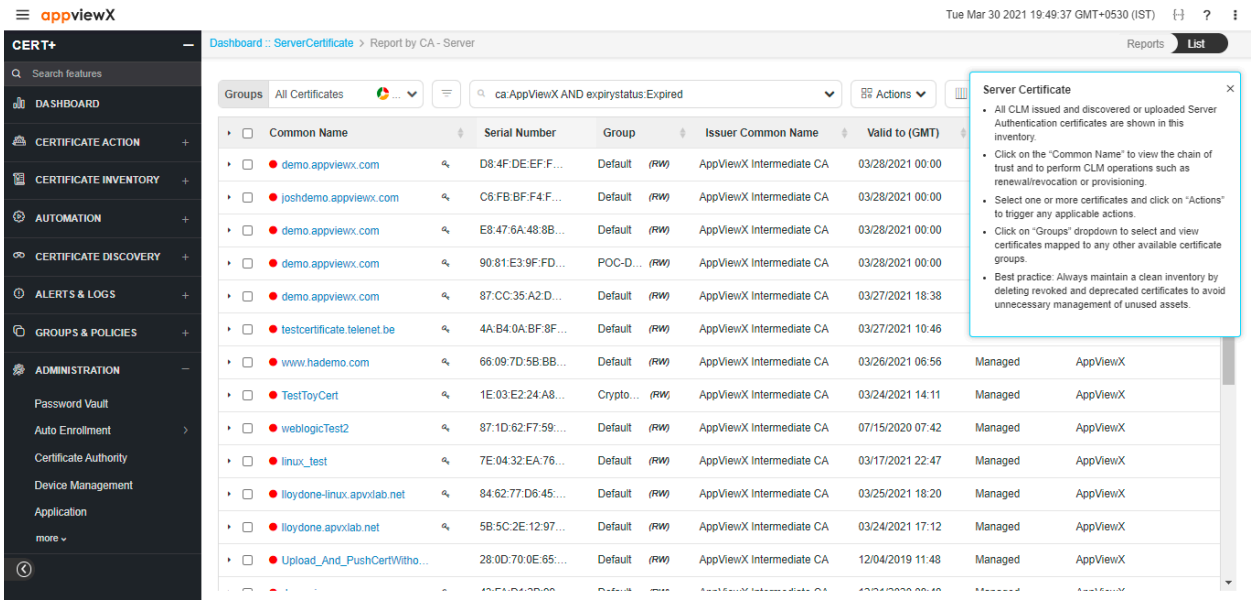
The certificates from the Server inventory will be shown in this dashboard as the following reports:

Report by Certificate Authority - Server

This report shows the count of certificates in the server inventory with respect to the certificate authorities and the expiry information.

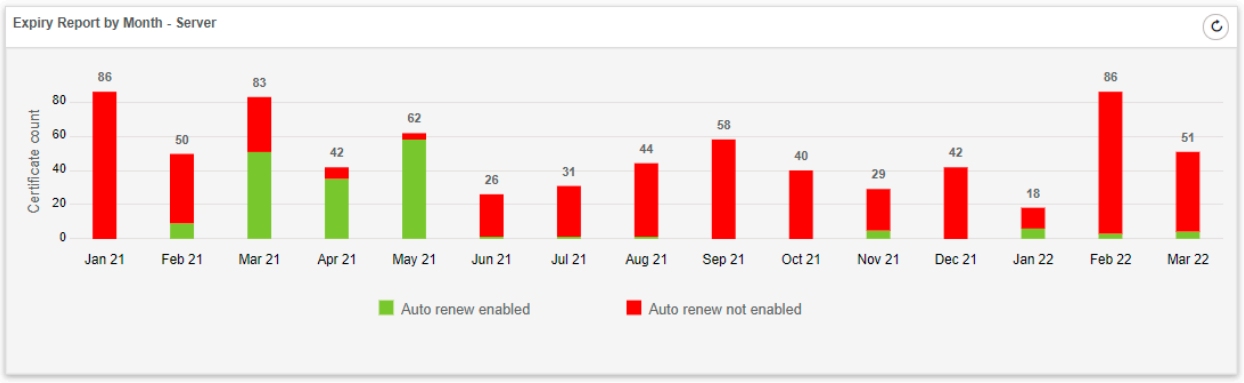


On click of any of the bar of this report, the filtered inventory view will be shown as below to proceed any further actions:

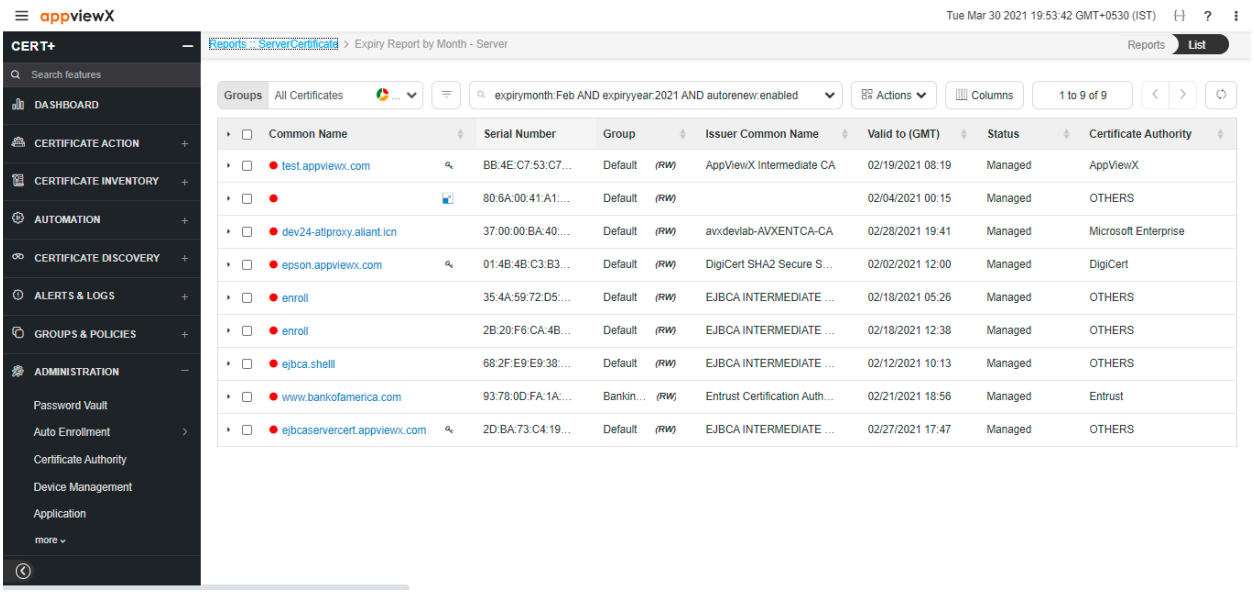


Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



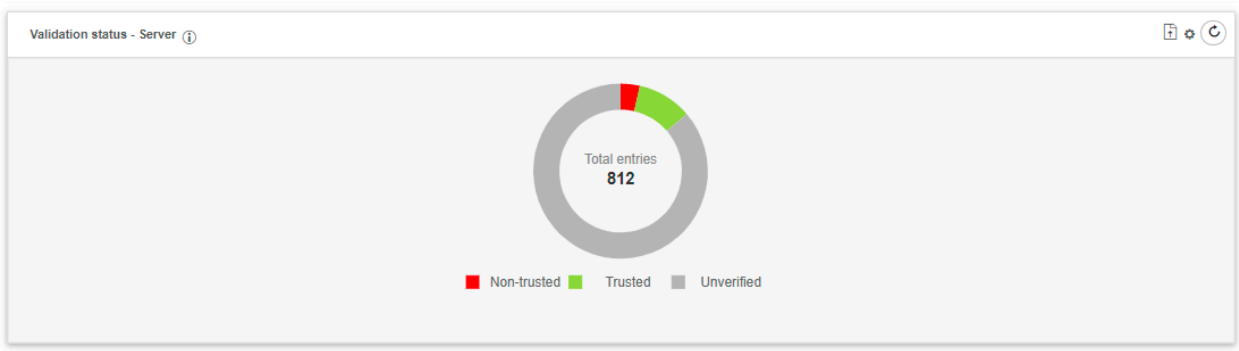
On click of any of the bar, the filtered certificates inventory will be shown as below to perform any inventory actions:



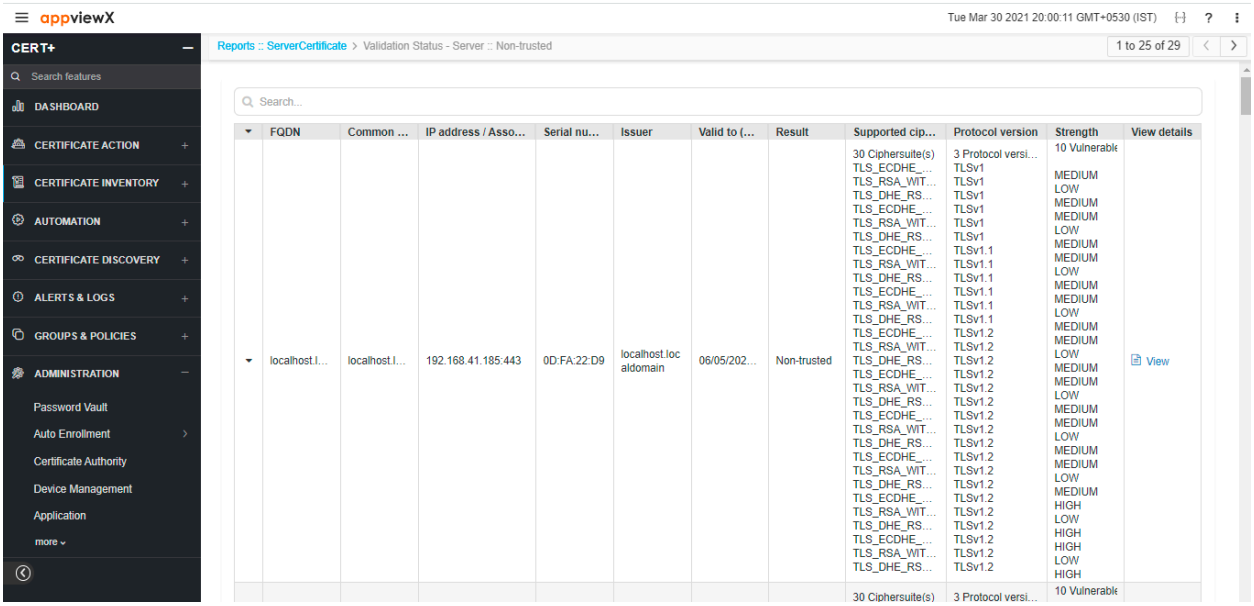
Validation Status

This report shows the count of server certificates with respect to the following:

- Trusted – When the chain of trust can be formed with the end server certificate it will be categorized as a trusted certificate.
- Non-trusted – When the chain of trust cannot be formed with the end server certificate it will be categorized as non-trusted.
- Unverified – When the server certificates are yet to be taken for validation, they will be categorized as unverified.

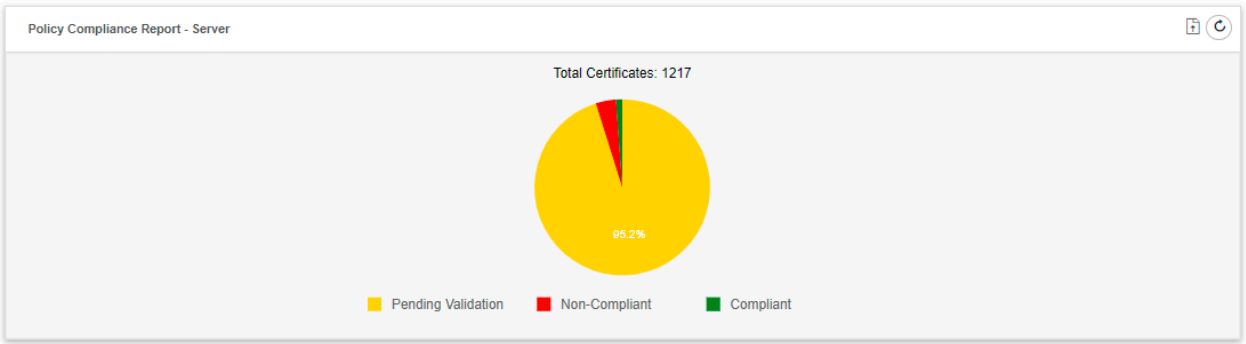


On click of anywhere in this pie chart, the filtered certificates data will be shown as below:

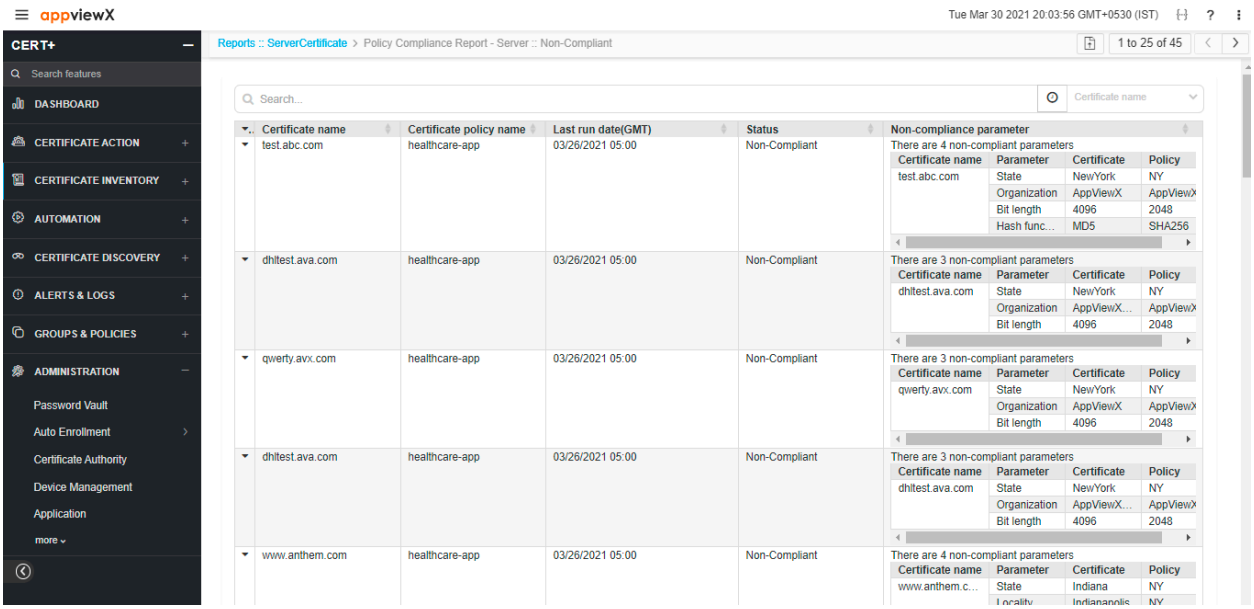


Policy compliance status

This report shows the count of server certificates as compliance or non-compliance based on the certificate group policy associated with the certificates.

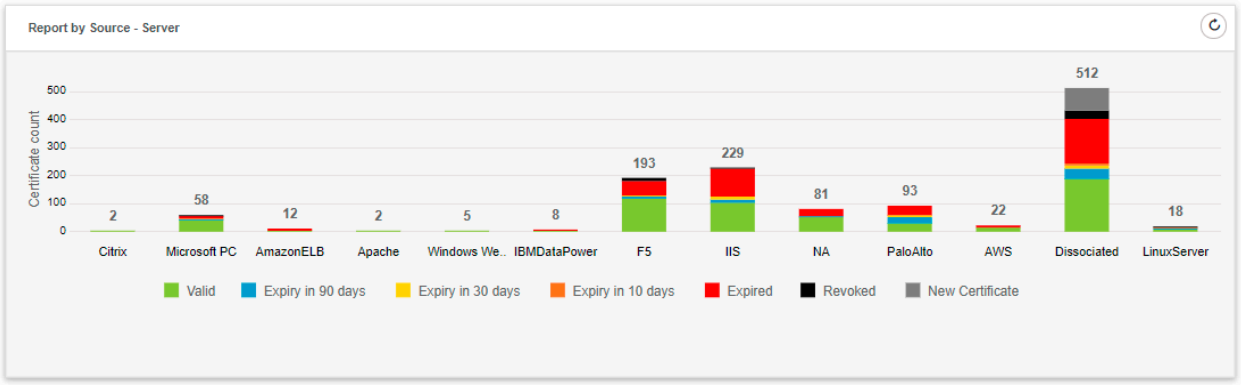


On click of anywhere in the pie chart, the filtered certificates data will be shown as below:

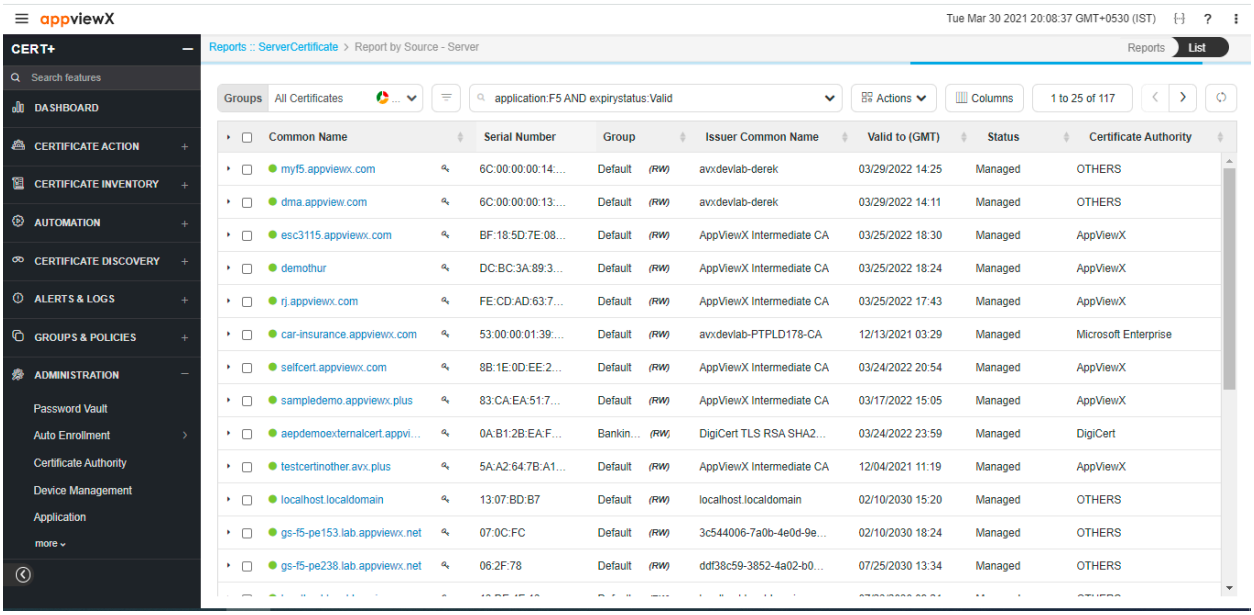


Report by source

This report shows the count of server certificates with respect to the source from where the certificates are discovered along with the expiry status.

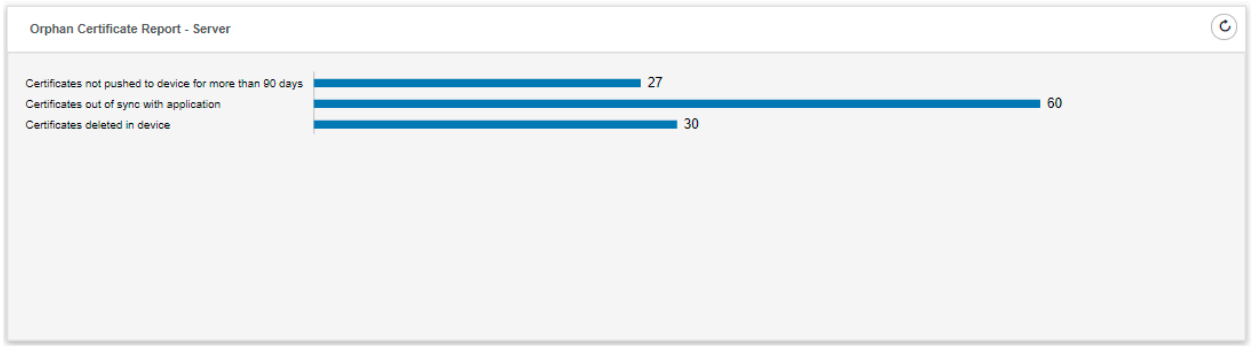


On click of anywhere in the bar chart, the filtered certificates data will be shown as below:



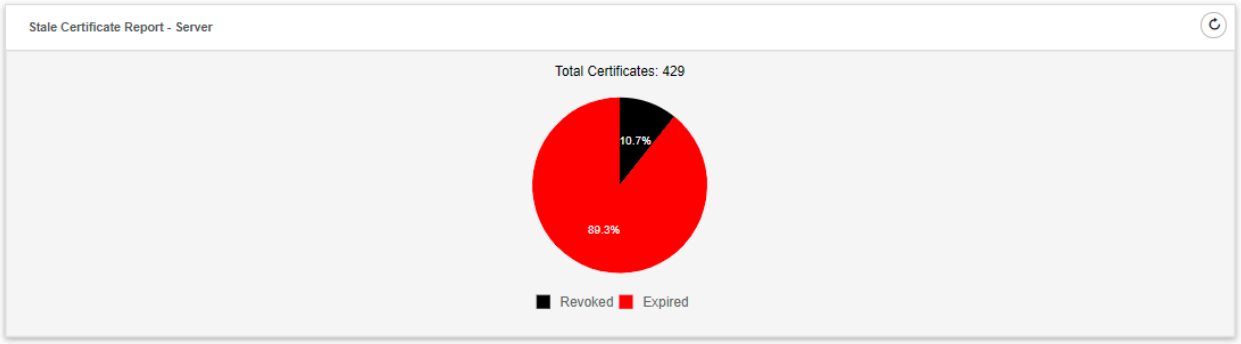
Orphan Certificate Report

This report shows the count of server certificates that are not associated/installed in any device/server.



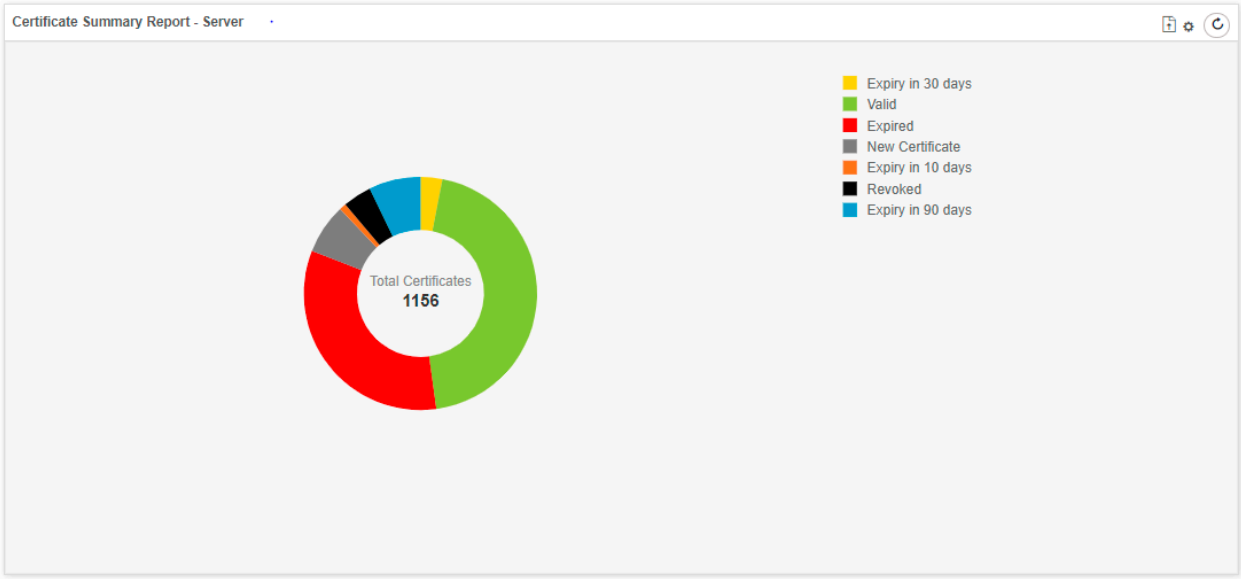
Stale Certificate Report

This report shows the count of server certificates that are either revoked or expired.



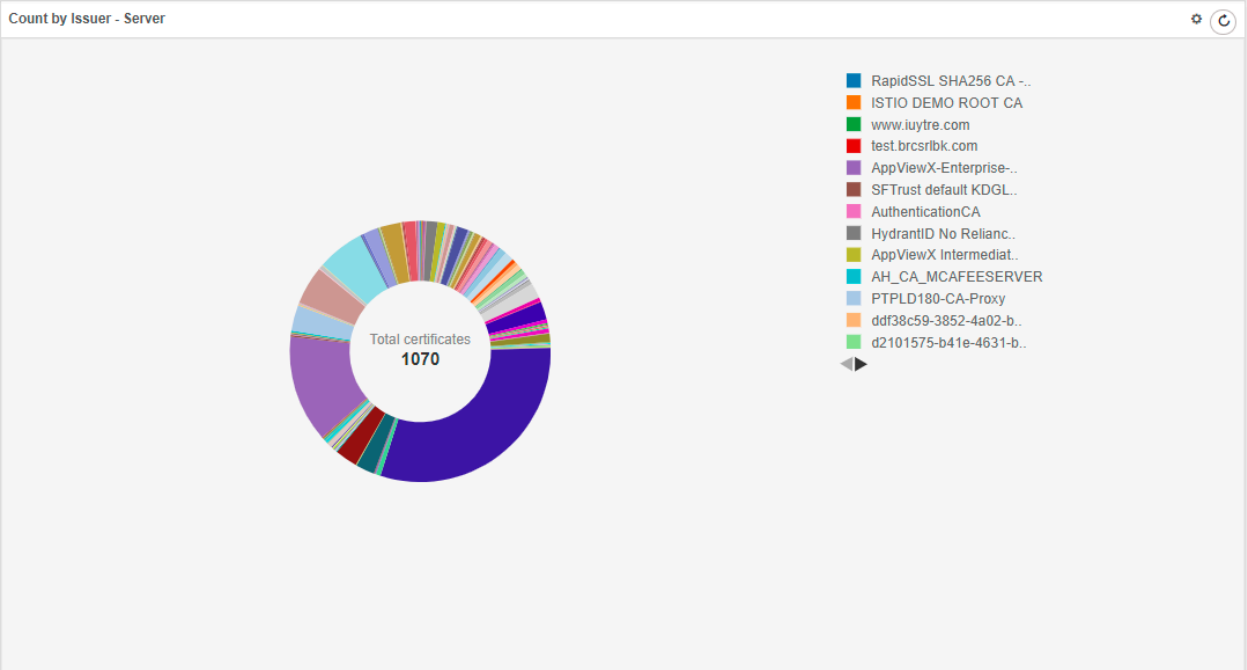
Certificate Summary Report

This report shows the count of certificates with respect to their expiry status.



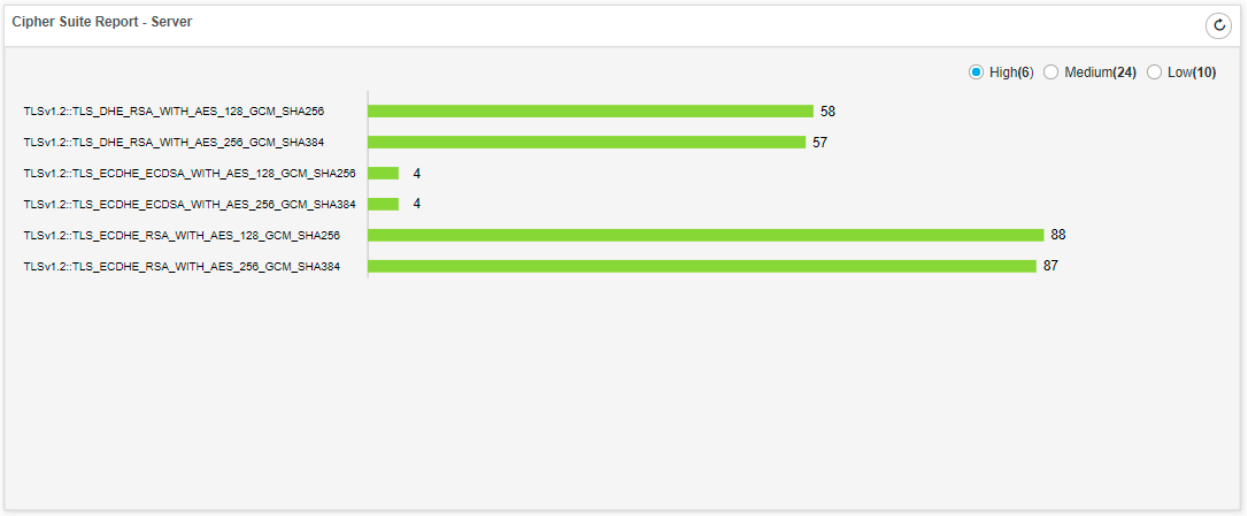
Count by Issuer

This report shows the count of certificates with respect to the issuer details.



Cipher Suite Report

This report shows the count of certificates with respect to the cipher suites. They are also categorized as Low, Medium, and High based on the cipher suites.



Client Certificate Dashboard

- Client Certificate Dashboard
- Report by Certificate Authority

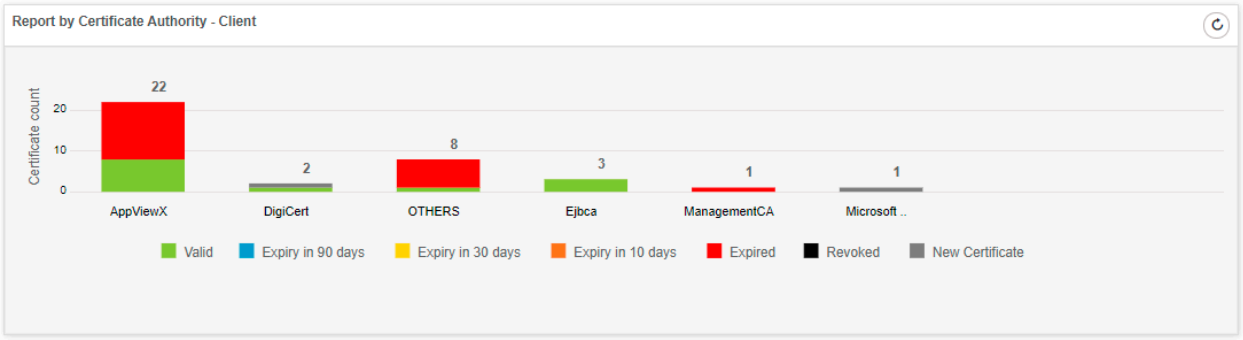
- Expiry Report by Month
- Policy compliance status
- Stale certificate report
- Certificate Summary Report
- Count of issuer

Client Certificate Dashboard

The certificates in the Client inventory will be shown in this dashboard as the following reports:

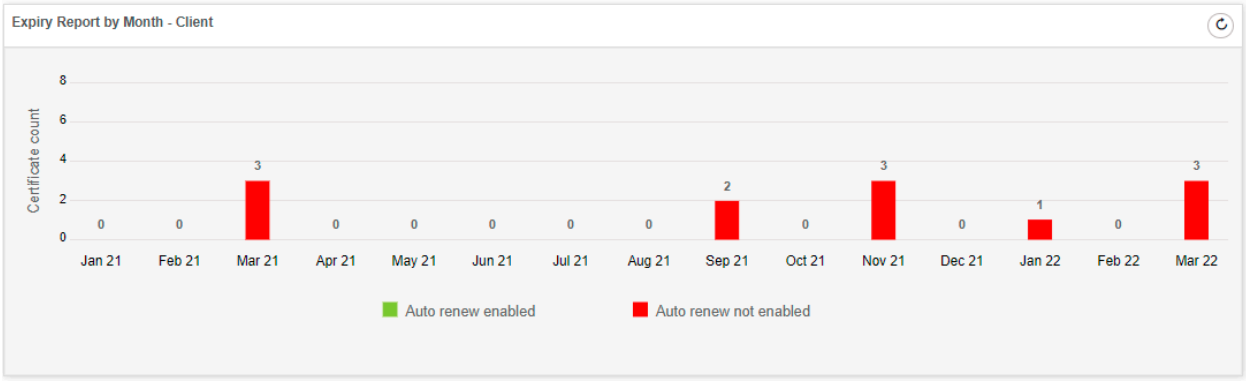
Report by Certificate Authority

This report shows the count of certificates in the client inventory with respect to the certificate authorities and the expiry information.



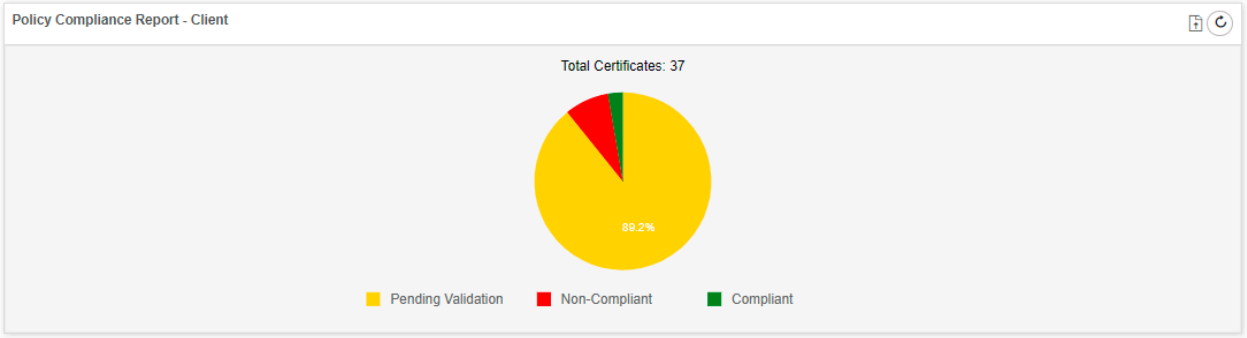
Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



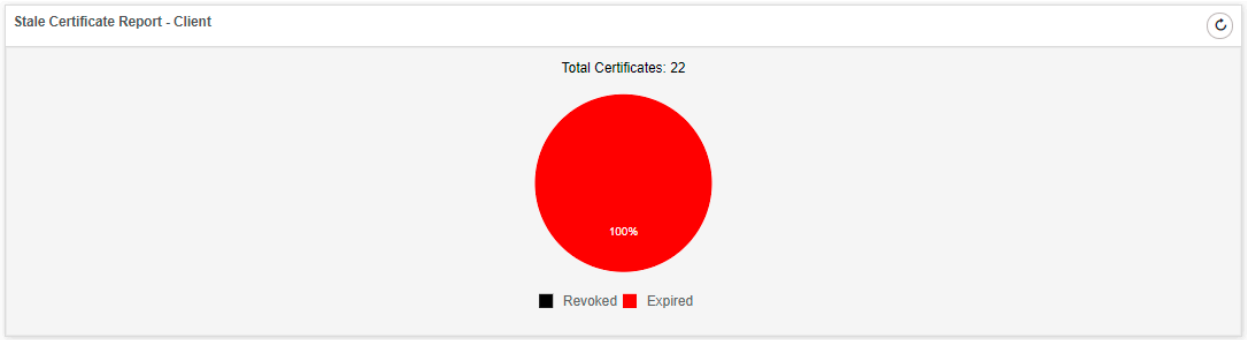
Policy compliance status

This report shows the count of client certificates as compliance or non-compliance based on the group policy assigned to the certificate.



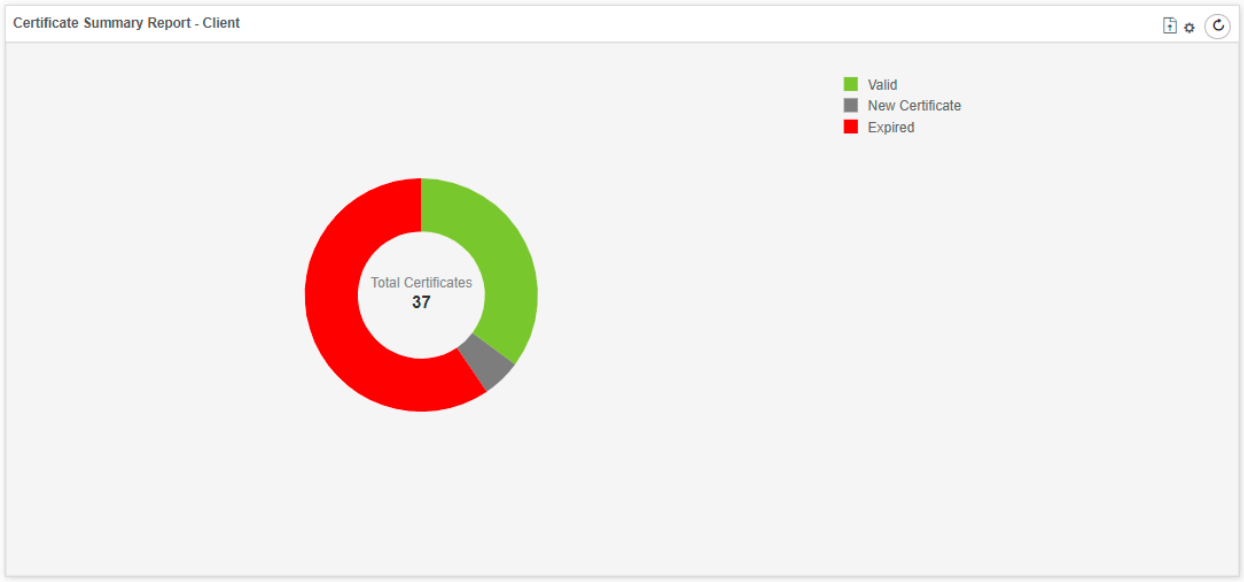
Stale certificate report

This report shows the count of client certificates that are either revoked or expired.



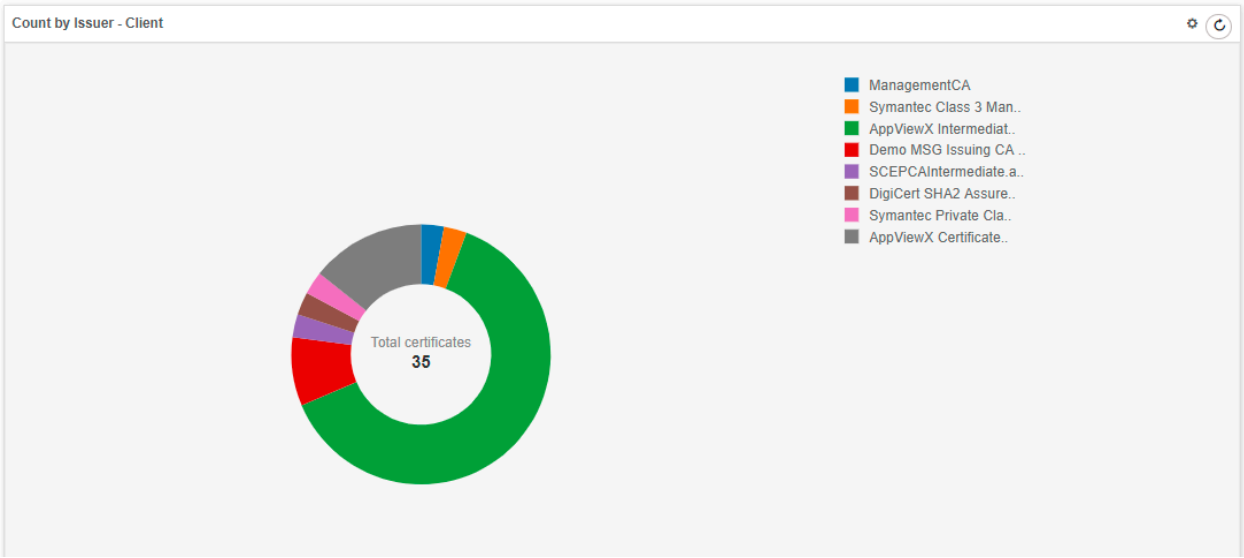
Certificate Summary Report

This report shows the count of certificates with respect to their expiry status.



Count of issuer

This report shows the count of client certificates with respect to the issuer details.



Code Signing Dashboard

- Code Signing Dashboard
- Report by Certificate Authority
- Expiry Report by Month

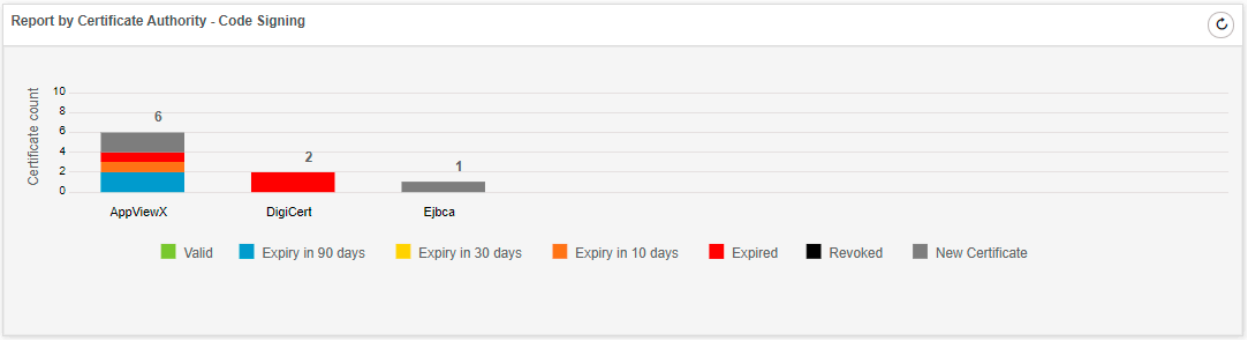
- Stale Certificate Report
- Count of issuer

Code Signing Dashboard

The certificates in the code signing inventory will be shown in this dashboard as the following reports:

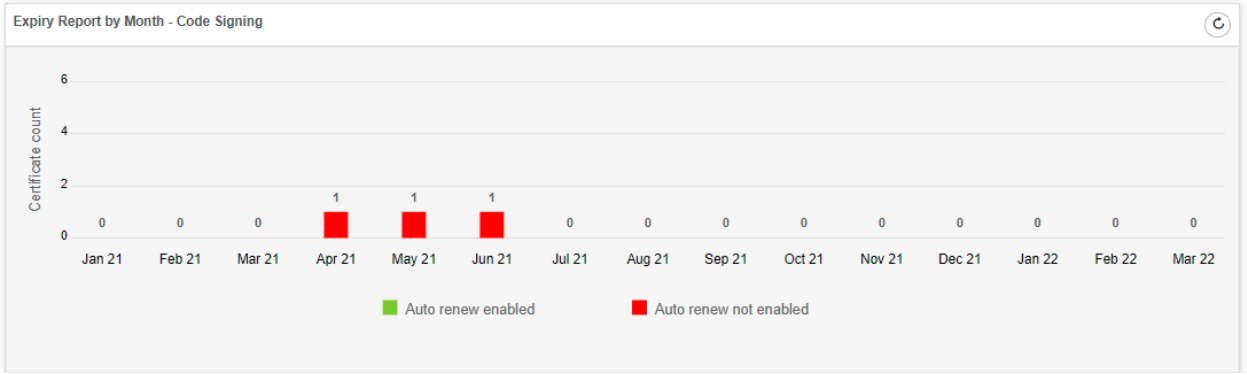
Report by Certificate Authority

This report shows the count of certificates in the code signing inventory with respect to the certificate authorities and the expiry information.



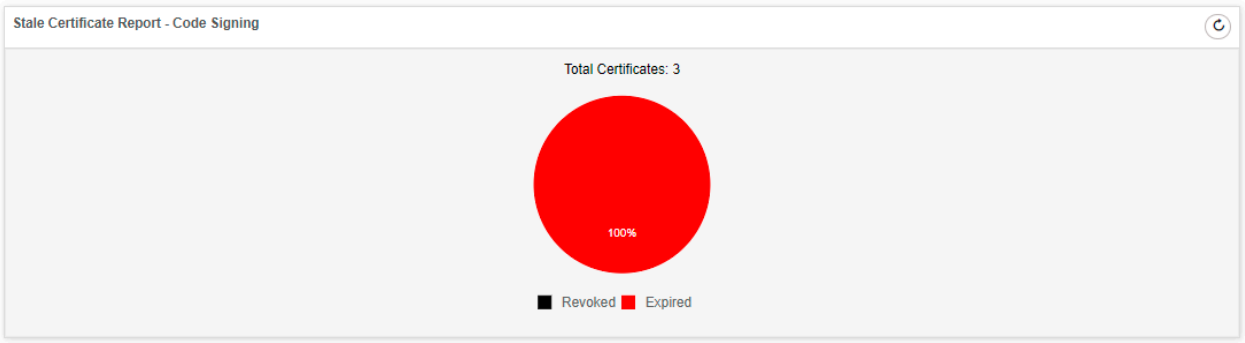
Expiry Report by Month

This report shows the count of code signing certificates with respect to expiry month information.



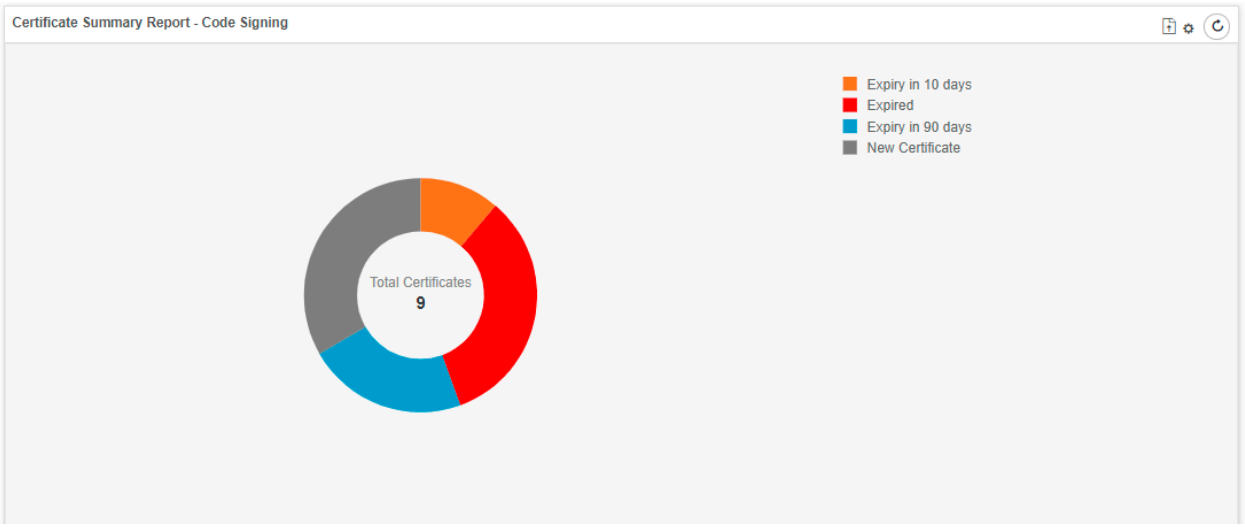
Stale Certificate Report

This report shows the count of code signing certificates that are either revoked or expired.



Count of issuer

This report shows the count of client certificates with respect to the issuer details.



Server Certificate Security Dashboard

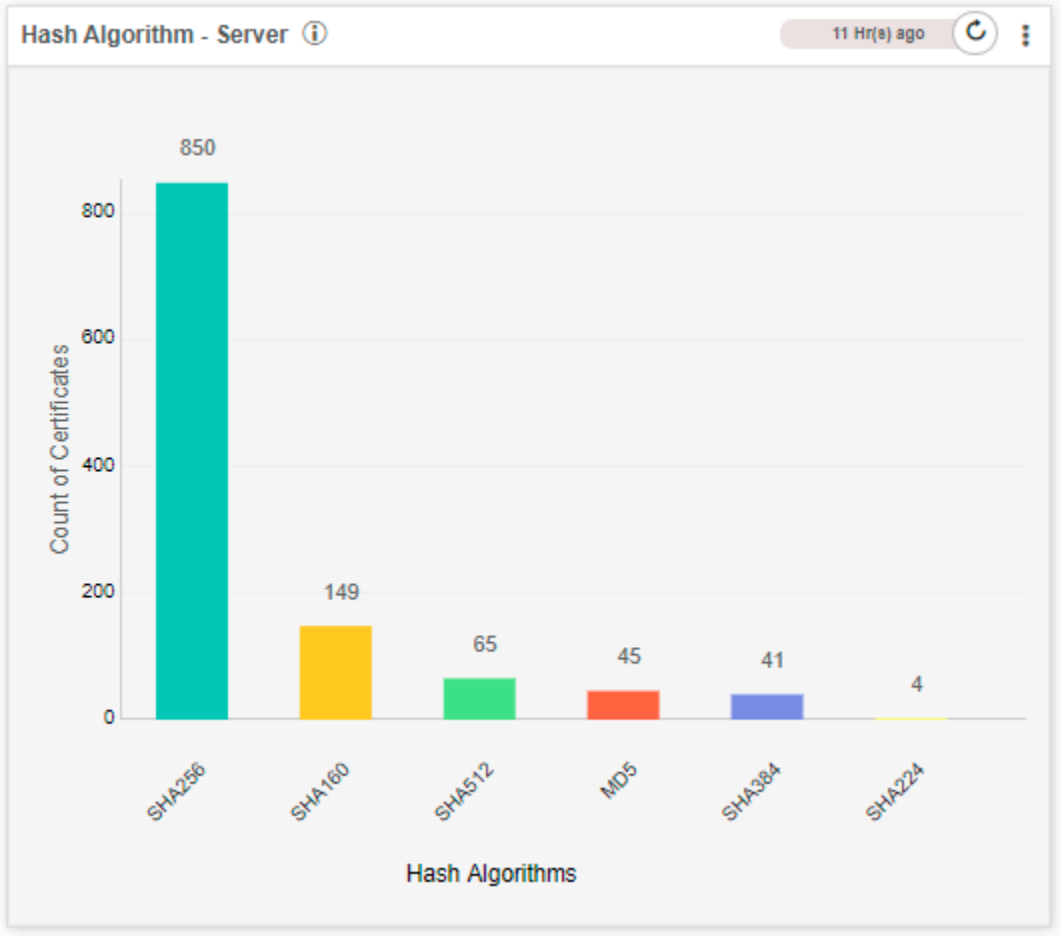
- Server Certificate Security Dashboard
- Hash Algorithm - Server
- Key Algorithm - Server
- CAA Record – Server
- Certificate transparency – Server

Server Certificate Security Dashboard

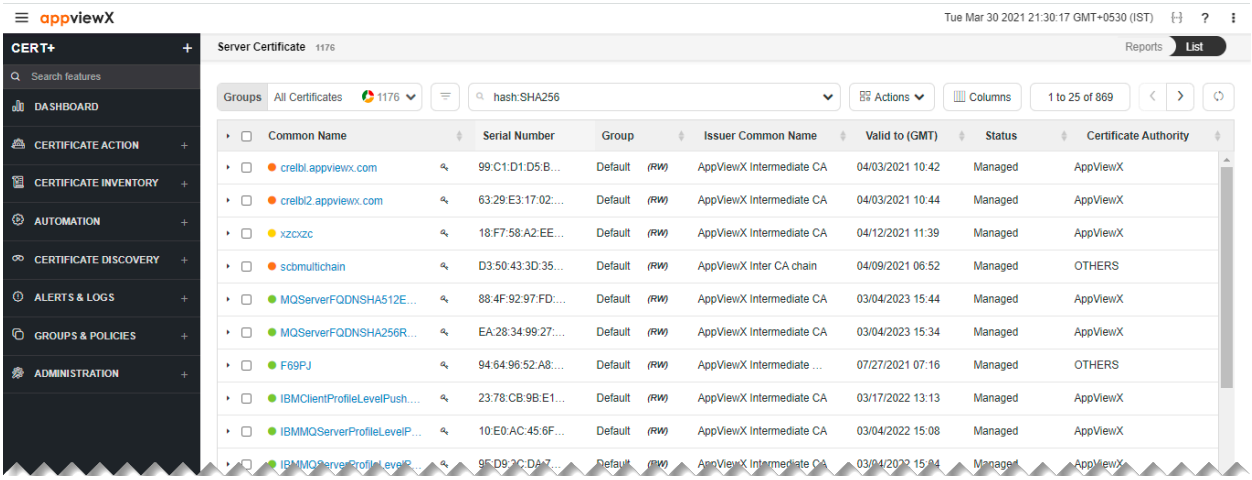
For the certificates in the Server inventory, this dashboard will show the reports as below:

Hash Algorithm - Server

This report shows the count of certificates with respect to the hash algorithm available in the server inventory.

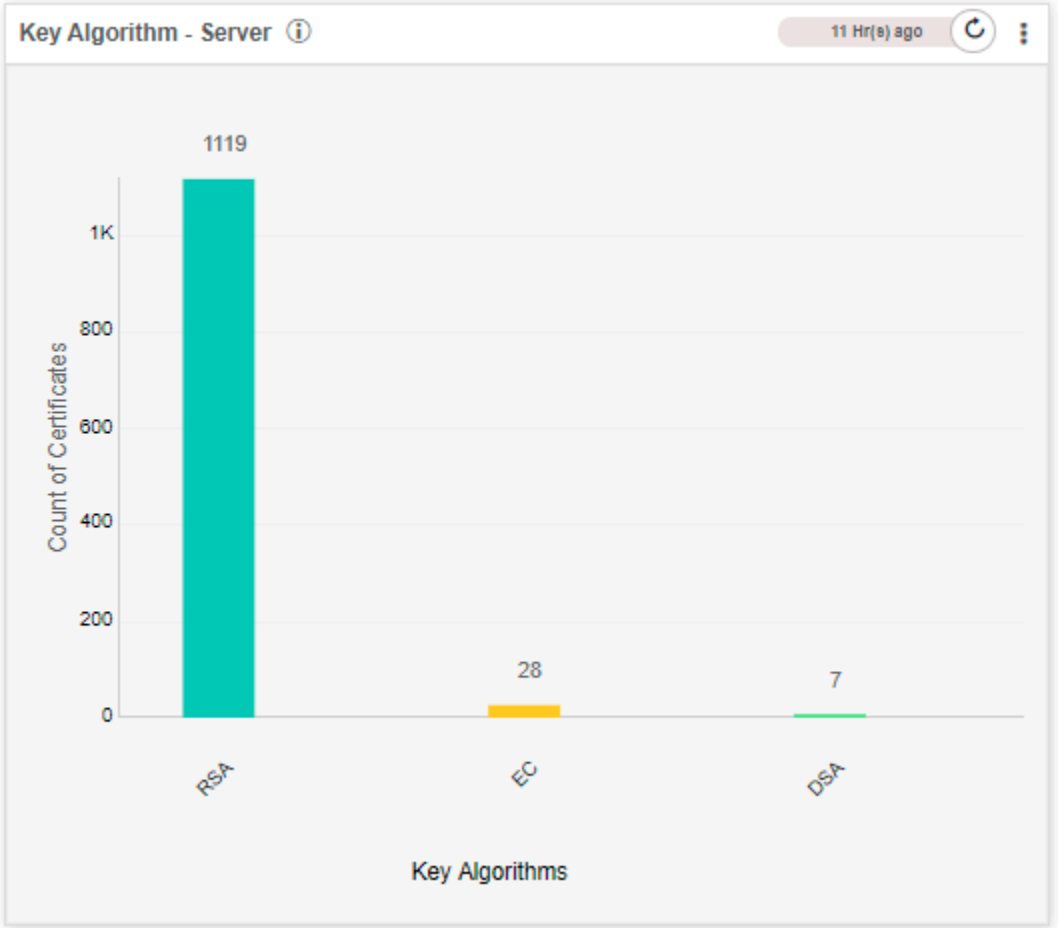


On click of the report, the filtered data of certificates will be shown as below:

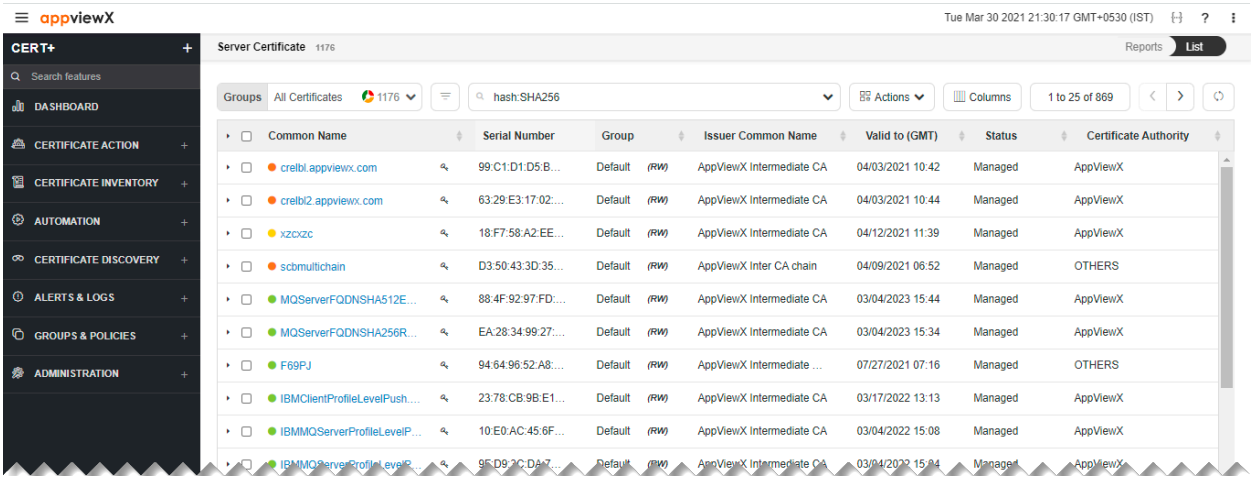


Key Algorithm - Server

This report shows the count of certificates with respect to the key algorithms available in the server inventory.

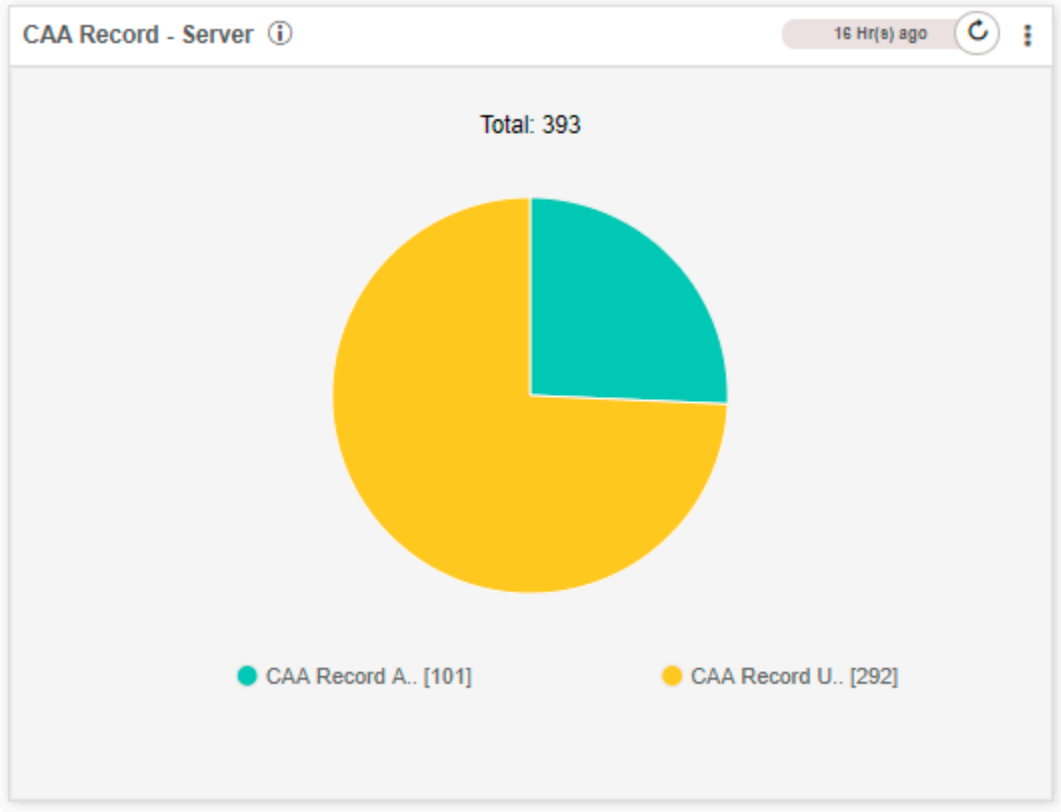


On click of the report, the filtered data of certificates will be shown as below:

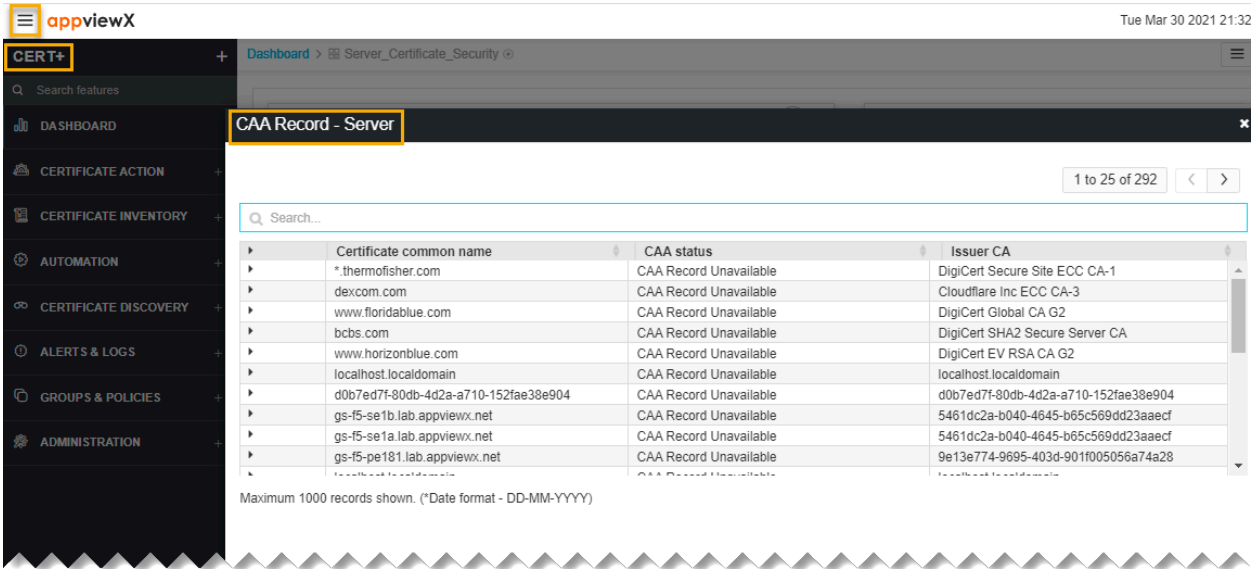


CAA Record – Server

This report shows the count of certificates with and without CAA records in the server inventory.

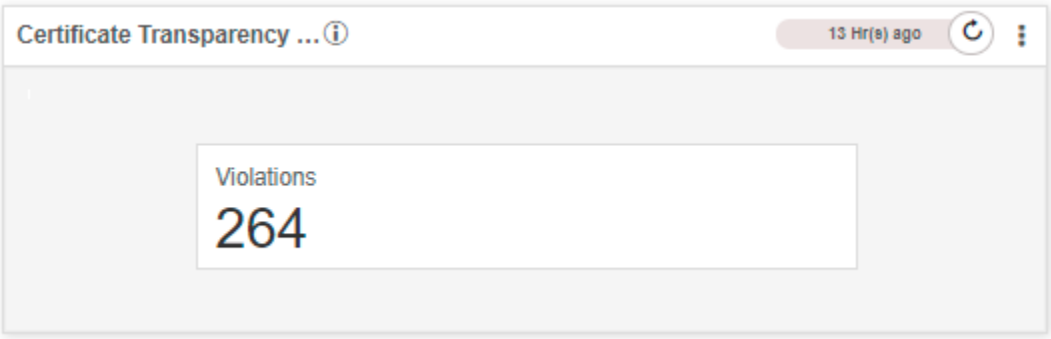


On click of the report, the filtered data of certificates will be shown as below:

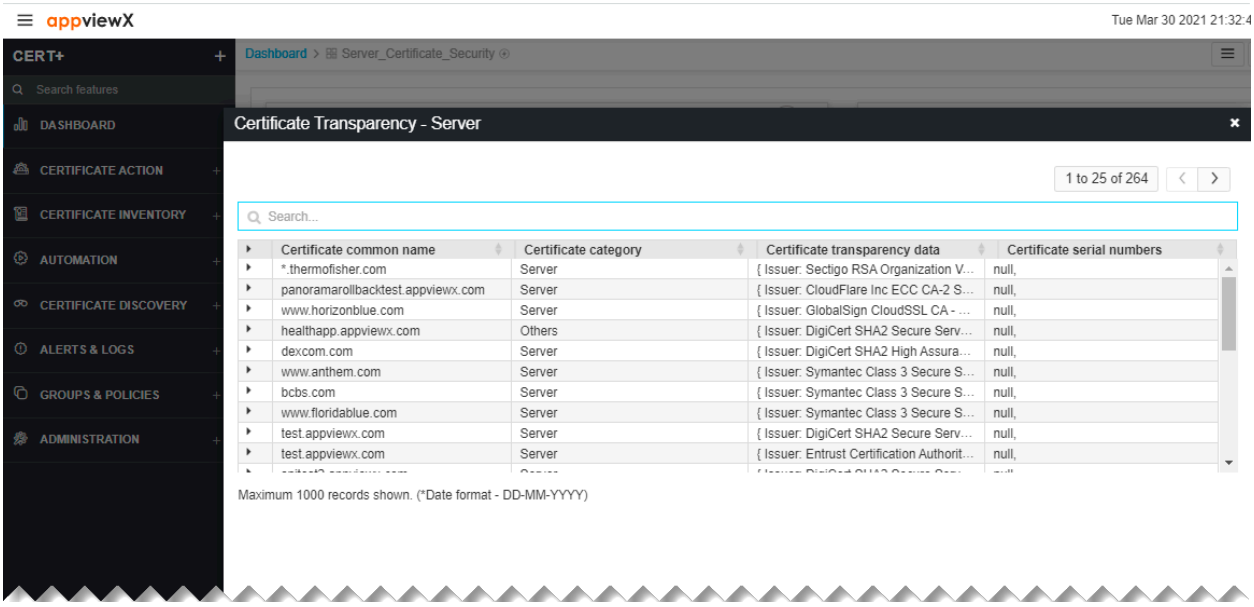


Certificate transparency – Server

This report shows the count of domain names for which more certificates are available and only a few are managed/monitored in server certificate inventory.



On click of the report, the filtered data of certificates will be shown as below:



Client Certificate Security Dashboard

- Client Certificate Security Dashboard
- Hash Algorithm - Client
- Key Algorithm - Client

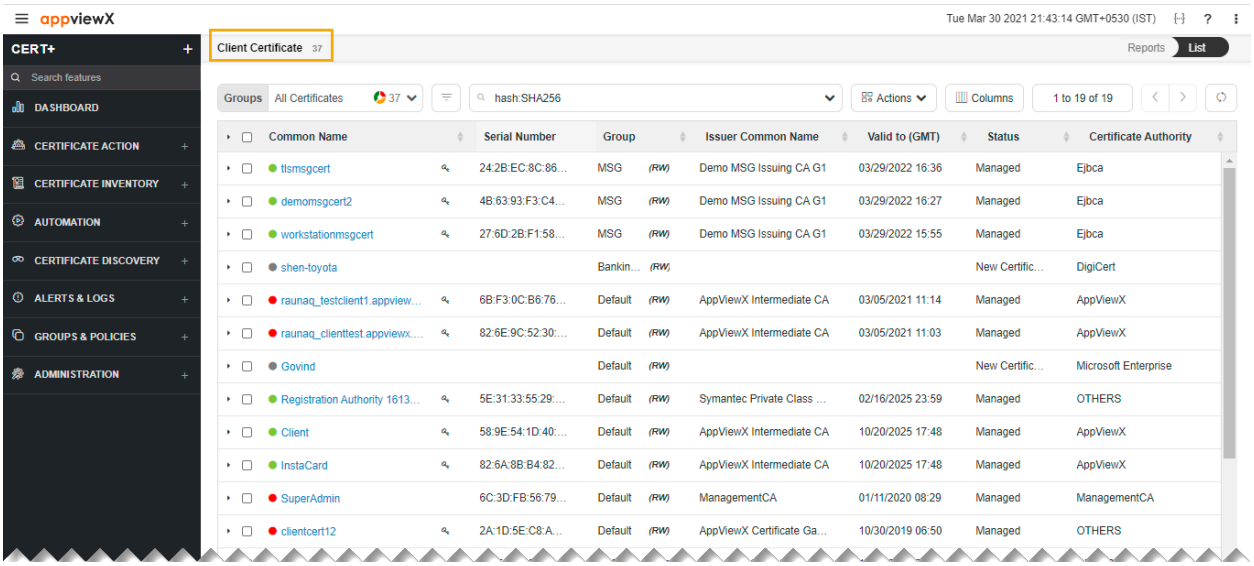
Client Certificate Security Dashboard

For the certificates in the Client inventory, this dashboard will be shown as the reports:

Hash Algorithm - Client

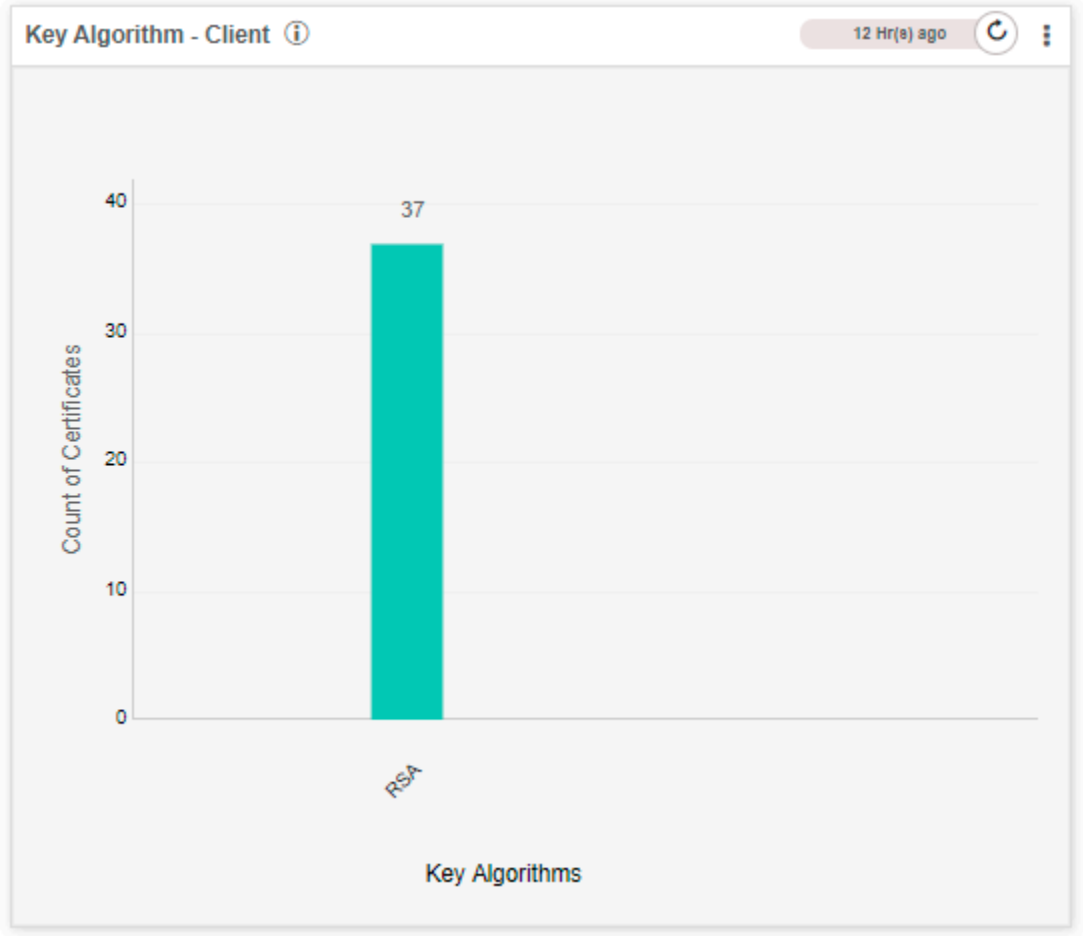
This report shows the count of certificates with respect to the hash algorithm available in the Client inventory.

On click of anywhere in the report, the filtered data of certificates will be shown as below:



Key Algorithm - Client

This report shows the count of certificates with respect to the key algorithms available in the Client inventory.



On click of anywhere in the report, the filtered data of certificates show the details.

Server Endpoint Security Dashboard

- Server Endpoint Security Dashboard
- TLS version - Server
- Cipher suites - Server
- Heartbleed & Poodle report - Server

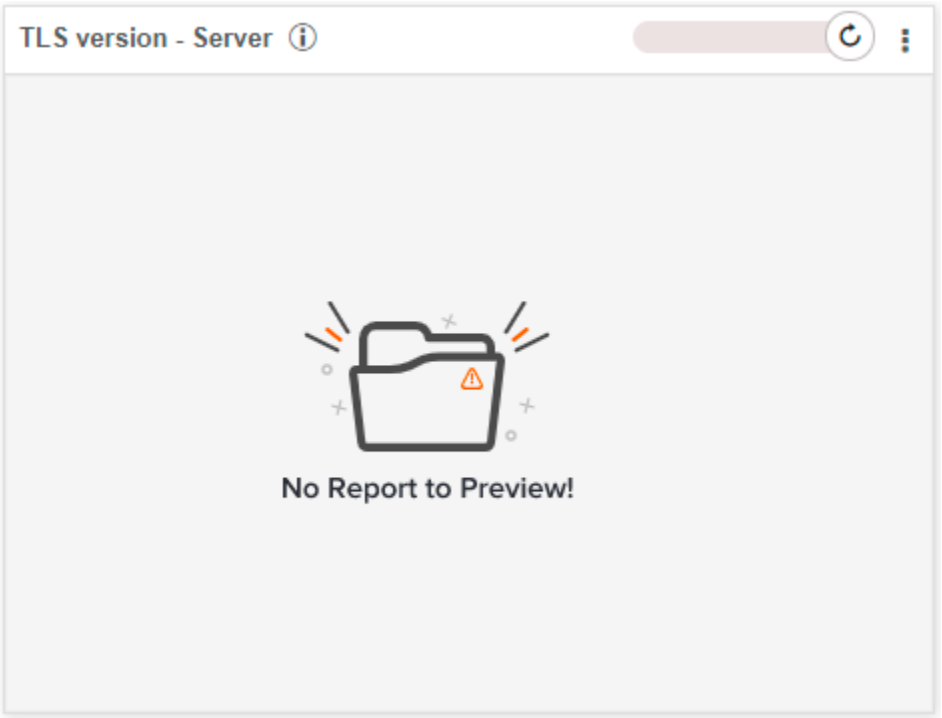
- Certificate Monitor Statuses - Server
- Certificate Auto Push - Server

Server Endpoint Security Dashboard

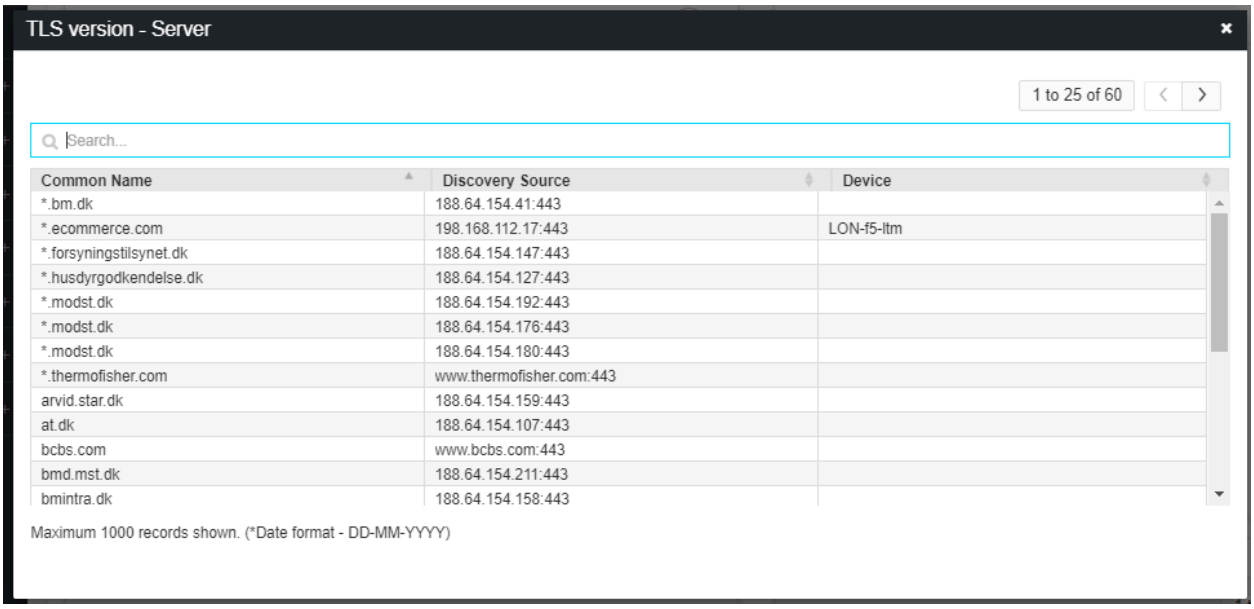
For the certificates in the Server inventory which are associated with the endpoints, from the security perspective, the following are the reports available:

TLS version - Server

This report shows the count of certificates with respect to the TLS versions available in the server inventory.

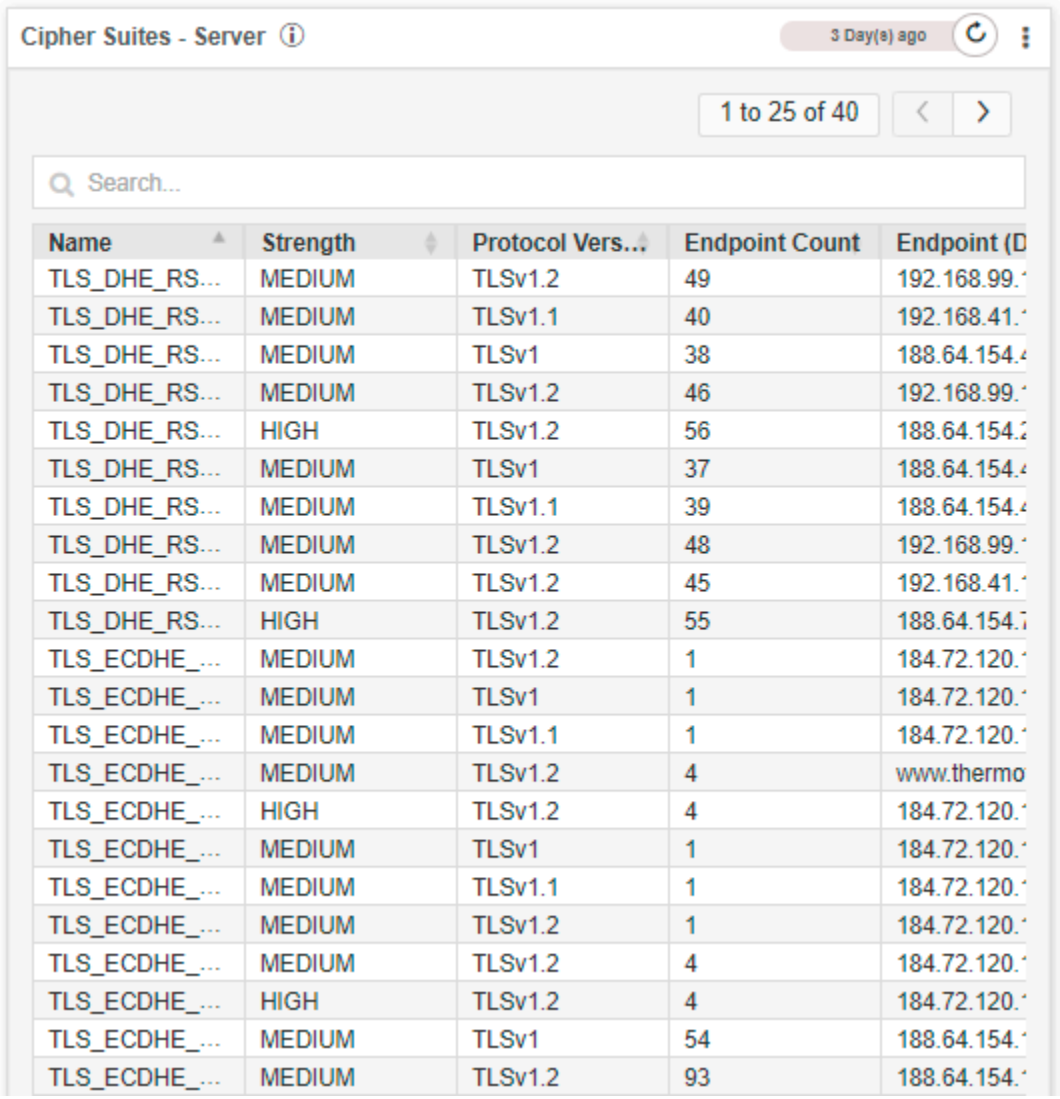


On click of the Endpoint Count value in the report, the respective data of certificates will be shown as below:

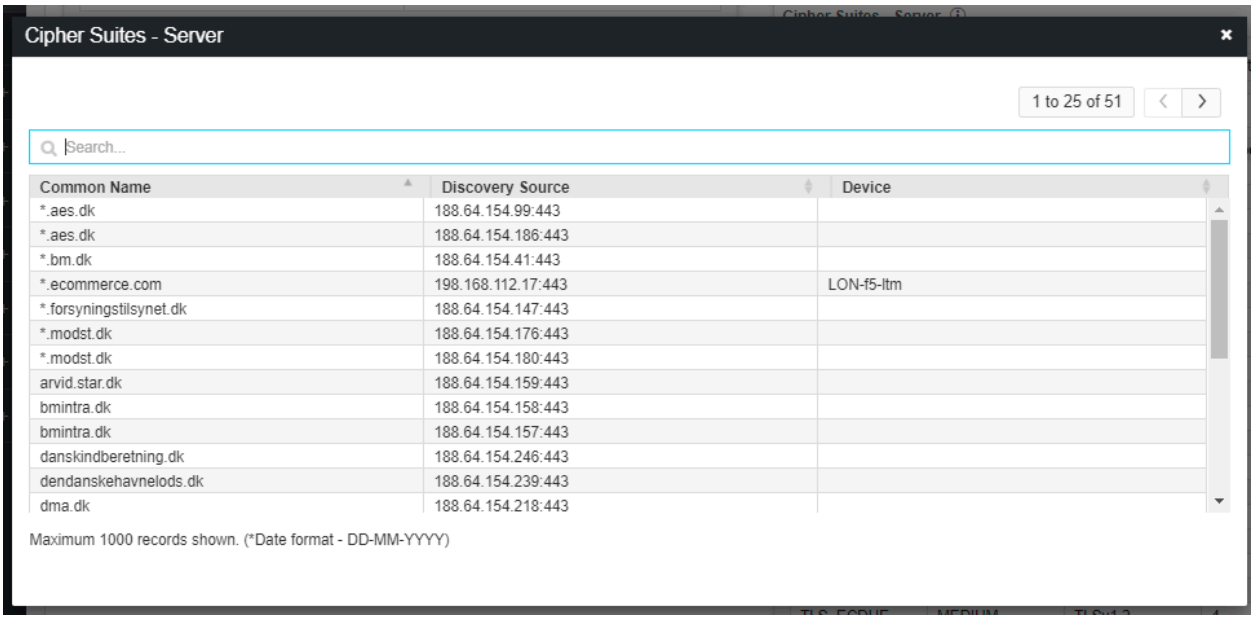


Cipher suites - Server

This report shows the count of certificates with respect to the cipher suite details and the TLS versions. The cipher suites are shown based on the priority.

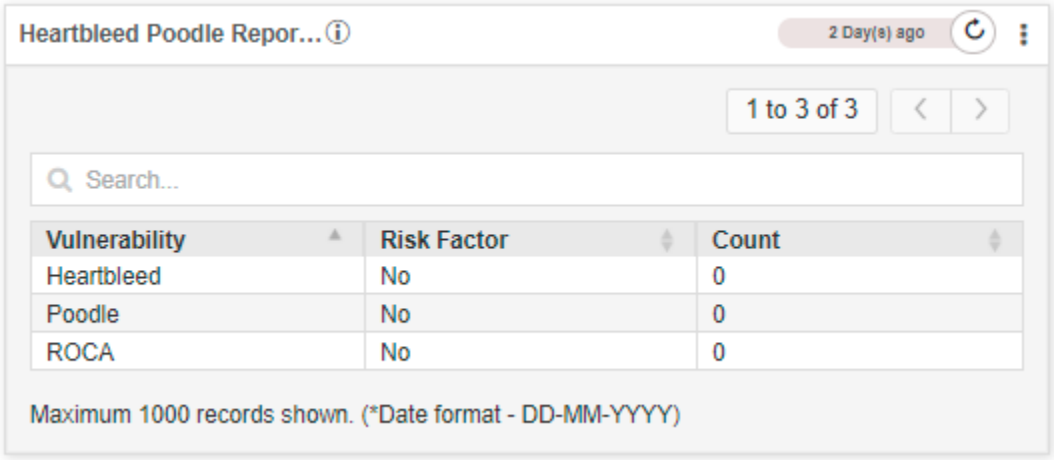


On click of the Endpoint count value in the report, the respective data of certificates will be shown as below:

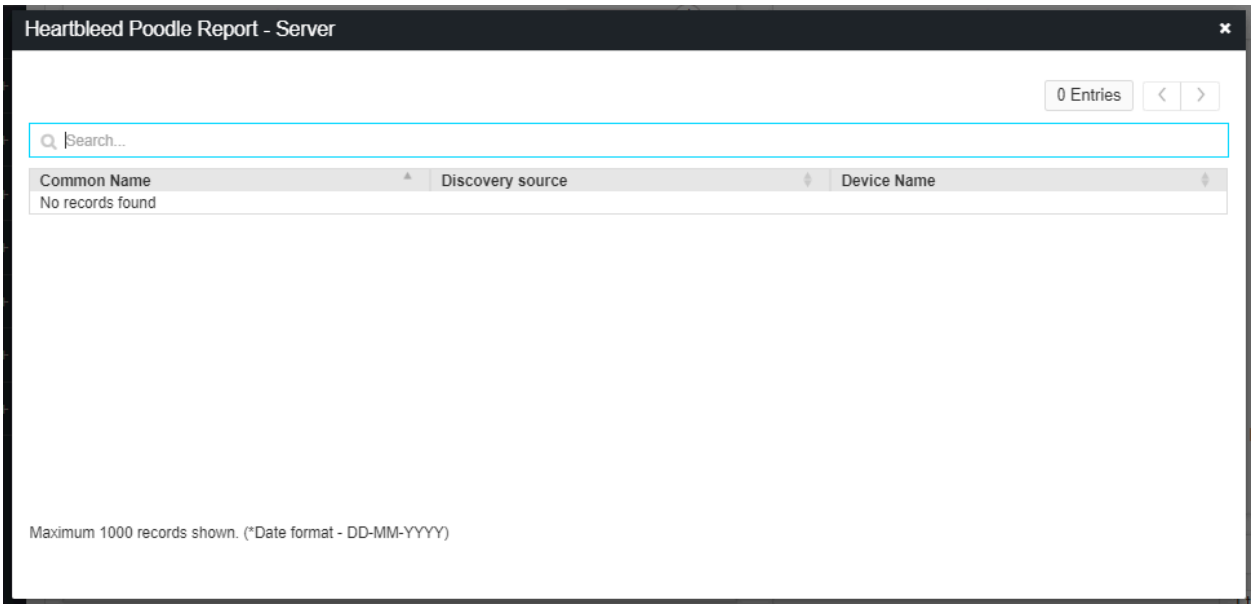


Heartbleed & Poodle report - Server

This report shows the count of device endpoints are exposed to Heartbleed, Poodle, and ROCA vulnerabilities.



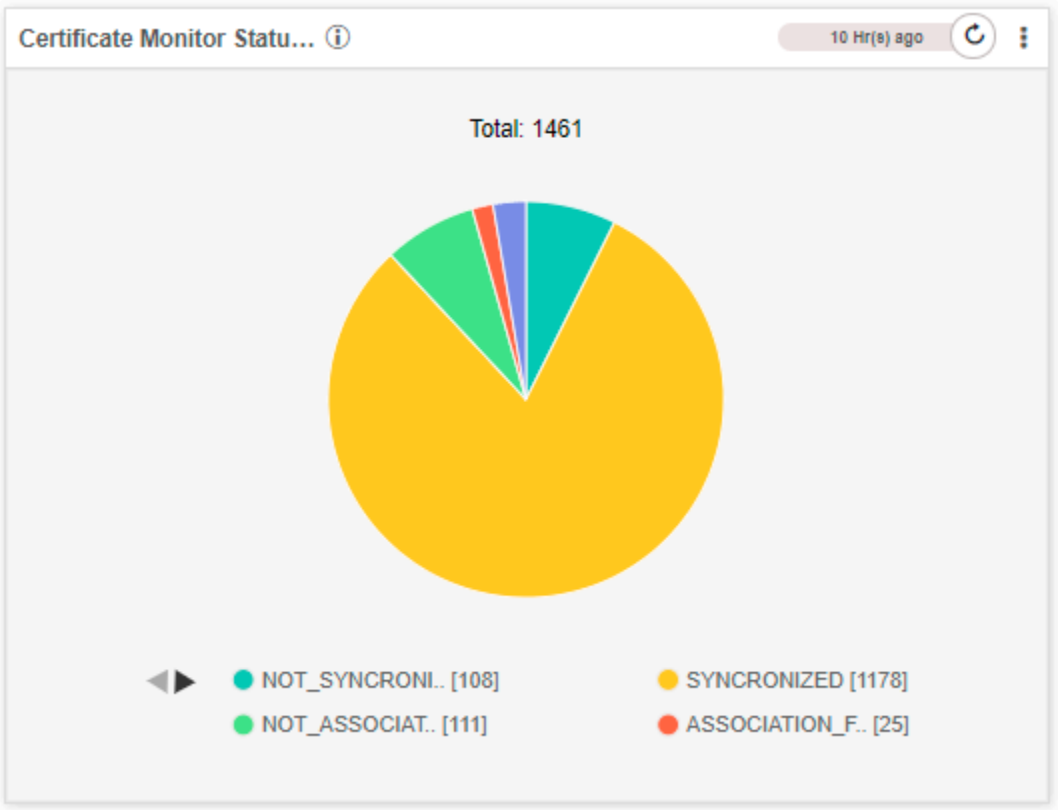
On click of the Count value in the report, the respective data of certificates will be shown as below:



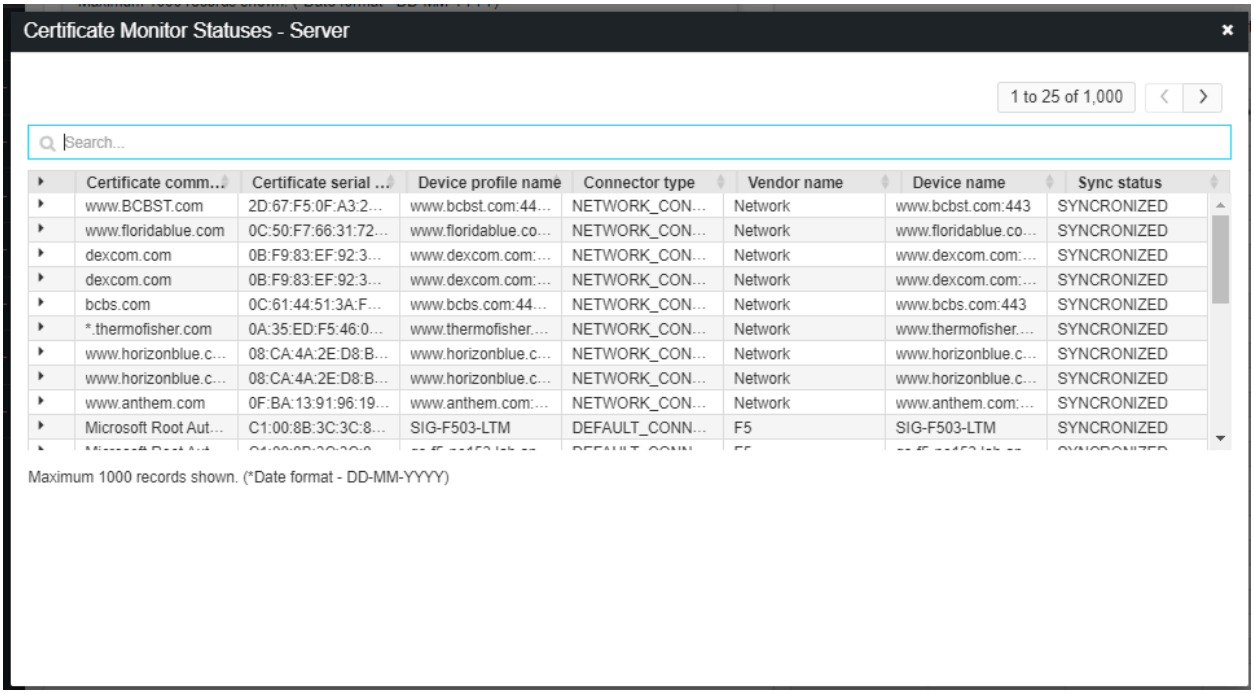
Note: Since there are no vulnerable data available in the product, this report is shown as No records found.

Certificate Monitor Statuses - Server

This report shows the count of domain names for which more certificates are available and only a few are managed/monitored in the Client certificate inventory.

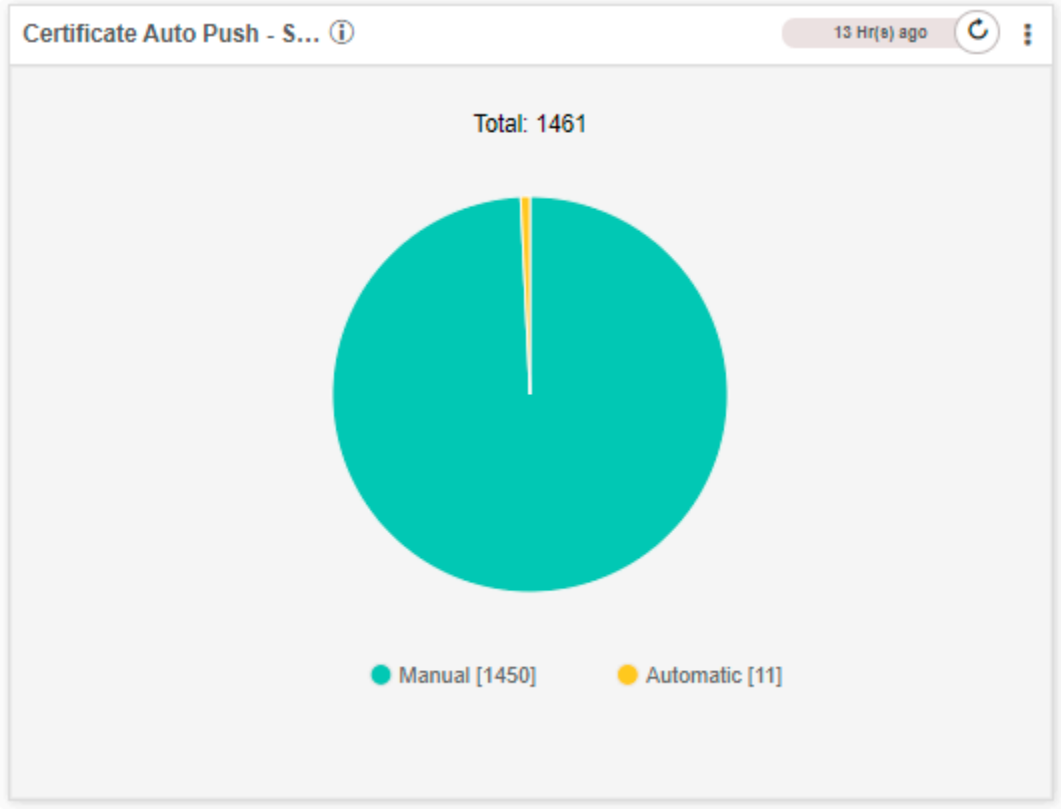


On click of the chart in the report, the respective data of certificates will be shown as below:



Certificate Auto Push - Server

This report shows the count of certificates in the Server inventory which are enabled and not enabled with auto push feature.



If you click on the chart, the respective details will be shown.

Client Endpoint Security

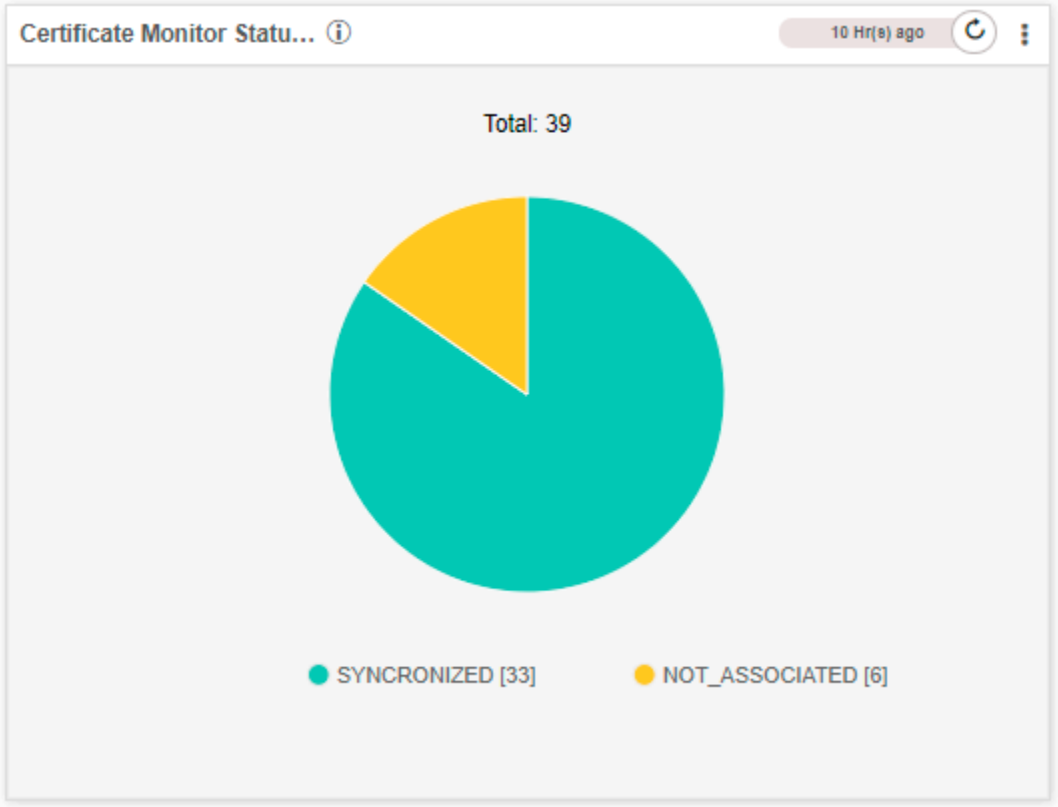
- Client Endpoint Security
- Certificate Monitor Statuses - Client
- Certificate Auto Push - Client
- Shared Client Report

Client Endpoint Security

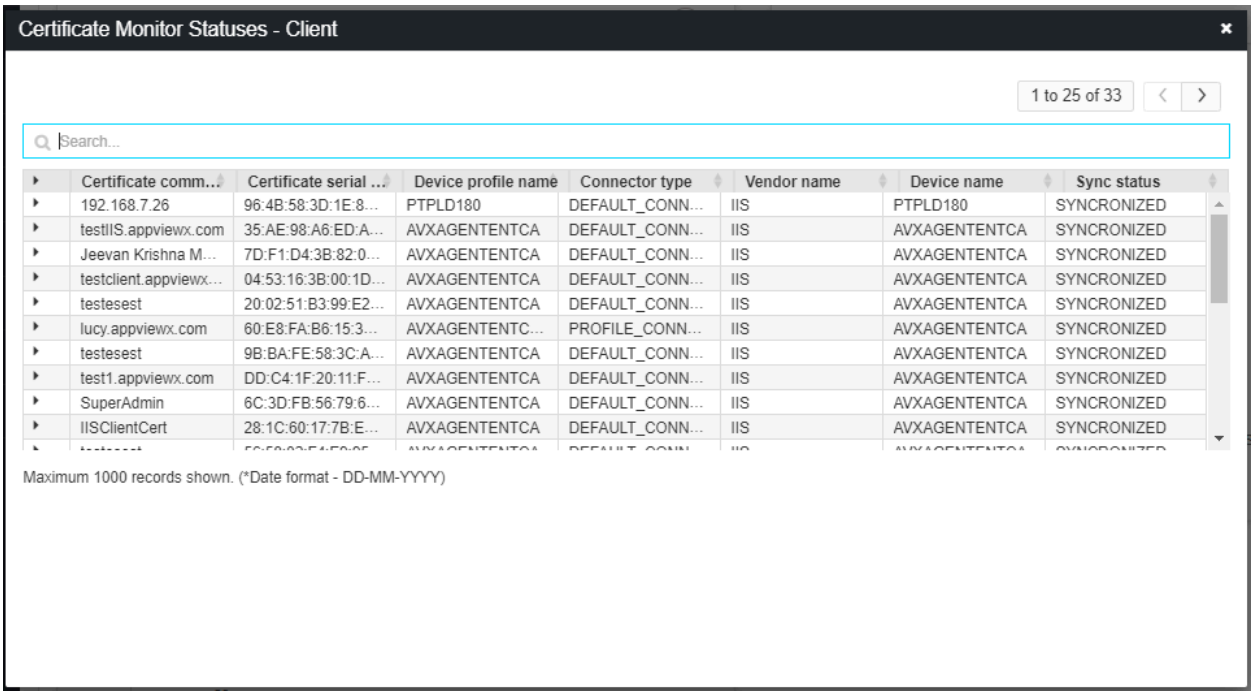
For the certificates in the Server inventory which are associated with the endpoints, from the security perspective, the following are the reports available:

Certificate Monitor Statuses - Client

This report shows the count of endpoints with respect to their certificate monitor statuses available in the client inventory.

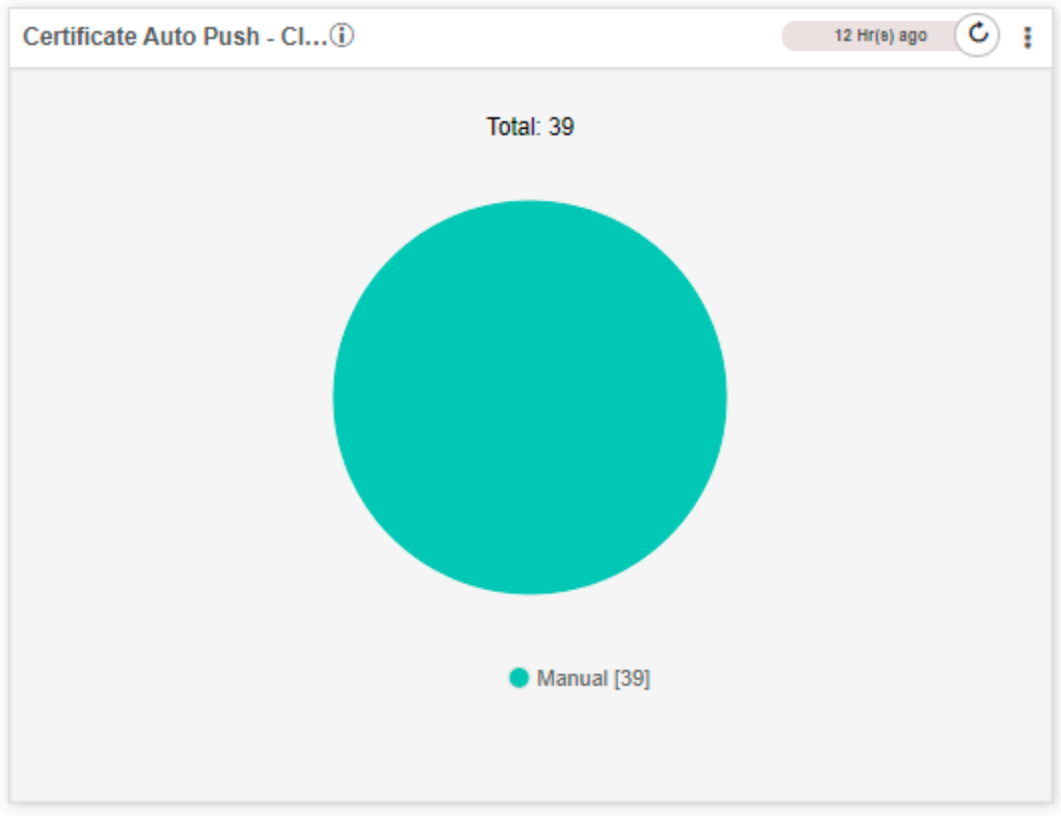


On click of this chart, the respective filtered data of certificates be shown as below:

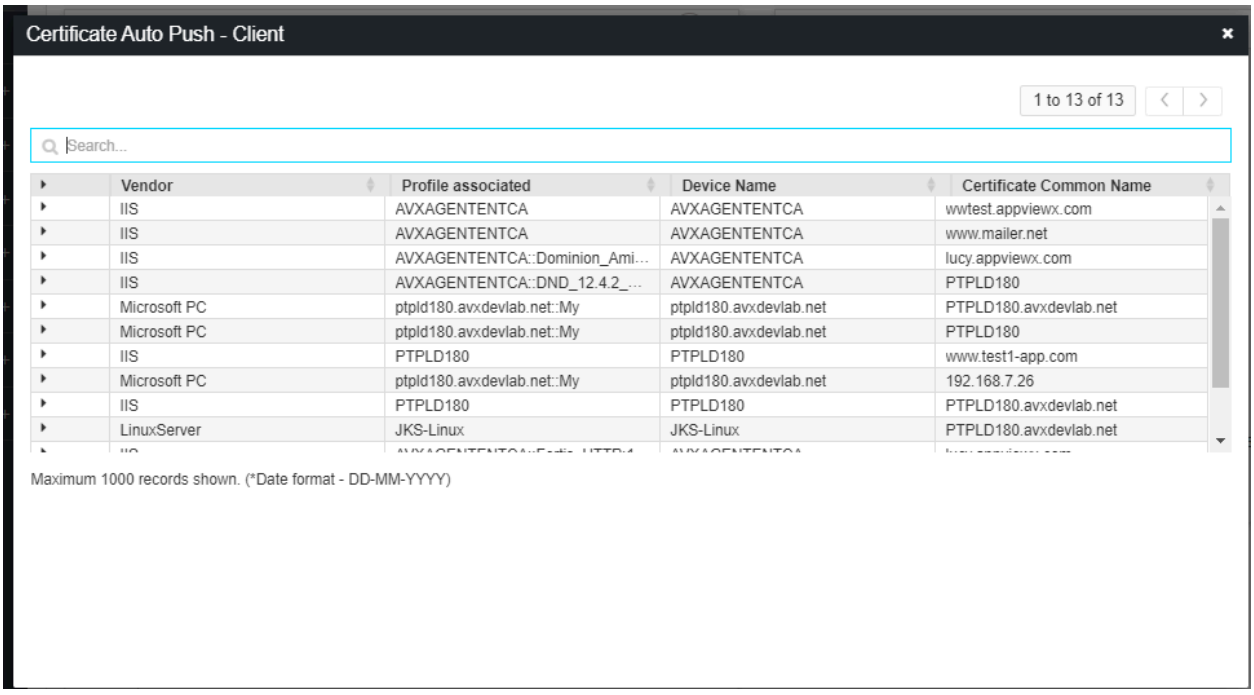


Certificate Auto Push - Client

This report shows the count of certificates in the client inventory which are enabled and not enabled with auto push feature.

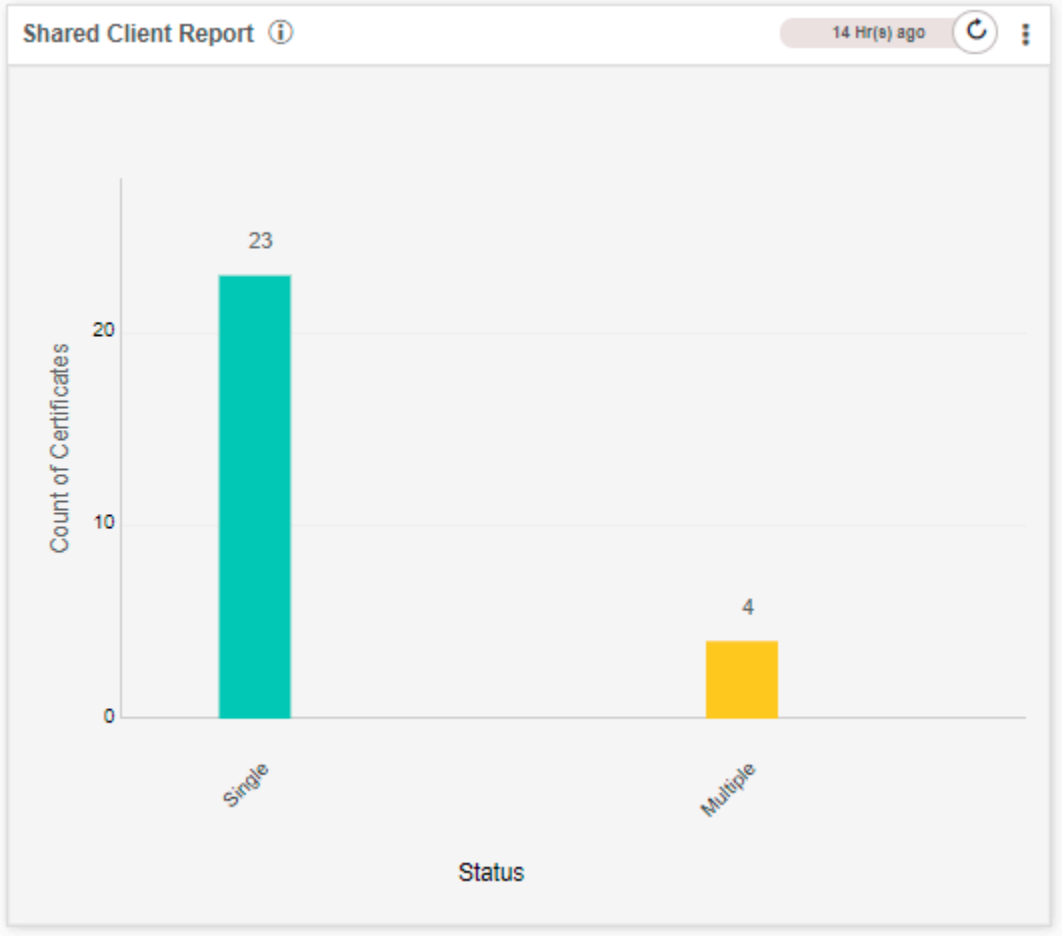


On click of this chart, the respective filtered data of certificates be shown as below:

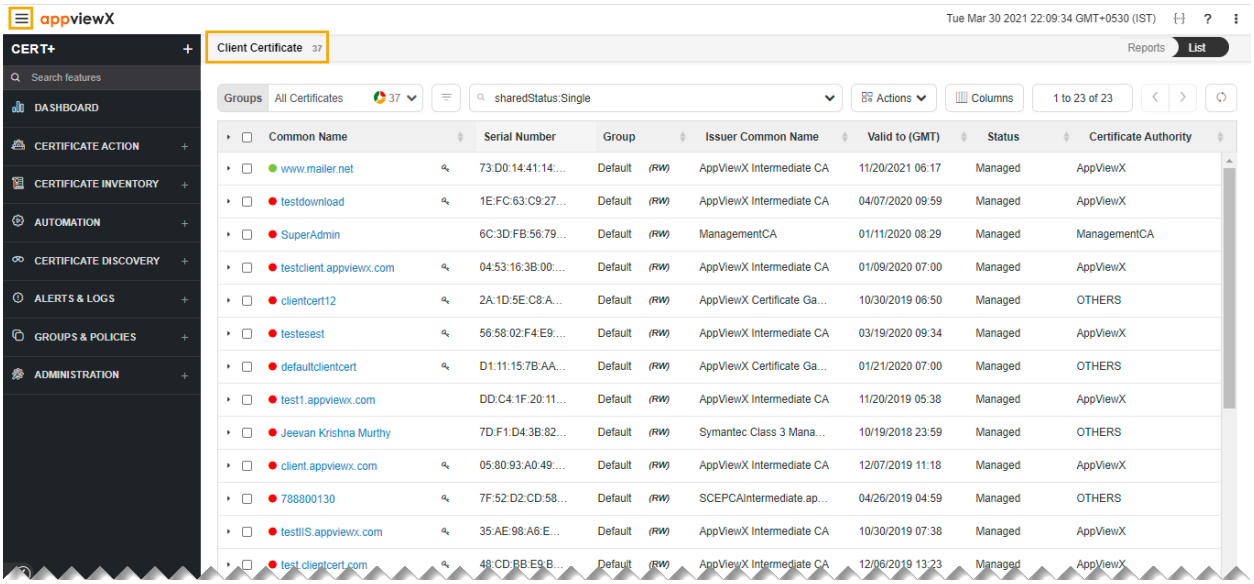


Shared Client Report

This report shows the count of certificates in the client inventory which are shared with a single endpoint or multiple endpoints.



On click of this chart, the respective filtered data of certificates be shown as below:



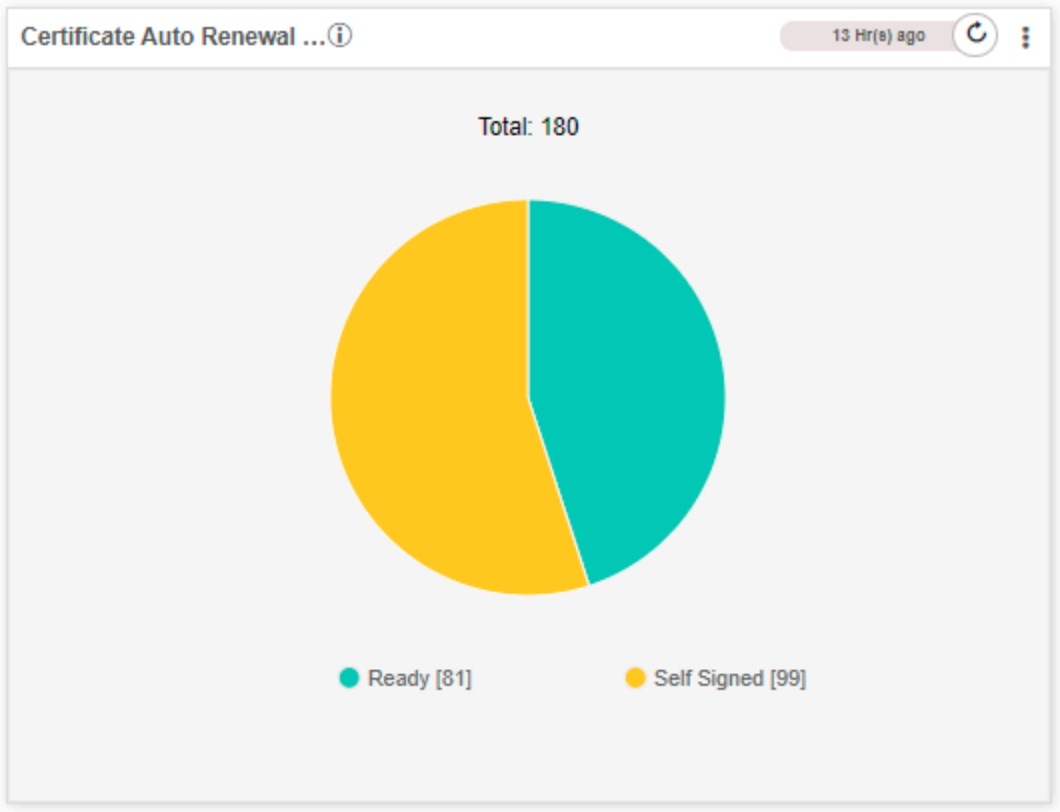
Server Standard Dashboard

Server Standard Dashboard

For the certificates in the Server inventory, from the standard perspective, the following are the reports available in this dashboard:

Certificate Auto-Renewal Readiness - Server

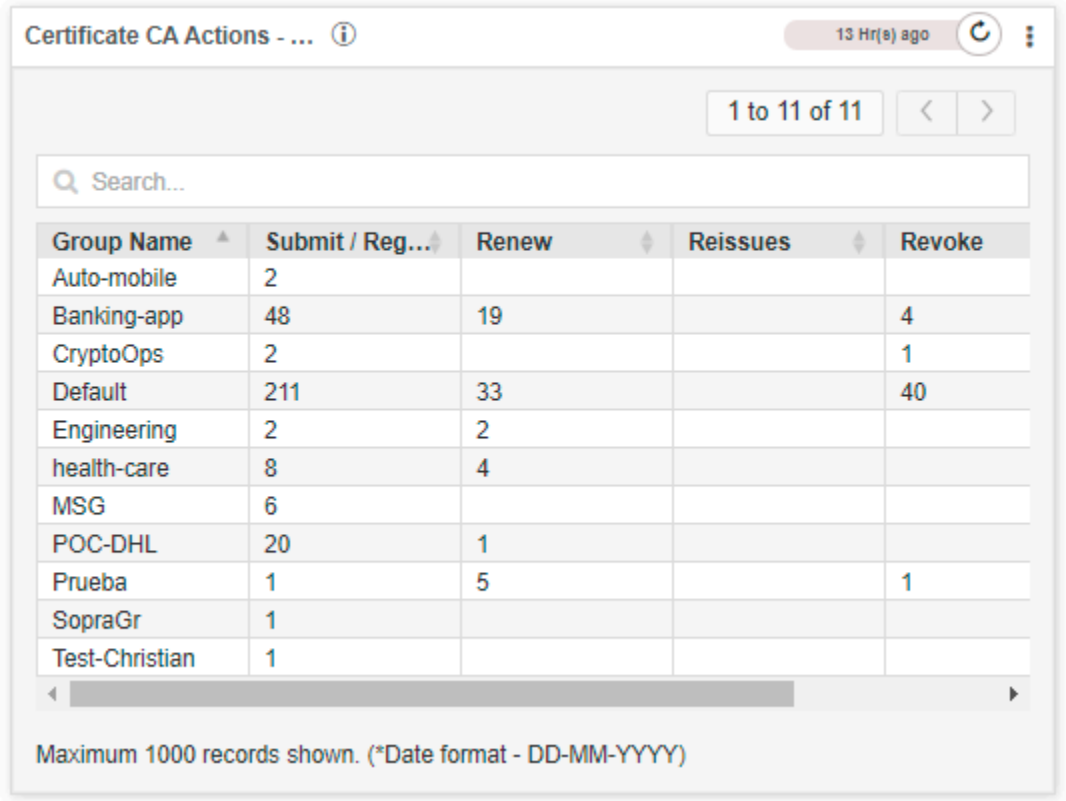
This report shows the count of certificates ready for the auto-renewal process available in the server inventory.



On click of the chart, the filtered data of certificates are shown as below:

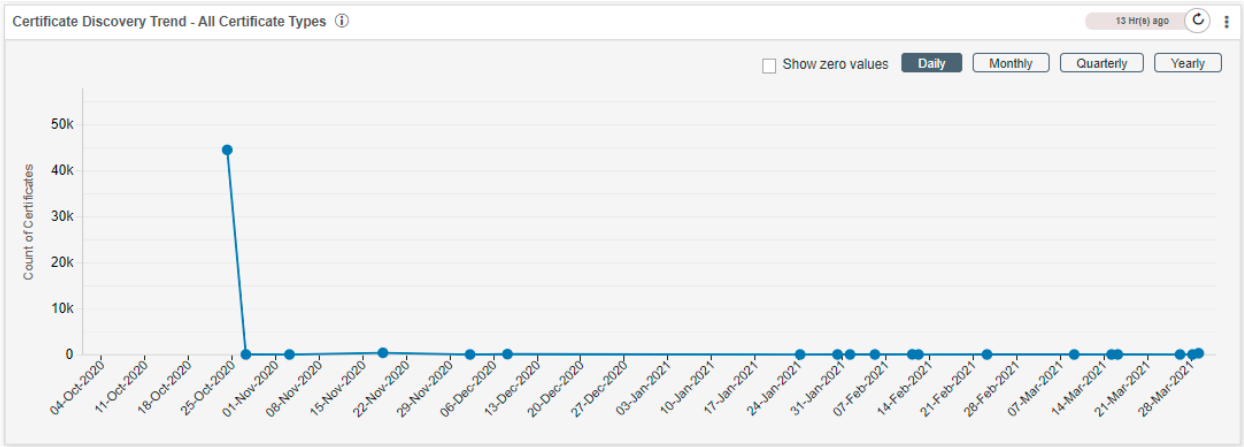
Certificate CA Actions - All Certificate Types

This report shows the count of CA actions performed with respect to the certificate groups available in the server inventory.



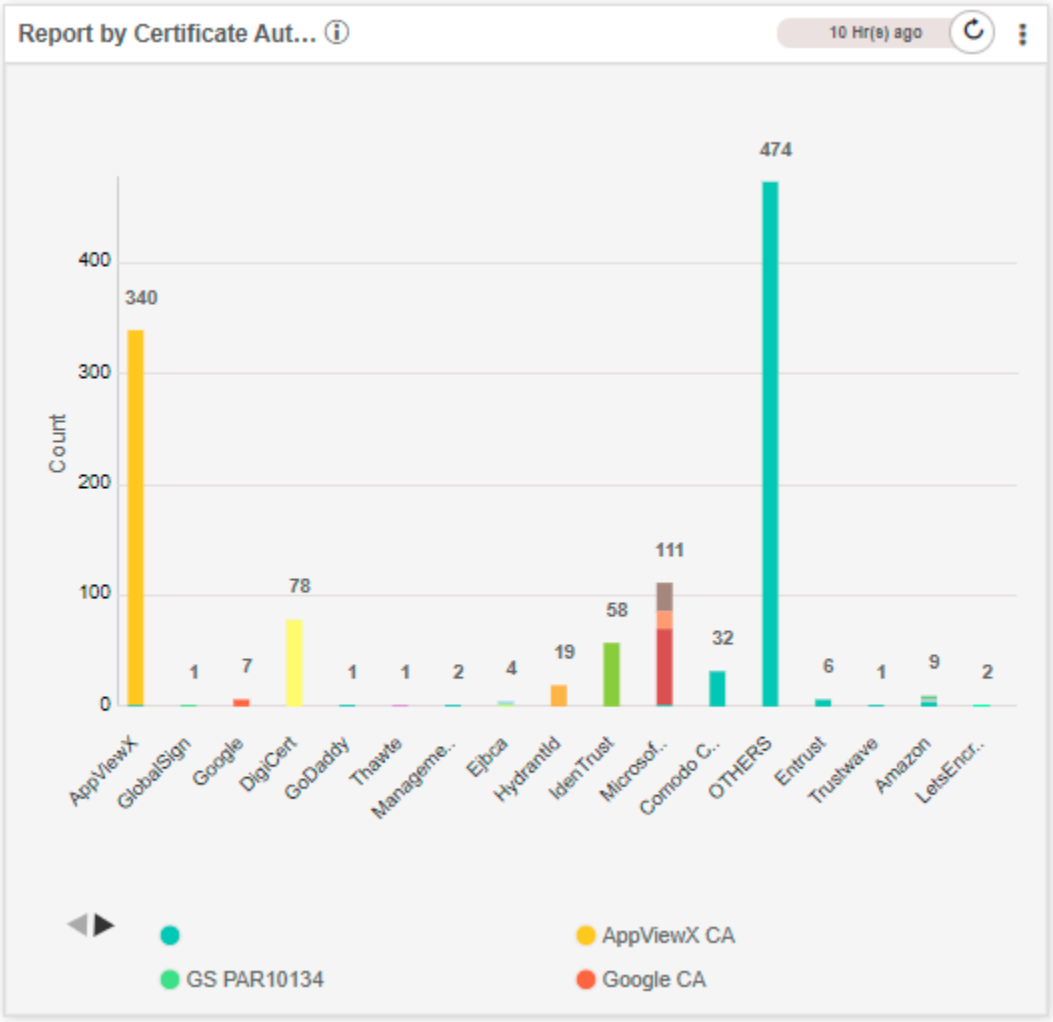
Certificate Discovery Trend - All Certificate Types

This report shows the trend of the count of certificates discovered into AppViewX in the last year.

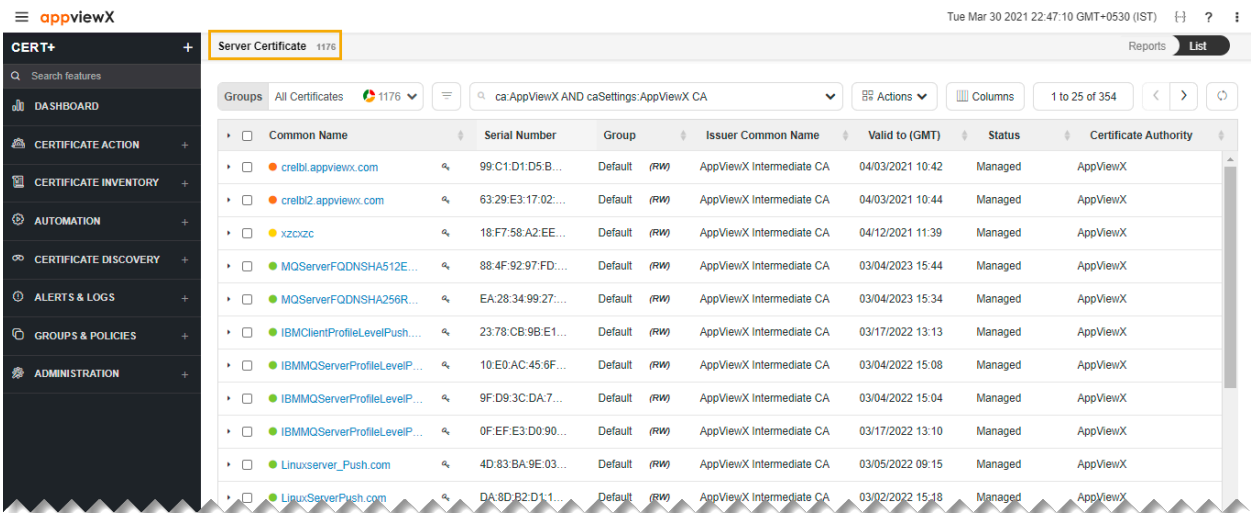


Report by Certificate Authority - Server

This report shows the count of certificates available in the server inventory with respect to the CA accounts.



When you click of the chart, the filtered data of certificates are shown as below:



Client Standard Dashboard

Client Standard Dashboard

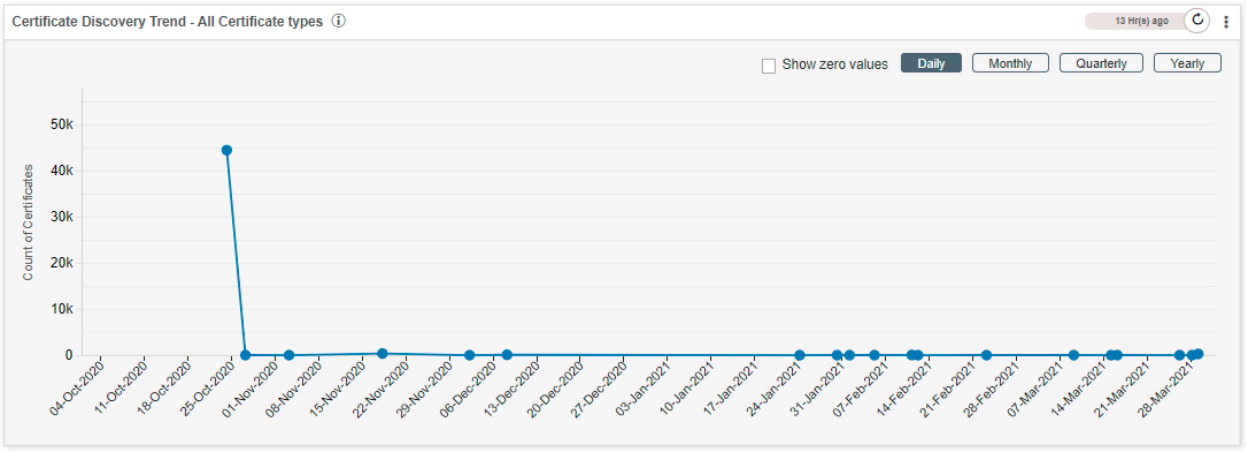
For the certificates in the Client inventory, from the standard perspective, the following are the reports available in this dashboard:

Certificate Auto-Renewal Readiness - Client

This report shows the count of certificates ready for the auto-renewal process available in the Client inventory.

Certificate Discovery Trend - All Certificate Types

This report shows the trend of the count of certificates discovered in AppViewX in the last year.



Certificate CA Actions - All Certificate Types

This report shows the count of CA actions performed with respect to the certificate groups available in the Client inventory.

Certificate CA Actions - ... 13 Hr(s) ago

1 to 11 of 11

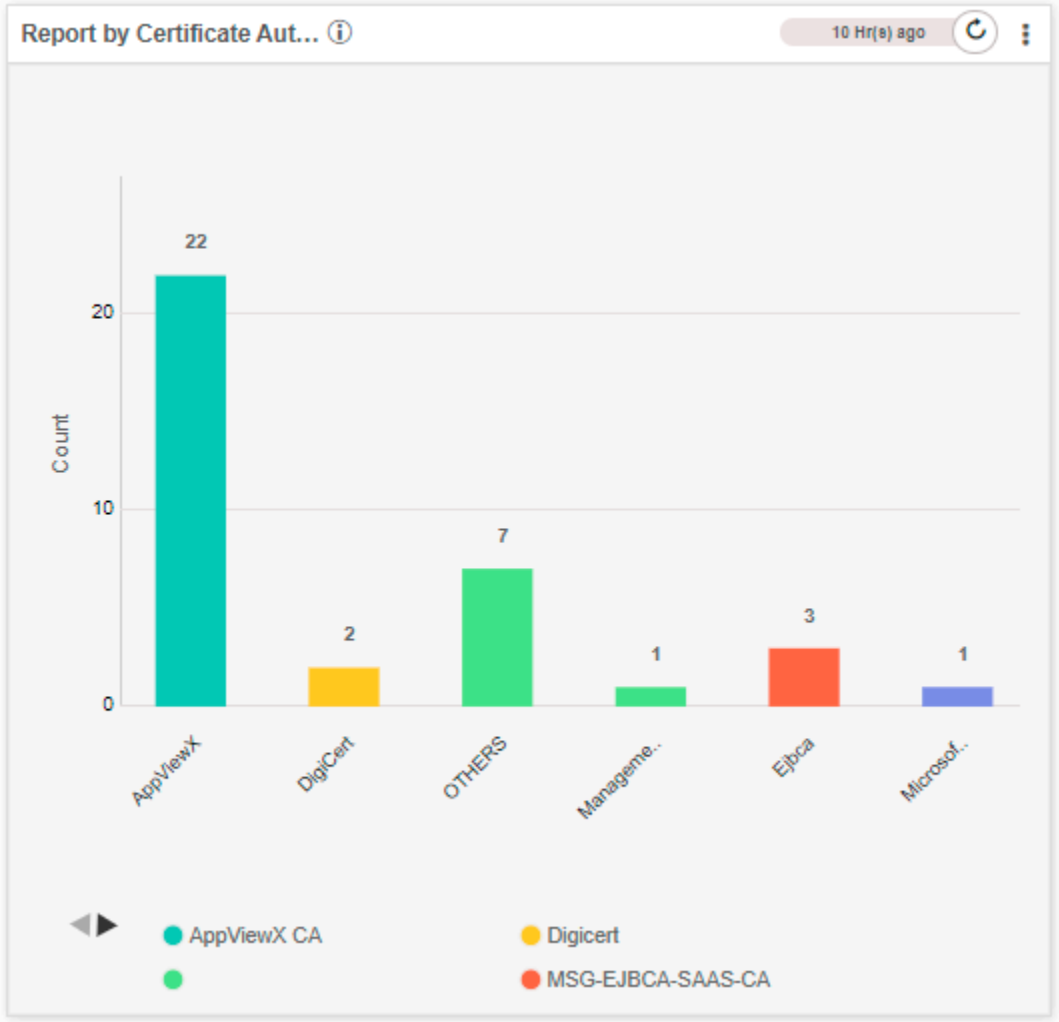
Search...

Group Name	Submit / Reg...	Renew	Reissues	Revoke
Auto-mobile	2			
Banking-app	48	19		4
CryptoOps	2			1
Default	211	33		40
Engineering	2	2		
health-care	8	4		
MSG	6			
POC-DHL	20	1		
Prueba	1	5		1
SopraGr	1			
Test-Christian	1			

Maximum 1000 records shown. (*Date format - DD-MM-YYYY)

Report by Certificate Authority Accounts - Client

This report shows the count of certificates available in the client inventory with respect to the CA accounts.



On click of the chart, the respective filtered data of certificates will be shown.

Trust Store Certificates

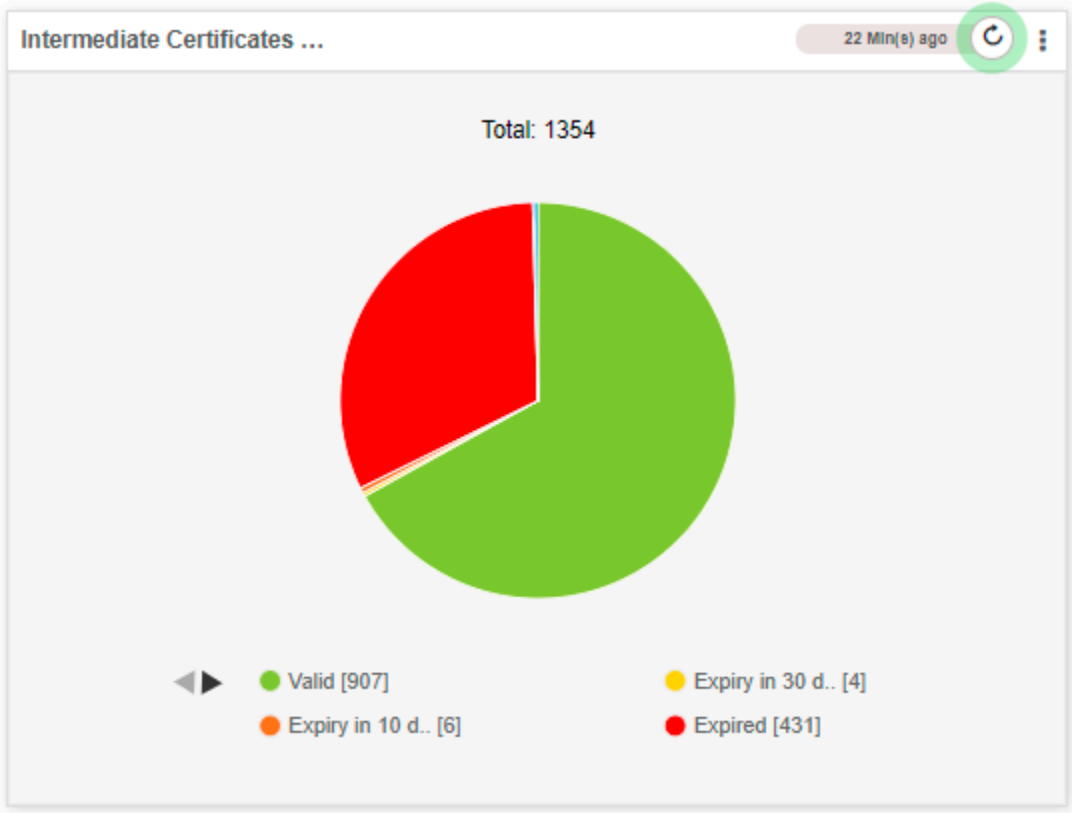
- Trust Store Certificates
- Intermediate Certificates Expiry Statuses
- Root Certificates Expiry Statuses

Trust Store Certificates

For the certificates in the Root and Intermediate inventories, the following are the reports available in this dashboard:

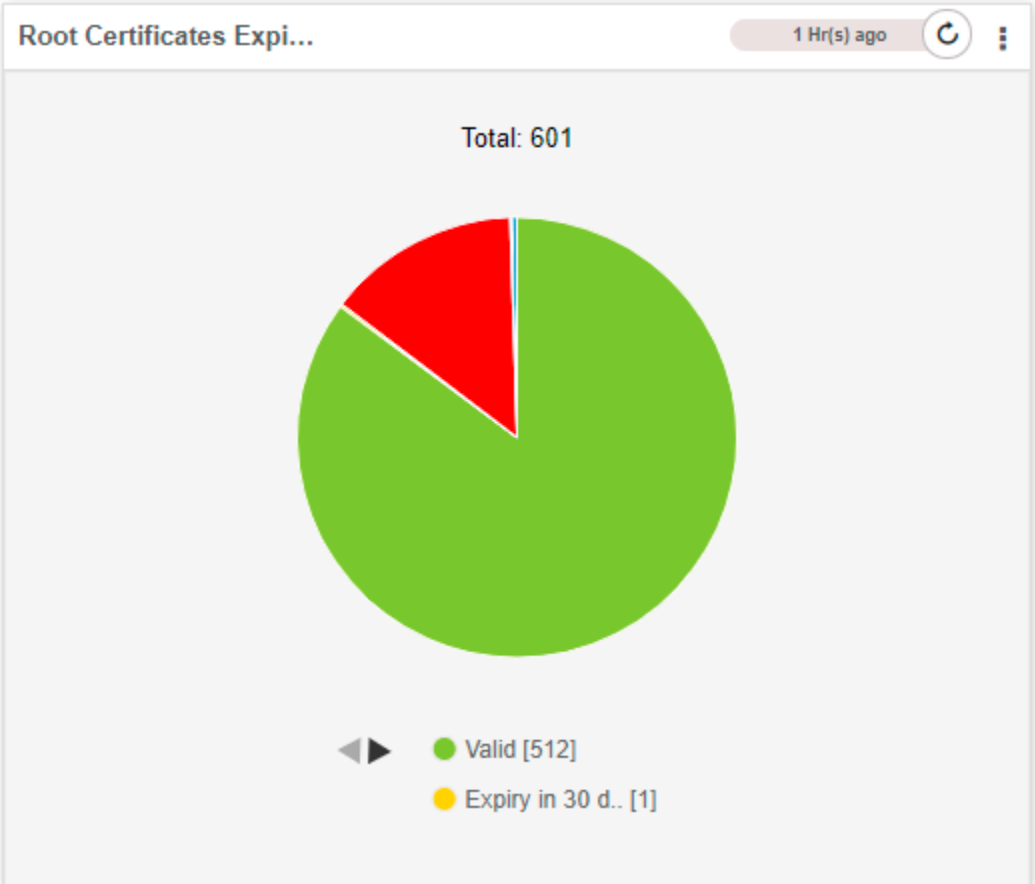
Intermediate Certificates Expiry Statuses

This report shows the count of certificates in the intermediate certificate inventory with respect to the valid and expiry status of the certificates.



Root Certificates Expiry Statuses

This report shows the count of certificates in the root certificate inventory with respect to the valid and expiry status of the certificates.



Report Customization

AppViewX CERT+ allows you to customize your reports based on the organization's needs. Depending on the customization, reports are classified into:

- My Reports
- Store
- Widget

My Reports

Personalized reports can be generated based on a user account. This will be useful when an operator is assigned to do a specific task and has to generate reports on the same. To know more about **My Reports**, refer below.

- Create a New Report
- Clone a Report

- Delete a Report
- Pin a Report
- Share a Report

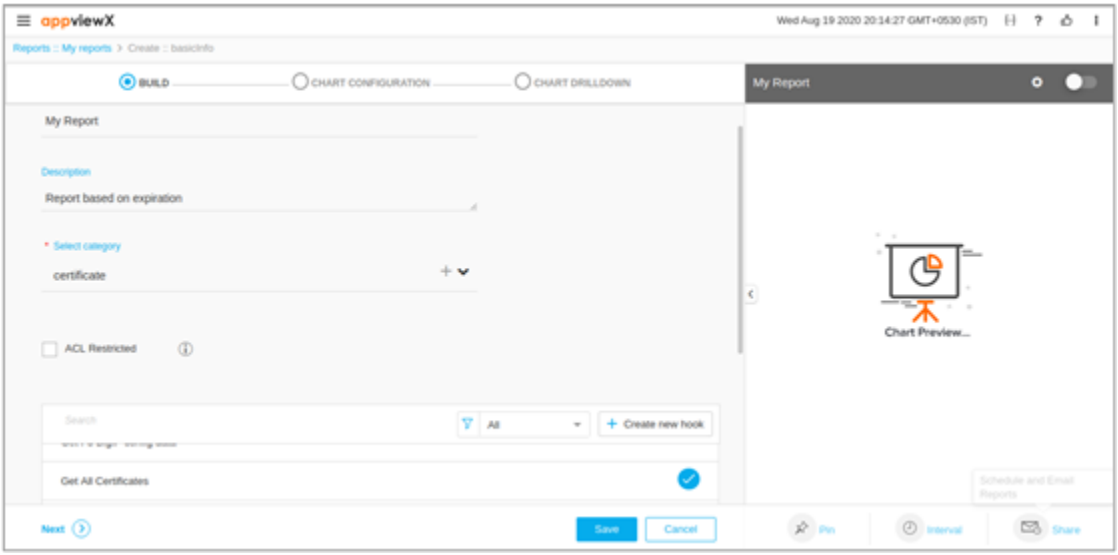
Create a New Report

To generate or create reports,

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

   The left navigation pane appears.
3. Click **Studio > Reports**.

   By default, **My Reports** page will be displayed.
4. Click **Create New Report** on the top-right.
5. On the **Create Report** page, enter the **Report Name**, **Description** and select a **Category** from the list.
6. Enable **ACL Restricted** option if required.
7. Select **ACL settings** to query certificates based on the role of permission.
8. Select a hook from the list of available hooks or click **Create New Hook**.
9. Click **Save** to save details.
10. Click **Next** at the bottom-left.



11. On the **Chart Configuration** page, select one of the following chart types:
    - Pie
    - Donut

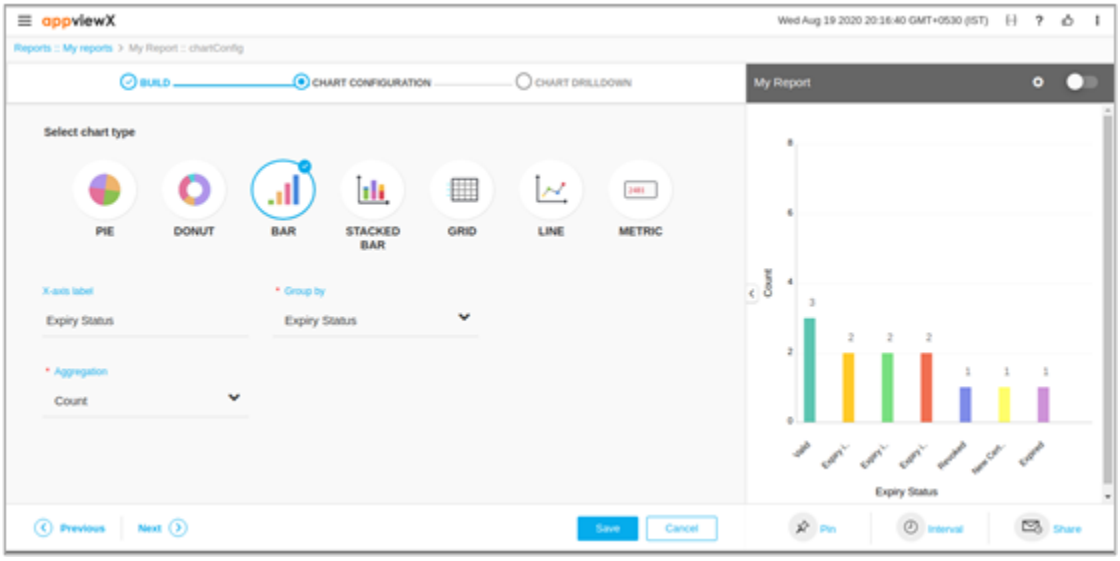
- Bar
- Stacked Bar
- Grid
- Line
- Metric

- If you have selected **Pie** chart type, choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Donut** chart type, choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected the **Bar chart** type, fill the **X-axis Label** field and choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Stacked Bar** chart type, fill the **X-axis Label** field and choose an option from the **Group By**, **Aggregation**, and **Stacked By** dropdown.
- If you have selected **Grid** chart type, enable the **Show Column Headers** option if required. Then, under **Columns**, select columns or click the **Select All** option.

Note: For the Select All option, only 10 columns can be selected.

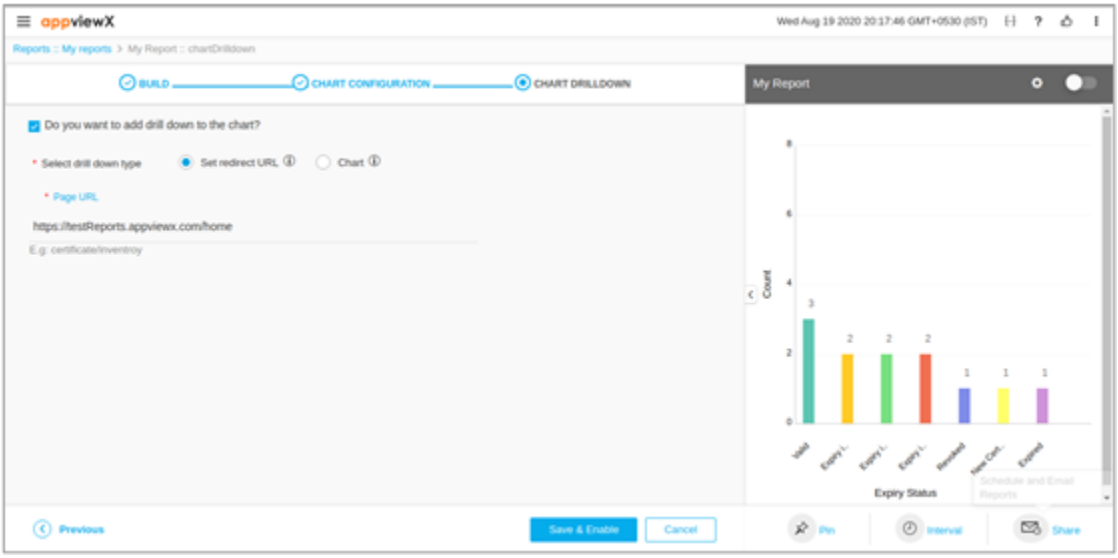
- If you have selected **Grid** chart type, fill the **X-axis Label** field, choose a **Date Format**, and choose an option from the **Group By** and **Aggregation** dropdown.

- If you have selected **Metric** chart type, enter a **Chart Title** and choose an option from the **Aggregation** dropdown. Under **Chart Formatting**, select a chart size, alignment, font color, and icon.



12. Click **Save**.
13. Click **Next** at the bottom-left.
14. On the **Chart Drilldown** page, enable the **Do you want to add drill down to the chart?** option to add drilldown.
15. Click **Save & Enable**.
    The graphical representation of the report will be displayed on the right.
16. To enable the generated report, click the enable icon on the top-right of the report window.
17. To pin the report to the dashboard page, click the **Pin** icon at the bottom right.
18. To set the polling interval to collect data, click the **Interval** icon at the bottom right.

19. To share the report, click the **Share** icon at the bottom right.

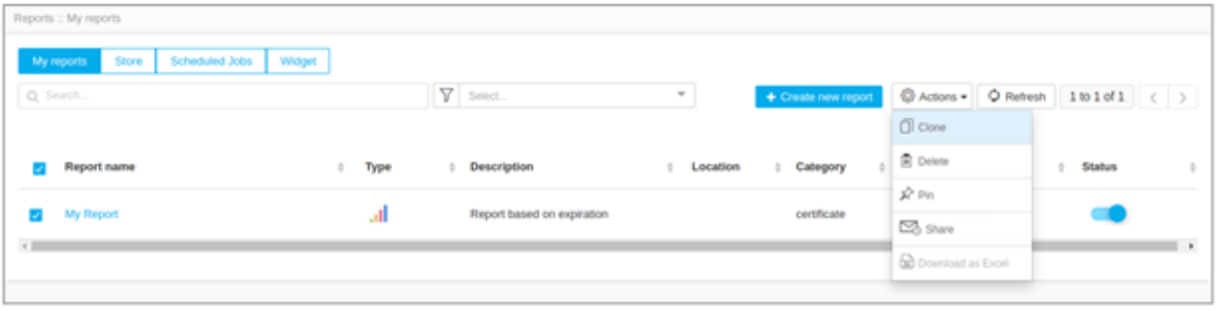


Clone a Report

To clone a report,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

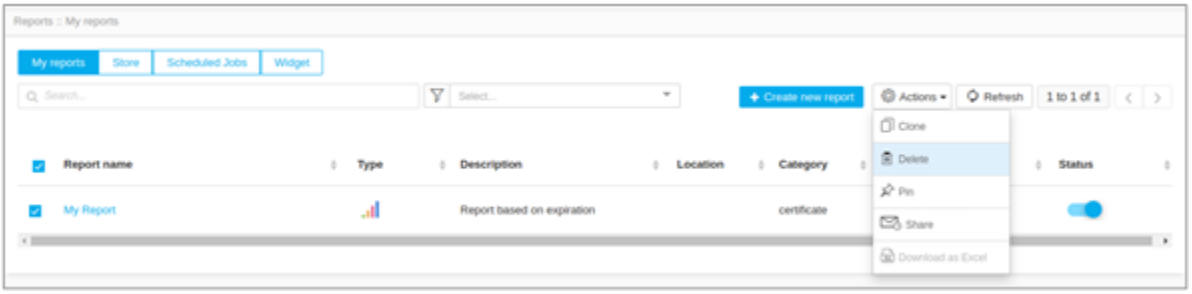
   The cloned reports will be displayed under the **My Reports** tab.



Delete a Report

To delete a report,

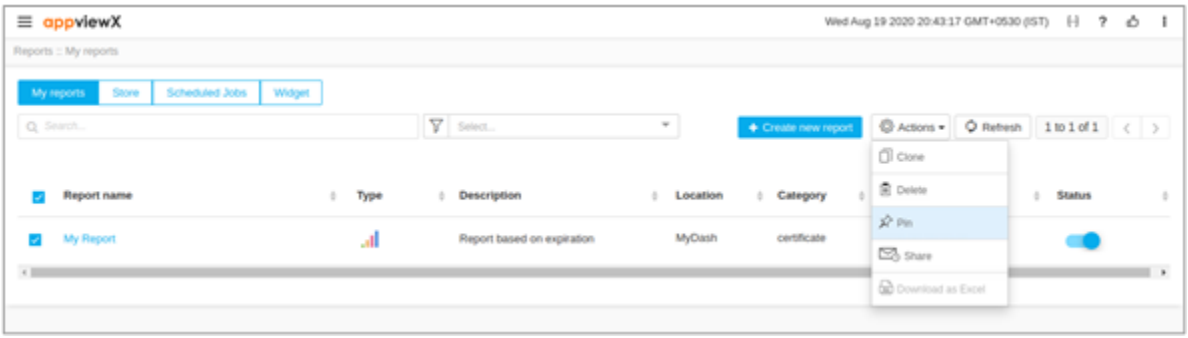
1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.



Pin a Report

To pin a report,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.

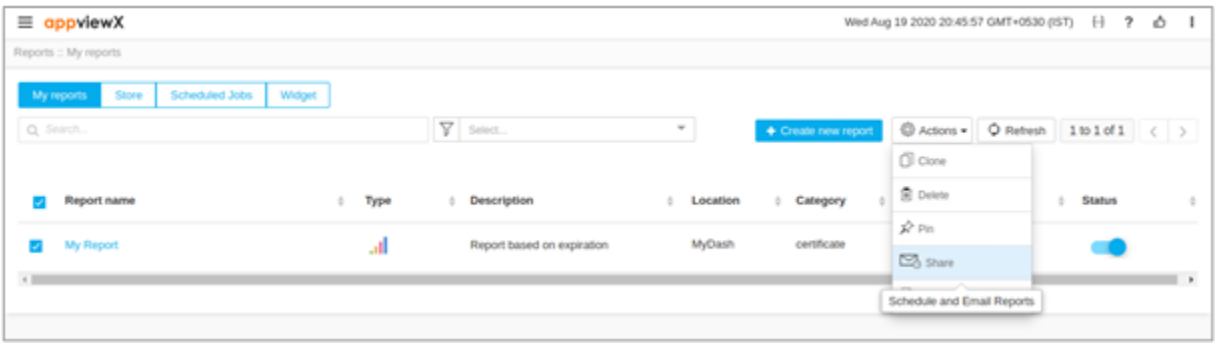


Share a Report

To share a report,

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

3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share** to schedule and email reports.
5. On the **Schedule reports** window, fill the **General** section for mail content and **Schedule** section for scheduling emails.
6. Click **Save**.



Store

There are a few pre-defined reports available in the store. These reports can be cloned and customized to have personalized reports, but cannot be modified. To know more about **Store**, refer below.

- View Pre-built Reports
- Clone a Pre-built Report
- Pin a Pre-built Report
- Share a Pre-built Report

View Pre-built Reports

To view Pre-built reports,

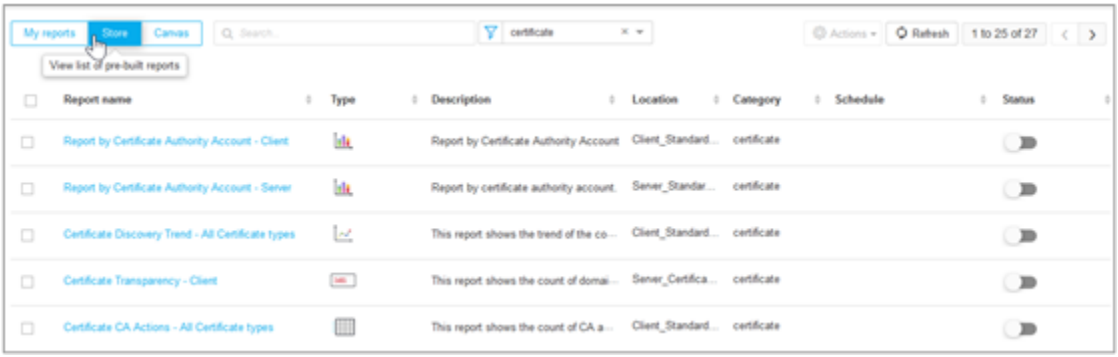
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

   The left navigation pane appears.
3. Click **Studio > Reports**.

   By default, the My Reports page will be displayed.
4. Click **Store** on the top-left.

   A list of pre-built reports will be displayed.

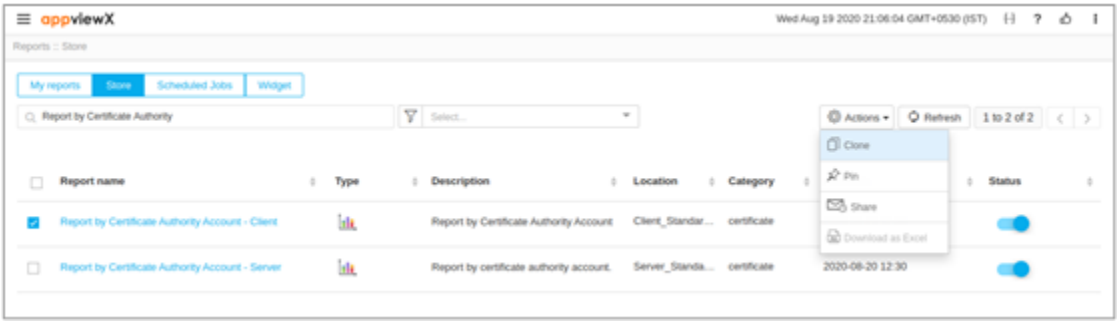
5. You can search for reports and filter reports by category.



Clone a Pre-built Report

To clone a pre-built report,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.



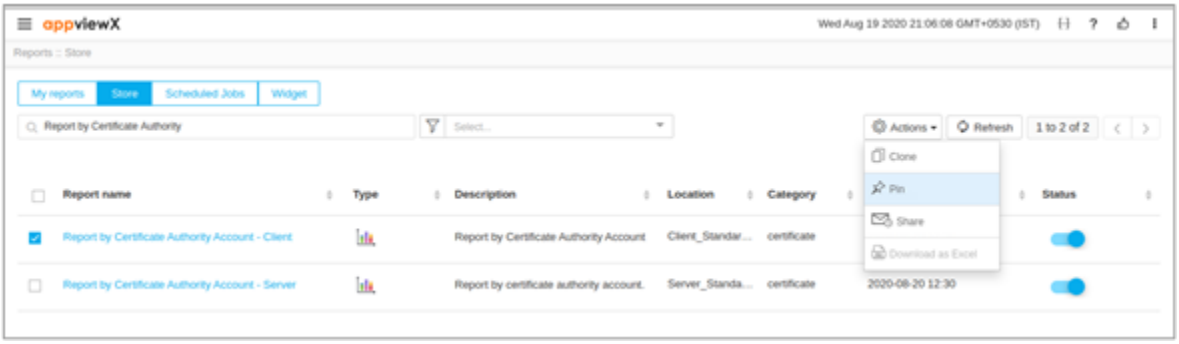
The cloned reports will be displayed under the **Store** tab.

Note: By default, store/pre-built reports are enabled. You cannot disable or delete it.

Pin a Pre-built Report

To pin a pre-built report,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu >> Studio >> Reports**.
3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to the Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.



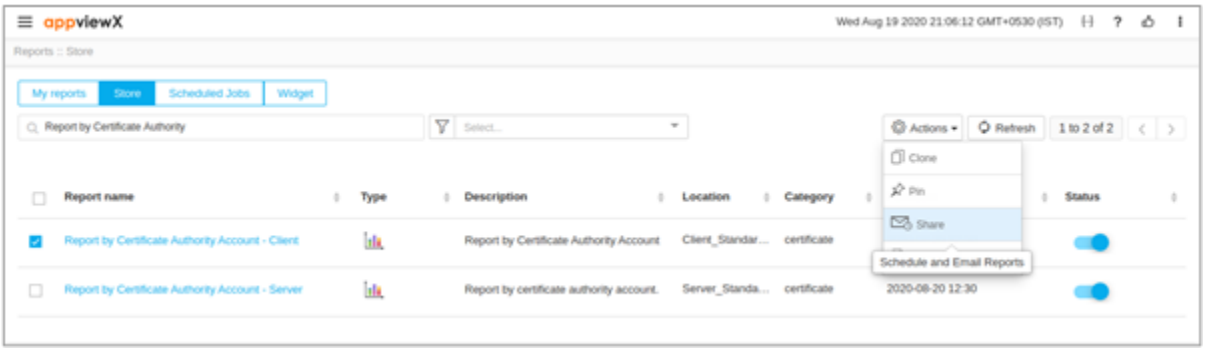
6. Click **Save**.

   The pinned reports will be displayed in the dashboard.

Share a Pre-built Report

To share a pre-built report,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the Store tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.
5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.
6. Click **Save**.



Widget

Widget reports are useful when an operator creates their widget based on the business needs. These widgets display the count of a specific operation that is executed and pending in the system. To know more about **Widget**, refer below.

- View Custom Reports
- Create a New Widget
- Clone a Widget
- Delete a Widget
- Pin a Widget
- Share a Widget

View Custom Reports

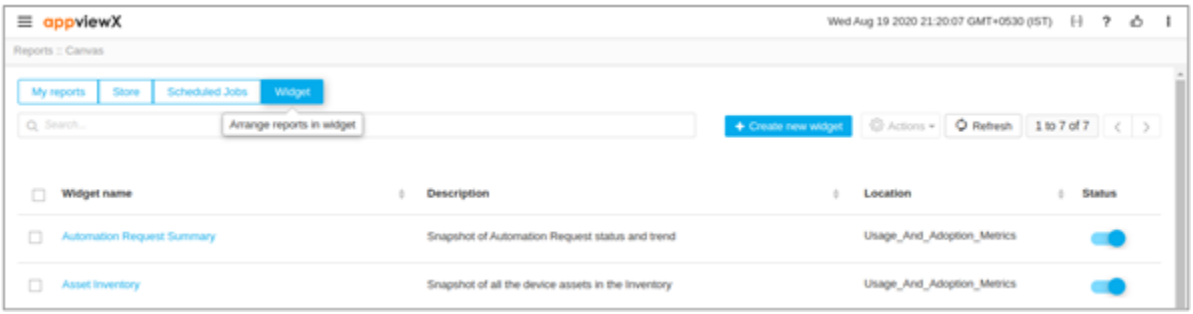
To view custom reports,

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

   The left navigation pane appears.
3. Click **Studio > Reports**.

   By default, **the My Reports** page will be displayed.
4. Click **Widget** on the top-left.

   A list of custom reports with the Widget Name, Description, Location, and Status will be displayed.
5. You can search for reports and filter reports by category.

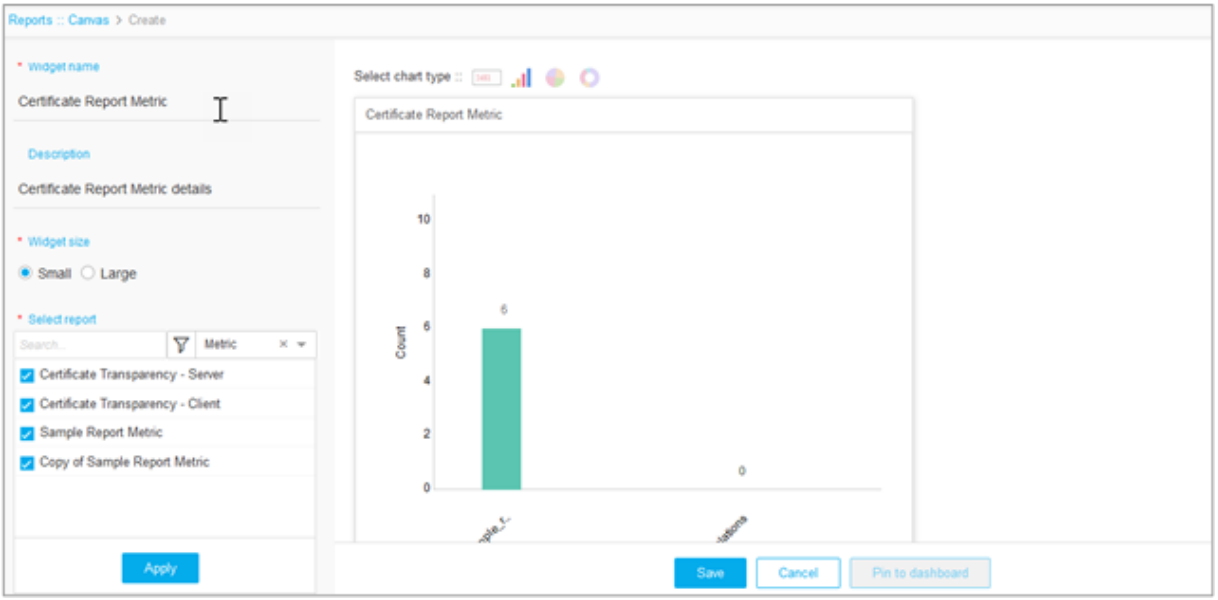


Create a New Widget

To create a new widget,

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

   By default, **the My Reports** page will be displayed.
3. Click **Widget** on the top-left.
4. Click **+ Create New Widget** on the top-right.
5. On the **Create Widget** page, enter a **Widget Name** and **Description**.
6. Select the **Widget Size**: **Small** or **Large**.
7. Under **Select Report**, select a report from the list or search for specific reports.
8. Click **Apply**.
9. Select a **Chart Type**: **Metric**, **Bar**, **Pie** or **Donut**.
10. Click **Save**.
11. Click **Pin to Dashboard** to pin the widget to the existing or new dashboard.
12. To enable the widget status, click the **Status** icon on the top-right.



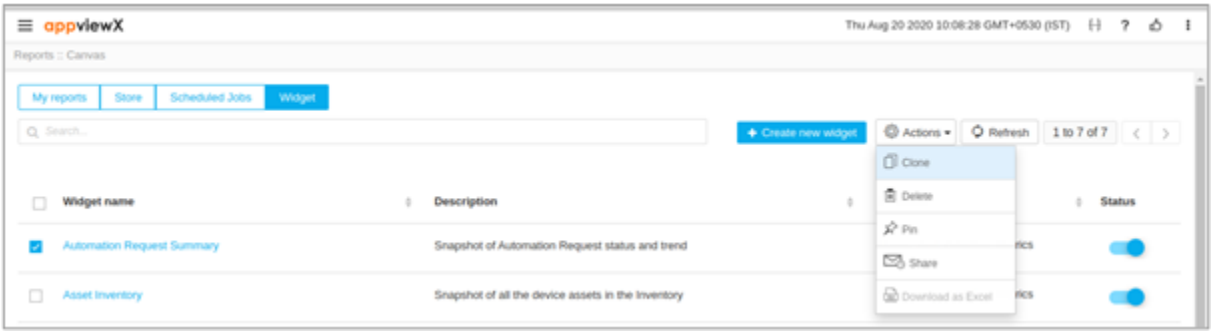
Clone a Widget

To clone a widget,

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

3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

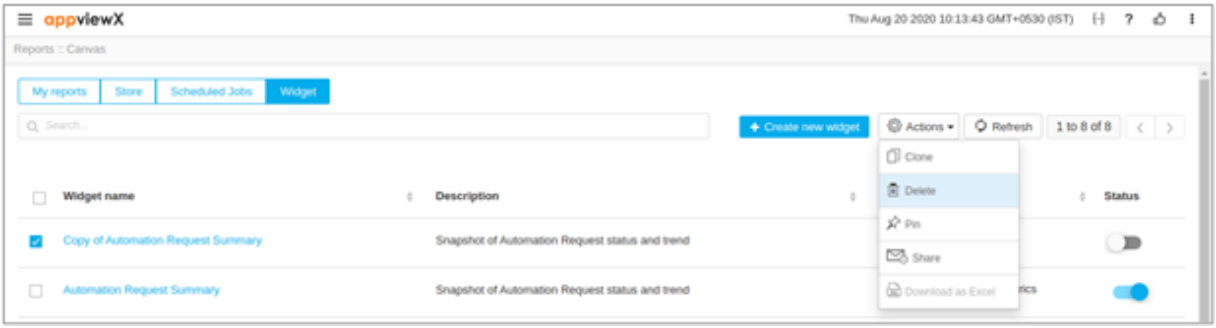
The Cloned reports will be displayed under the **Widget** tab.



Delete a Widget

To delete a widget,

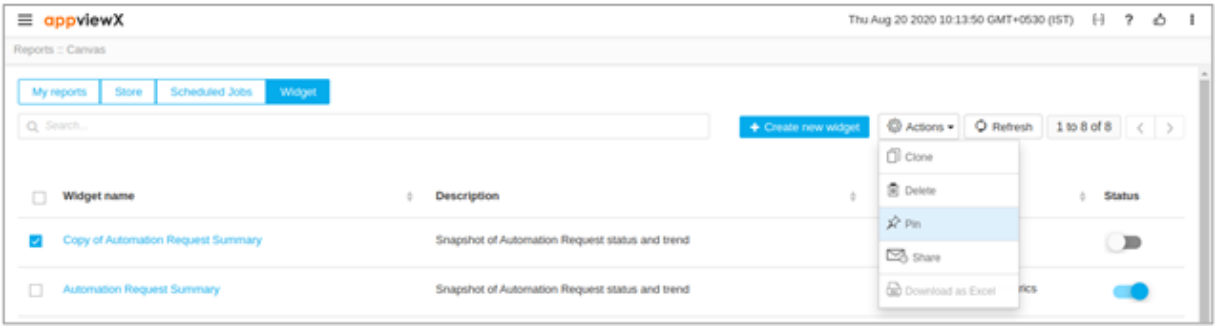
1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.



Pin a Widget

To pin a widget,

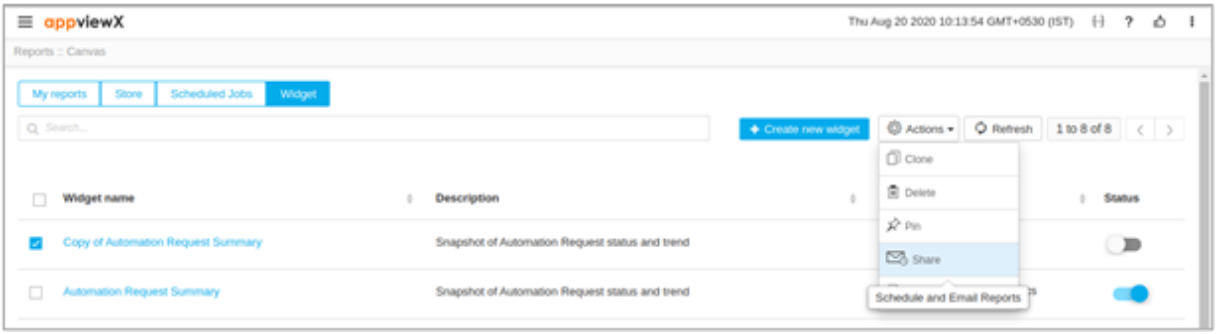
1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.



Share a Widget

To share a widget,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Studio > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.
5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.
6. Click **Save.**



Security Posture Determination and Interpretation

Security Posture Determination and Interpretation

Application security score reports, TLS, and Cipher suite reports allow you to identify the security level of service. To reduce security risks, change the application configuration to restrict the cipher suites and the TLS versions that are marked as LOW. Also for certain applications, OS upgrades will be applied to align with the security standard.

You can generate security reports through,

TLS Report

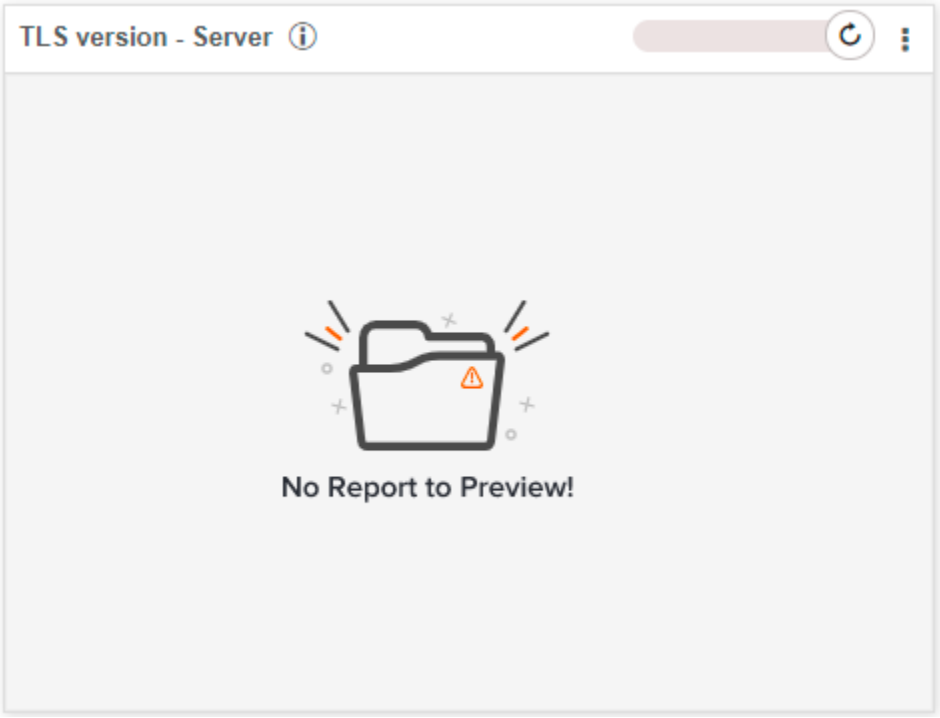
TLS report fetches data from SSL sessions and generates the report. It makes it easy for customers to check the protocol version of their servers based on this data. This report will generate data to identify vulnerable protocol versions. For example, in your infrastructure, there may be endpoints that still support TLSv1.0 and TLSv1.1 versions.

To view TLS version - Server reports,

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

   The left navigation pane appears.
3. Click **Dashboard**.
4. On the Dashboard list view, select Server Endpoint Security.

5. On the Server Endpoint Security dashboard, you can view the TLS version - Server report.



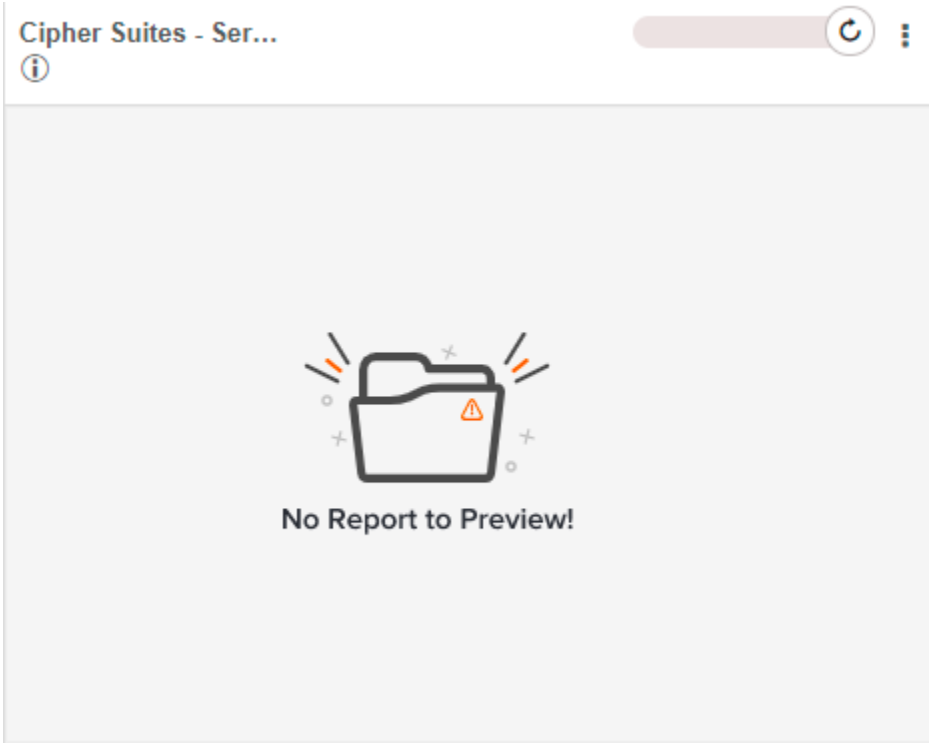
Cipher Suite Reports

Some ciphers use SHA1 that is still supported by servers. Cipher Report will discover servers that support these ciphers and provide data as per security standards. This report will generate data to identify vulnerable ciphers.

To view Cipher Suite - Server reports,

1. Log in to the AppViewX application with valid credentials.
2. Click the **Menu** > **Dashboard**.
3. On the Dashboard list view, select Server Endpoint Security.

4. On the Server Endpoint Security dashboard, you can view the Cipher Suite - Server report.



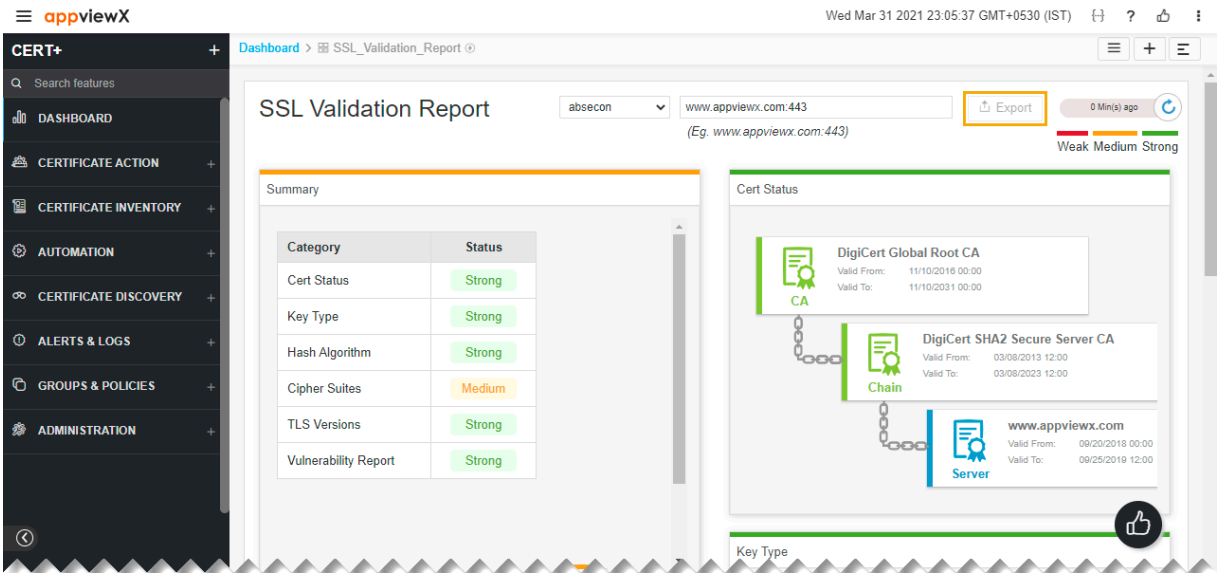
Application Score Reports

The application score report provides security scores of certificate parameters based on industry standards. You can get the score based on parameters such as Cert Status, Key Type, Hash Algorithm, CAA Record, TLS Version, and Vulnerability. Also, you can search for domains and check the security score. For example, you can check if the certificate name is valid through this report.

To generate application score reports,

1. Log in to the AppViewX application with valid credentials.
2. Click the **Menu** > **Dashboard**.
3. On the Dashboard list view, select the SSL Validation Report.
4. Choose a data center from the Data Center dropdown.
5. On the search bar, enter a domain name (www.appviewx.com:443) and click Enter.
6. The report is generated with the summary and all required parameters.

7. To export this report as a PDF, click the Export icon on the top-right.



Chapter 7: Alerts and Logs

Overview

CERT+ allows you to monitor the AppViewX component level and certificate-related alerts in a dashboard with predefined filters. Also, you can configure alerts based on your business needs. With these alerts, you can trigger an email with the necessary information. To run a custom logic based on the alert condition, you can configure it through a visual workflow in AppViewX. Alerts and logs help you to ensure the system performance is monitored.

You can view logs and receive certificate alerts through,

- Certificate Logs
- Certificate Alerts

Certificate Alerts

Certificate Alerts helps you with alerts that are related to certificates. You can configure these alerts based on certificate events such as sync, validation, or expiry. Any certificate-related actions performed in your application are captured as logs. Also, you can notify users of a specific certificate action through these alerts.

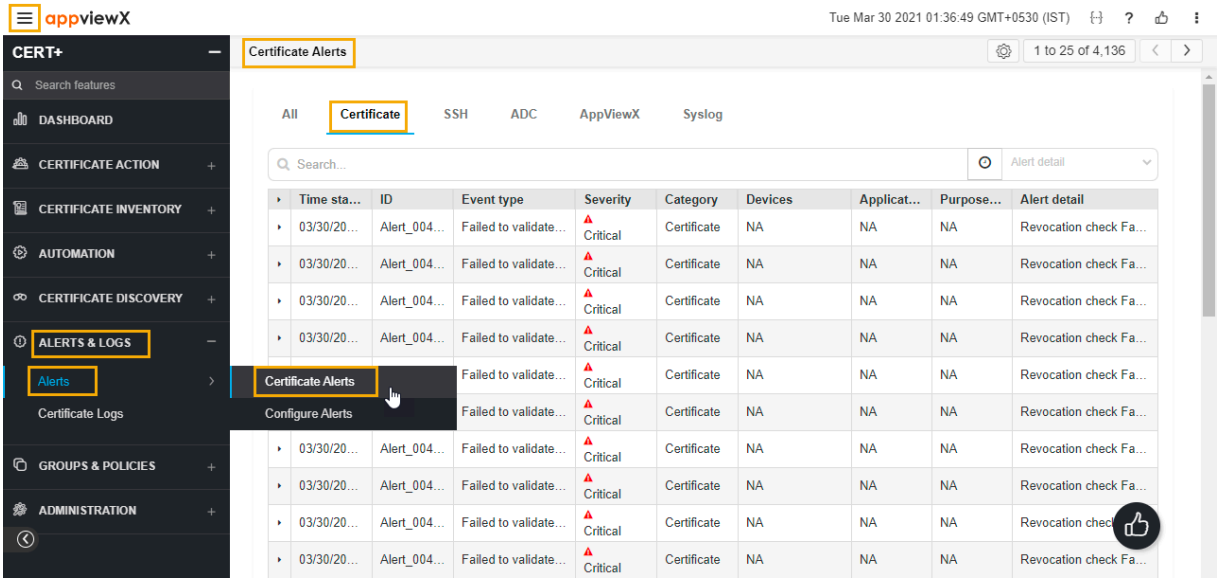
To verify certificate alerts,

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

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

   The **CERT+** left navigation pane appears.
4. Expand **ALERTS & LOGS**.
5. Click **Alerts**, and then select **Certificate Alerts**.

   The **Certificate Alerts** screen appears.



6. On the Certificate Alerts list view page, you can find the list of alerts related to the certificates. Any actions performed on the certificates are captured under this list view.
7. You can search for alerts based on the Alert ID, Alert Event type, Severity, Category, Devices, Applications, and Alert detail.
8. On the alert screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

Configuring a Certificate Expiry Alert

Certificate expiry alerts are sent to designated recipients for all certificates that are set to expire on the date specified on the Settings: Certificate expiry alert screen.

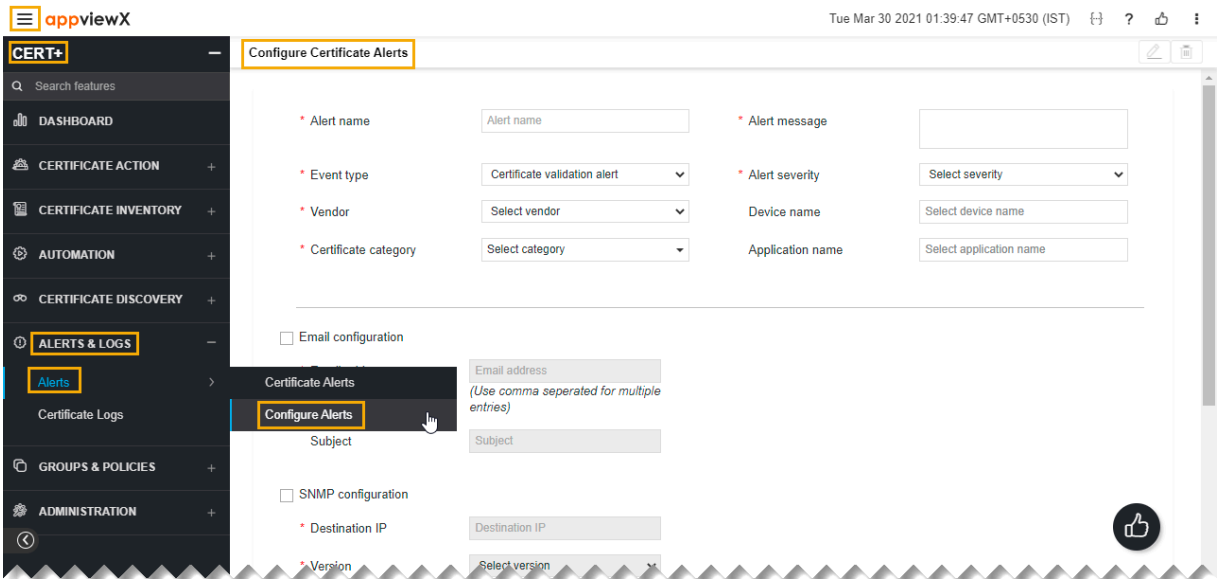
To create a certificate expiry alert,

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

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

   The **CERT+** left navigation pane appears.
4. Expand **ALERTS & LOGS**.
5. Hover on **Alerts**, and then select **Configure Alerts**.

   The **Configure Certificate Alerts** screen appears.



6. Enter a name for the certificate alert.
7. In the Event Type field, select Certificate Expiry Alert.
8. Select Critical as the severity of the alert.
9. In the Expires in (days) field, enter the number of days before a certificate expires. An alert will be sent out.
10. To use Email Configuration to send the alert, complete the following steps:

- Select the Email Configuration checkbox.
- In the Email Address field, enter the email addresses you want to send the alert to. Use commas to separate the addresses.
- In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.

11. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
    - Enter the Destination IP for the alert.
    - Select the version of SNMP you want to use: V1 or V2.
    - Enter the port that should be used for the alert.
12. Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
13. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Sync Alert

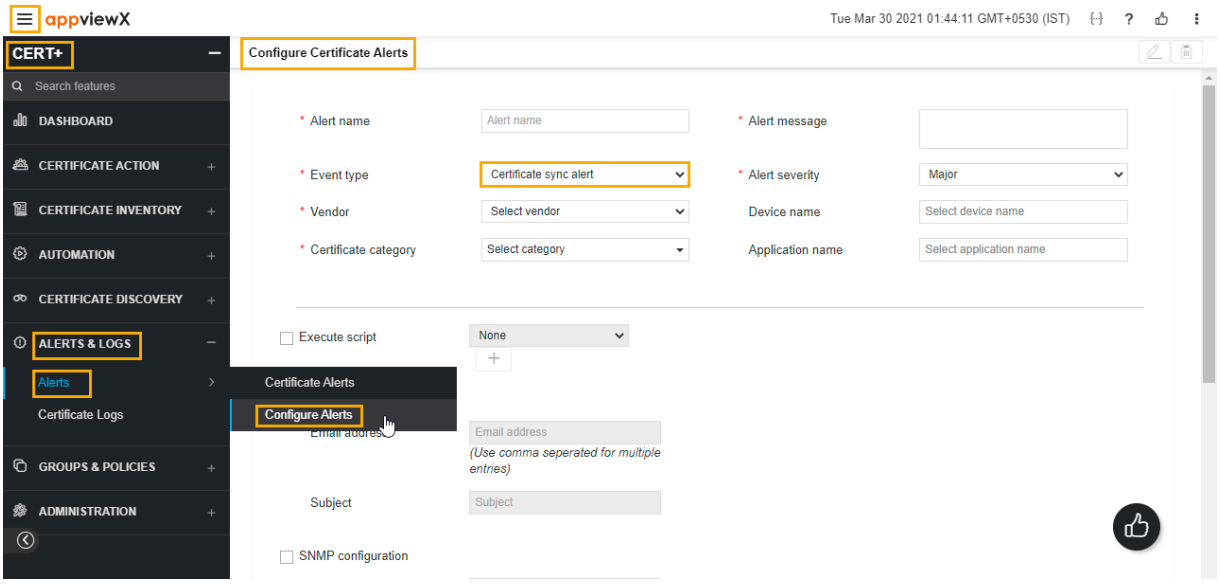
To create a certificate sync alert,

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

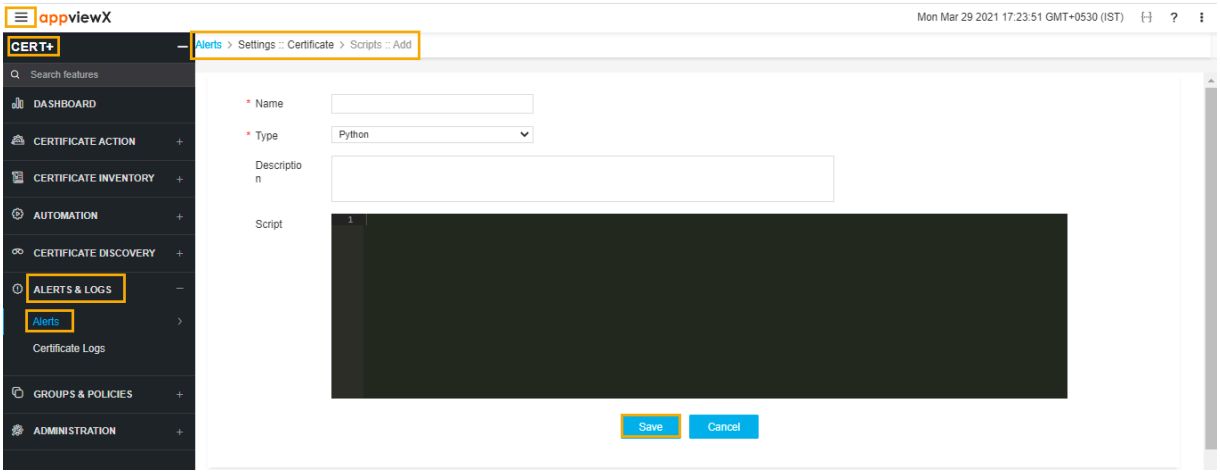
   The left navigation pane appears.
3. Click **CERT+**.

   The CERT+ left navigation pane appears.
4. Expand **ALERTS & LOGS**.
5. Hover on **Alerts**, and then select **Configure Alerts**.

   The **Configure Certificate Alerts** screen appears.



6. In the Event Type field, select Certificate Sync Alert.
7. Enter a name for the certificate alert.
8. Select the Alert severity of the alert: Critical, Major, and Notification.
9. In the Alert Message field, enter the text that users see when the alert appears on the screen.
10. Select the Vendor whose device or application you are creating an alert for.
11. In the Device Name field, select the device associated with the certificate you are creating an alert for.
12. In the Application field, select the application associated with the certificate you are creating an alert for.
13. Select the Execute Script checkbox.
14. In the Execute Script dropdown list, select the script to trigger the alert. To create a script, click the (Add new script) icon. The below page appears.



- Provide value in the Name field.
- Type by default is selected as Python.
- Provide description value in the Description field.
- Enter the script to be executed in the Script field and click **Save**.

15. To use the Email Configuration to send the alert, complete the following steps:
    - Select the Email Configuration checkbox.
    - In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.
    - In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.
16. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
    - Enter the Destination IP for the alert.
    - Select the version of SNMP you want to use: V1 or V2.
    - Enter the port that should be used for the alert.
    - Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
17. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Validation Alert

To create a certificate validation alert,

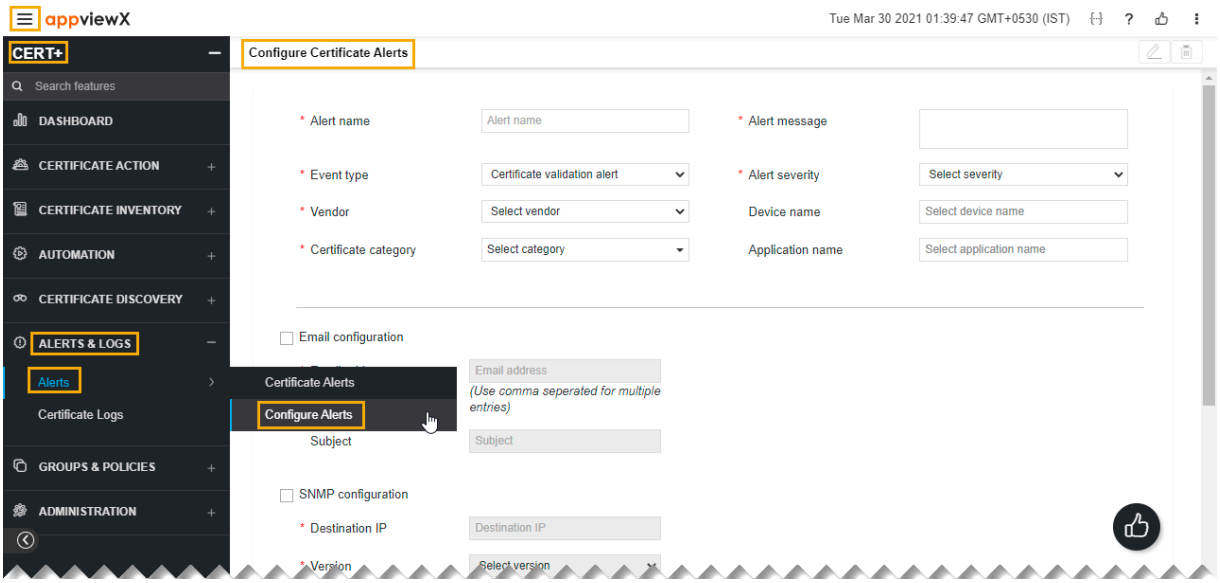
1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

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

The CERT+ left navigation pane appears.

4. Expand **ALERTS & LOGS**.
5. Hover on **Alerts**, and then select **Configure Alerts**.

   The **Configure Certificate Alerts** screen appears.



6. In the Event Type field, select Certificate Validation Alert.
7. Enter a name for the certificate alert.
8. Select the severity of the alert: Critical, Major, or Notification.
9. In the Alert Message field, enter the text that users see when the alert appears on the screen.
10. Select the Vendor whose device or application you are creating an alert for.
11. In the Device Name field, select the device associated with the certificate you are creating an alert for.
12. In the Application field, select the application associated with the certificate you are creating an alert for.
13. To use the Email Configuration to send the alert, complete the following steps:

    • Select the Email Configuration checkbox.

    • In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.

    • In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.

14. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:

- Enter the Destination IP for the alert.
- Select the **version** of SNMP you want to use: V1 or V2.
- Enter the port that should be used for the alert.
- Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.

15. Click **Add** to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Connection Failure Alert

When a certificate is enrolled with AppViewX, a connection is established between the Certificate Authority (CA) signing the certificate. This connection is vital to perform CLM actions and certificate discovery tasks seamlessly.

When you can check manually if the connection is successfully established between AppViewX and certificate authority, and continues to stay so, starting version 2021.1.0, AppViewX allows you to configure automatic alerts when this connection fails. These alerts will be recorded in AppViewX logs as well as sent as email notifications.

To configure a connection failure alert:

1. Login 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 **ALERTS & LOGS**.
5. Click **Alerts** and then **Configure Alerts**.

   The **Configure Alerts** page is displayed.
6. Enter an **Alert name**.
7. Enter the **Alert message** that will be entered in the logs and sent as the email message body.
8. From the **Event type** dropdown list, select **Certificate authority connection alert**.
9. Set the **Alert severity** to critical.

10. Select the certificate **Vendor** name.
11. Select the **Certificate category**.
12. To configure email alerts, in the **Email configuration** section, enter the **Email address** that will receive the email notifications in the event of a connection failure.
13. To use the Simple Network Management Protocol (SNMP) for sending the alerts:
    a. Enter the **Destination IP** address for the alert.
    b. Select the SNMP **version** to be used.
    c. Enter the **Port** number to be used for the alert.
    d. Enter the **Community string** for the alert.

    The string is similar to a user ID or password and allows users to access the requested information on the device.
14. Click **Add** to create the alert.

The new alert is now listed in the **Certificate Alerts** page.

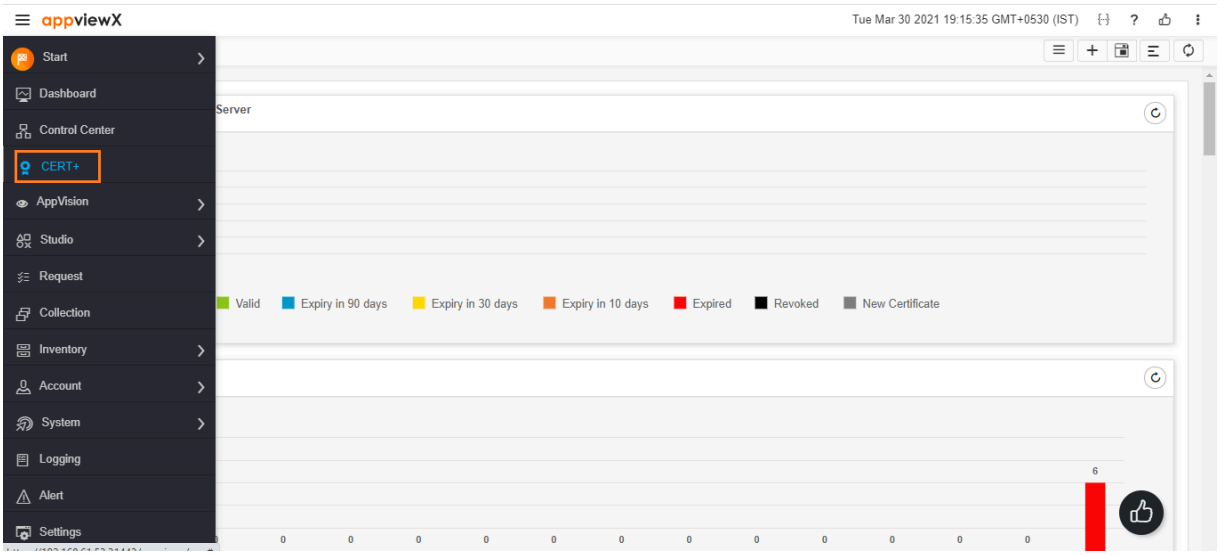
Certificate Logs

Logs keep track of all activities that take place within AppViewX or any external entity that is connected to the AppViewX system. The Logging functionality in AppViewX tracks user activities and creates the device and object-level event logs. Certificate Logs helps you with logs that are related to certificates. Any system or certificate-related actions performed in the application are captured as logs. With these logs, you can check the system performance and it helps you with audit purposes to meet industry standards.

To check logs,

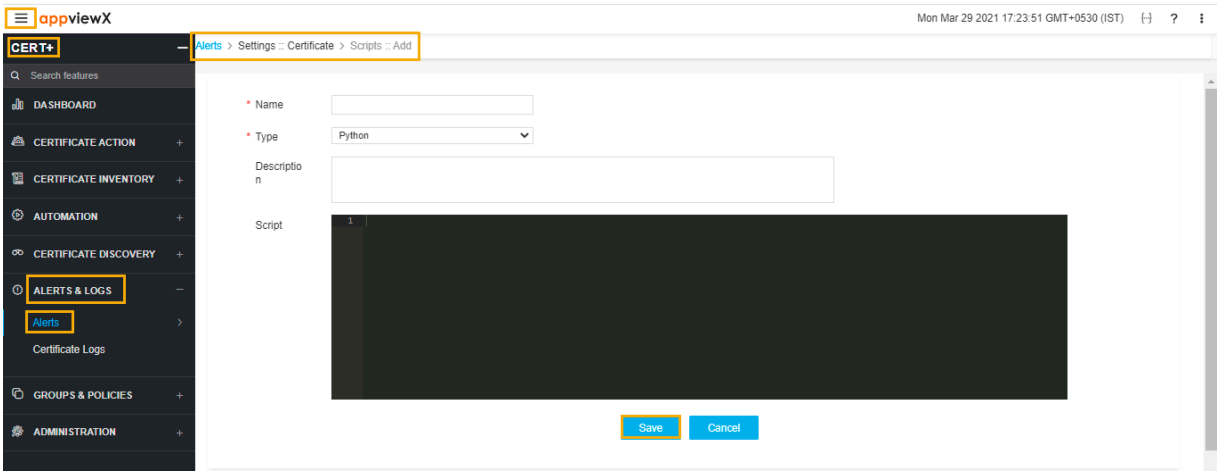
1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

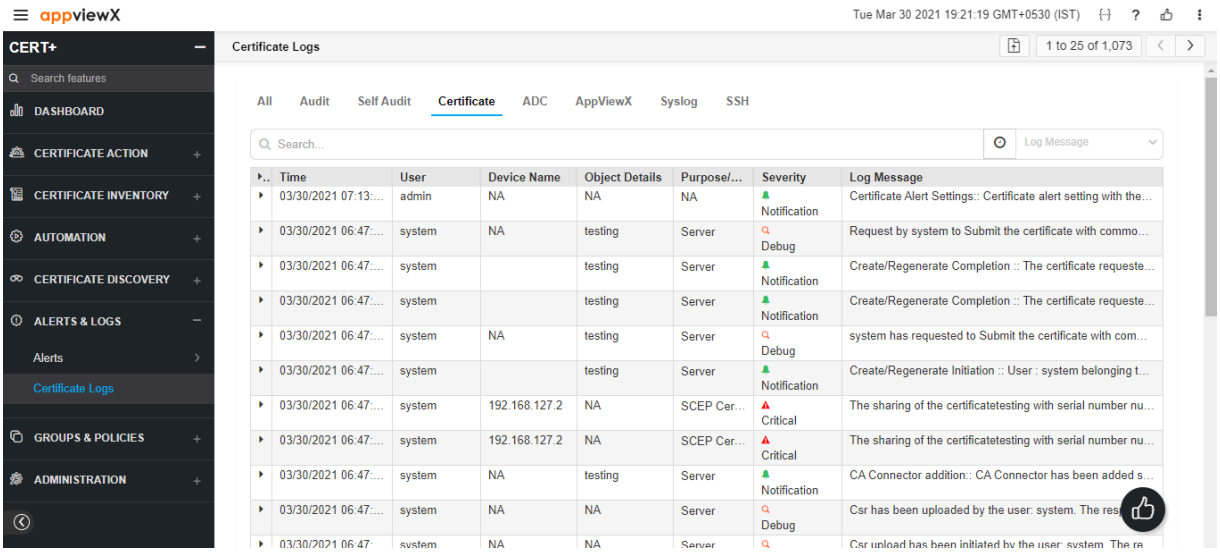


3. Click **CERT+**.

   The CERT+ left navigation pane appears Logging



4. Under the section Alerts & Logs, select Certificate Logs. The following page appears



5. On the Certificate logs list view page, you can find the list of logs related to the certificates. Any actions performed on the certificates are captured under this list view.
6. You can search for logs based on the time, user, device name, object details, and severity.
7. You can also filter logs based on the date and time and through the Log Message filter.
8. On the log screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

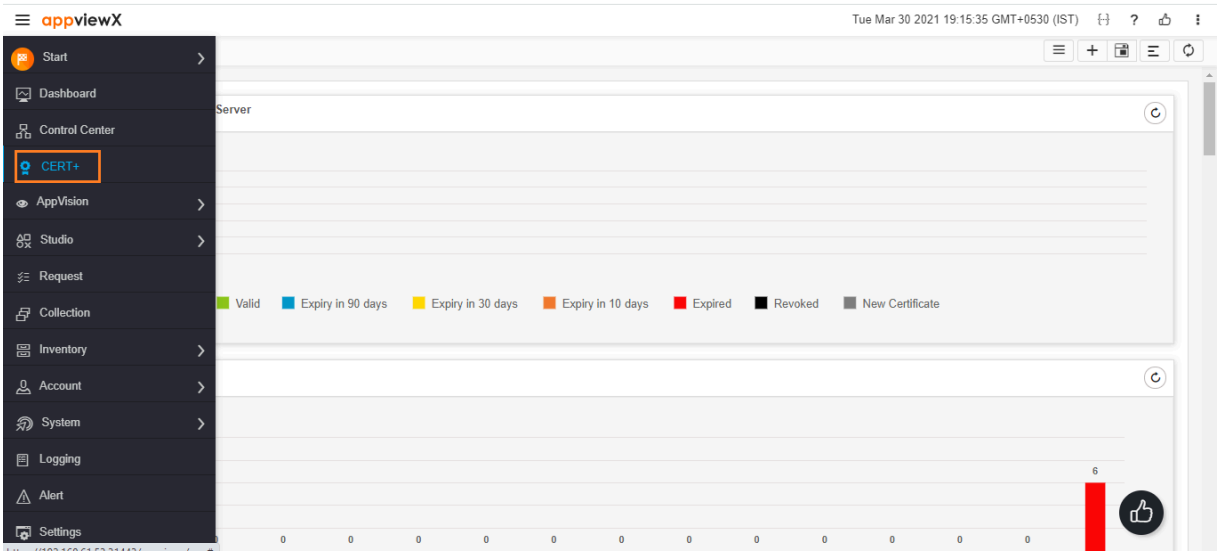
Export Certificates Logs

When exporting logs in AppViewX, you can export all of the logs of a given type-for example, all Configure files or all Audit files-or you can search for specific logs or filter the default log list using the Date Range and Log Detail fields and then export only the logs that remain.

To export a logging report,

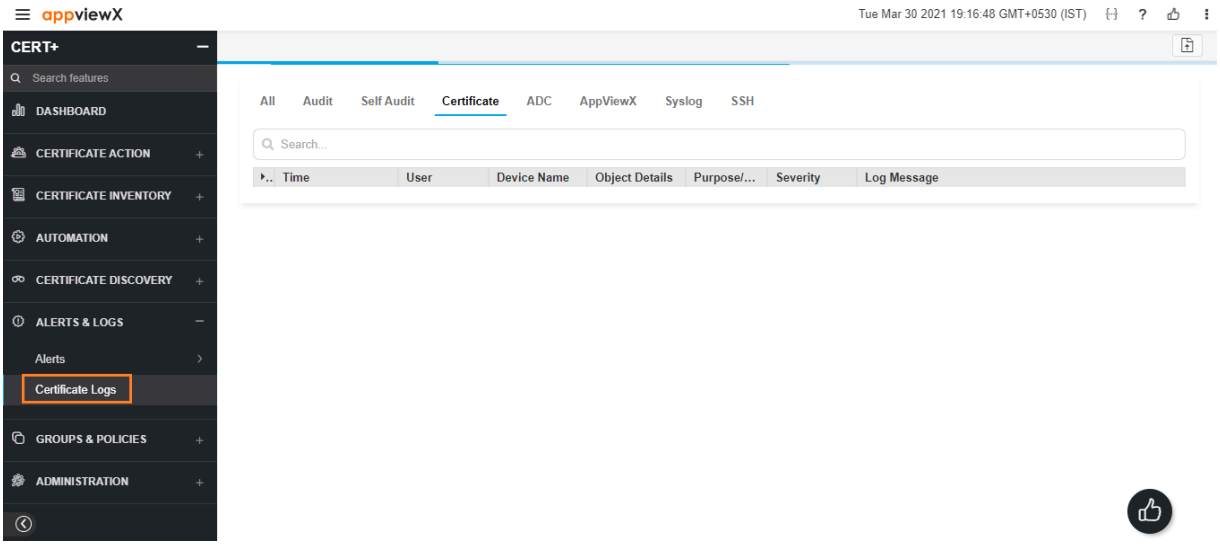
1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.

   The left navigation pane appears.



3. Click **CERT+**.

   The CERT+ left navigation pane appears Logging.



4. At the top of the Logging screen, click the tab for the type of logs you want to export: Certificate (in this case).
5. (Optional) Run a search for specific logs or filter the default list using the Date Range and/or Log Detail fields in the Search bar.
6. Click the export button in the Command bar in the top-right corner of the page.
7. The log report is then downloaded as a tar.gz file.

Chapter 8: Standard Practices

PKI Standard Practices

Offline Root CA

- The root CA should never be connected to the network or to the domain and no fingerprint of the server should ever be recorded since the root key compromise will impact the entire PKI hierarchy.
- Root CAs should always stay offline and shut down except when signing the Issuing CA certificates and during root CRL publish.
- Access to the Root CA to sign the Issuing CA request should be initiated in an agreed and controlled workflow so as to not compromise the Root CA in any means.
- Once the Issuing CA certificate has been issued and Root CRL published the Root CA should be turned off.
- Ensure to publish a reasonably short-lived Root CA CRL, the recommendations from NIST is to have the Root CA CRL published for 1 year and ensure to renew the CRL before expiry.
- We strongly recommend that all your CA keys be stored securely in a FIPS 140-2 Hardware Security Module (HSM).
- Protect the server during boot using Bitlocker or any other encryption system of choice and ensure to backup CA private key, CA registry Key, the CA database, and the CA certificate.
- Ensure to enable an audit event to track all actions performed on the Root CA.

Inline with Compliance

- Ensure to have a CP and CPS created to suit the organization's needs and ensure the PKI infrastructure meets all standards and requirements with respect to the CP and CPS.
- Any changes or addition of features ensure to capture in the CP and CPS documents.
- Ensure to renew the CA certificates(Root and Subordinate) within half its lifecycle.
- Enterprise key and certificate security policies should align with the latest regulatory, industry-standard recommendations, and guidelines such as key storage, secure communication protocols (TLSv1.2), cryptographic algorithms (RSA-2048), and hashing algorithms (SHA-2).
- Enterprise security architects should constantly monitor security standard recommendations and periodically update the enterprise's security policy.
- Ensure all security events are audited and a periodic security audit is performed to validate the security adherences and metrics.
- Encourage short-lived certificates for all key usages.

CSR Generation Standardization

- A process must be defined across the enterprise to generate CSR that aligns with the security standards and to store keys securely.
- Harden parameters such as Country and Organisation in accordance with organizational requirements.
- Access to keys should be restricted to authorized personnel.
- Key Generation, Certificate Request, and Approval processes should be well defined.

Archival

Signing keys do not require archival. We can always generate new keys for signing since the signed data is not encrypted. But encryption keys have to be archived so that the encrypted files during the certificate validity can be decrypted even after the certificate expiry. Also, this is recommended for security audits.

Secure Storage of Keys

- It is recommended to store private keys in HSM.
- Ensure respective certificate owners or certificate authorized administrators are granted access to private keys using the RBAC solution.
- Best practices training can be provided to certificate users and administrators to keep private keys secure.

Compromised CA/CA keys

- Ensure to discover a compromise as quickly as possible by implementing tracking and detection mechanisms and performing regular manual operational sanity checks.
- Establish well-defined communications plans for informing subjects, relying parties, and other stakeholders with sufficient details about the type of compromise so these parties can implement the appropriate remedial actions.
- If a CA system or signing key compromise occurs, the organization should perform the following steps:
  - Ensure that certificates issued to the organization’s systems or users from the compromised CA are revoked.
  - Notify all owners of the affected certificates about the CA compromise and establish a point of contact for responding to questions and providing guidance and instructions.
  - Replace all certificates from the compromised CA with new certificates from a different CA effective immediately.
  - Ensure that all relying parties have the certificate trust chains required to validate certificates from the new CA.
  - Ensure that revocation checking is enabled on all relying party systems.
- If the compromised CA is a root CA, the root certificate must be removed from all trust stores and relying on party systems.

Compromised Certificate Handling

- Ensured to be prepared to respond in a timely manner in case of a CA or end-entity certificate compromise and have a plan or workflow to replace all affected certificates or the trust chain.
- In the event of a key or certificate compromise, a fresh key pair should be generated on a secured system. The compromised item should be revoked and taken out of the service as soon as the systems are secured.
- If you are not sure of your private key possession, report it to your CA and suspend the key immediately. Once you find the key is secure, reinstate the certificate.

CA Compromise and Remediation Matrix

S/No.	Issue Type	Revoke compromised/ counterfeit certificates	Revoke CA certificate	Replace all certs issued	Remove/Revoke Root certificate
1	Impersonation	Yes	NA	NA	NA
2	RA compromise	Yes	NA	NA	NA
3	CA system compromise	NA	Yes	Yes	Yes
4	CA key compromise	NA	Yes	Yes	NA
5	Root CA compromise	NA	NA	Yes	Yes

CLM - Best Practices

Risks Involved in an Enterprise without CLM and their Solutions

S/No	Risks Involved in an Enterprise without CLM	Solutions
1	No centralized management for all certificates in an enterprise and to know the certificate's location.	Different modes to discover existing certificates along with the discovery source.

S/No	Risks Involved in an Enterprise without CLM	Solutions
2	Enforcing teams to follow the enterprise security standards.	• Get information about all certificates within an enterprise. • Run a validation for the existing certificate against the organization's security standard.
3	Poor monitoring of certificate validity causes outages due to expired certificates.	• Continuous monitoring of the certificate status and notifications. • Automated renewals and provisioning should be available.
4	Control over the generation of keys.	Provide a mode of access to teams to access and generate certificates for their requirements.

- Create a certificate lifecycle management action plan
- Start automating the certificate management process wherever feasible.
- Identify and expose all the neglected certificates, these are the certificates that will cause more damage during expiry.
- Ensure proper RBAC controls and avoid using direct user accounts and instead use identified admin accounts for access and control.
- Enable notifications and alerts to ensure timely renewal.
- Schedule scans to run overnight or after business hours.

Standard Practices followed in the Certificate Inventory Management

- Certificate Group
- Access Control
- Recommended Columns to View in the Default Inventory

Certificate Group

- Group similar certificates into logical groups
- Groups can be based on business units or teams using certificates
- Provide group owner details during configuration for easy tracking
- Create hierarchy-based grouping to leverage alert escalation on OOB workflow.
- Try and maintain the same policy across a hierarchy of groups. It is also allowed to set a different policy for each hierarchy.

The best way to manage certificates is to group certificates based on the following:

- AD Security Group vs Department
- Test vs Production
- Internal vs External Hierarchy
- Auto-renew vs Approved CSRs
- Auto Push Updated Certificate vs Controlled Push Updated Certificate

Access Control

Based on certificate groups, you can create resources and map devices/applications.

Identify various authorization roles that have to be created. Find the list of roles below:

- Certificate Administrator Team
- CERT Owner/Requester
- Approver
- Certificate Manager
- Inventory View

The certificate admin team should be granted access to view the entire certificate inventory and end-users should be able to view their respective certificates.

All managed/monitored certificates should be available on a single window for tracking and visibility. The product provides various columns that have rich information that might not be needed in all scenarios.

Recommended Columns to View in the Default Inventory

- Subject Distinguished Name (DN)
- Subject Alternative Names (SANs)
- Issue Date (not Before date)
- Expiry Date (not After date)
- Issuing Certificate Authority
- Key Length
- Key Algorithm (RSA, ECDSA)
- Signing Algorithm
- Validity Period (From the not Before date/time to the not After date/time)
- Installed location(s) of a certificate (IP or DNS address and file path)
- Certificate Owner (The group responsible for the certificate)
- Contacts (The group of individuals is notified of issues)
- Approver(s) (parties responsible for reviewing issuance and renewal requests)

As the inventory is a RegEx-based search engine, users can search for a certificate based on any parameter with various filters.

Securing CERT+

CERT+ Certificate Lifecycle Management (CLM) offers capabilities to discover and manage certificates on devices and self-service certificate enrollment for users. Cert+ also acts as a Key Escrow for keys discovered and enrolled.

Typically, the private keys are stored by the devices handling SSL termination, and an SSL management tool retrieves them during certificate renewal. The tools and devices store them in their storage in the

original format, which can be reused. If there is an attack on the device or tool storage, the private keys will be given away, which can be used to host an array of attacks.

AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using the AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key.

Thus, even if the hackers get the database, they will not be able to get the private keys. Only a maze of jumbled up characters will be visible to them, which does not make any sense and hence, rendering the attack useless.

Chapter 9: 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 smart phones, 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

Terms	Definition
	that need to acquire client certificates and associated certificate authority (CA) certificates. **EST** is described in RFC 7030
SCEP	Simple Certificate Enrollment Protocol (SCEP) is an IETF RFC. This enables network user to request their digital certificate electronically and as simply as possible. Supported by most of the network devices.
SSL/TLS Certificates	SSL refers to Secure Sockets Layer whereas TLS refers to Transport Layer Security. Both are cryptographic protocols providing secure data communication in a network.