appviewx

PKI+ User Guide

Version: 2023.1.0 FP2

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
1.0	Release of AppViewX_v2023.1.0 FP1 PKI+	Nov 2023

About this Guide

This guide explains the capabilities of AppViewX PKI+. This guide provides step-by-step instructions to configure and manage AppViewX PKI+.

Audience

This guide is intended for PKI Security, DevOps, 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: Introduction

AppViewX's PKI+ provides a ready-to-use PKI and a full-fledged PKI automation system that enables enterprises to scale at will. AppViewX makes it possible for you to enjoy all the benefits of a highly reliable, HSM-backed, and automated PKI system without having to worry about heavy investments into infrastructure and maintenance. The pay-as-you-go model offers you to choose the level of security, assurance, type of policies based on their needs as AppViewX's PKI+ is customizable, deployable, flexible, scalable, and is compliant with the best practices of PKI.

Chapter 2: System Requirements

Overview

This section details the hardware, operating system, and browser requirements.

Hardware Requirements

Ensure that you have, at minimum, the following hardware with the given specifications before proceeding with the installation:

- **Single Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Single node	8	32GB	500GB

- **Multi-Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Multi-node (master node)	4	4GB	100GB
Note: One node for a single master installation and a minimum of three nodes for multi-master installation.			
Multi-node (worker node)	8	32GB	500GB

- **Platform Bare Minimum Requirements**

Supported Virtualization Platforms	Versions	vCPU	RAM	HDD
VM Server, VMware ESXi	5.5 or later	8v	32GB	1TB

Operating System Requirements

Both single node and multi-node installations of AppViewX are supported on the following operating systems:

- RHEL 8.5
- RHEL 8.6
- RHEL 8.7
- Ubuntu 20.04

Browser Requirements

Following is the browser requirements to use the AppViewX CERT+ node:

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

Chapter 3: What is Certificate Authority

Overview

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

The CA signs the certificates, and the signature is verified by a client before establishing a connection with the organization's server. CAs are tasked with the domain control verification (DCV) process and for verifying the public key that the certificate is issued for belongs to the subject that requests it. The format of these certificates is specified by the x.509 or EMV standard.

There are two types of certificate authorities:

- **Public CA:** A public CA is a third-party entity that issues certificates for a fee after doing the necessary checks on the organization requesting a certificate. The checks, by default, include domain validation. Third-party CAs have their own public-private key pairs with which they sign the certificates. Most of the well-known CAs are recognized by servers and clients; therefore, certificates signed by them are immediately validated by the entity initiating a secure connection. Publicly-signed certificates offer a higher level of assurance since they are issued by a recognized CA, and are generally used for securing websites and other endpoints involving direct user interaction.
- **Private CA:** A private CA is when an organization creates its own CA hierarchy and issues certificates for its internal network where discretion is required. This may include VPNs, sensitive databases, secure mail servers among others.

How Certificate Authority Works

Certificate authorities are an integral part of public key infrastructure (PKI). The underlying purpose of any PKI setup is to manage the keys and the certificates associated with it, thereby creating a highly secure network environment for use by applications and hardware.

Depending on your organization's needs, you can go to the website of your preferred CA and choose a certificate that best suits your needs from the options listed. The next step would be to generate a certificate signing request (CSR). Once that is submitted, the CA will contact the owners of the domains that the certificate has been requested for and take the necessary verification steps.

AppViewX PKIaaS Certificate Authority

AppViewX's PKI+ combines the convenience of a customized PKI with our powerful certificate lifecycle automation capabilities, and allows you to consume the entire solution as a service. Setting up a secure, scalable, and compliant PKI has never been easier.

- PKIaaS Management Overview

PKIaaS Management Overview

Before you Begin

1. Select the data center to establish connection with PKIaaS using the **Settings** page. See Settings.
2. Onboard at least two custodians before creating CA hierarchy. You can complete the addition of custodians by going to **Menu > PKI+ > Custodian Management.**

> **Note:** No CA action is possible until at least two active custodians are in the system.

From the PKI+ menu, you can access:

- **Get Started:** Use this page to configure SMTP server, onboard custodians, create PKI CA, and set up Cloud Connector to enable connectivity to the Enterprise's private network.
- **Dashboard:** This page gives a quick summary of all the root and subordinate CAs created via AppViewX PKIaaS certificate authority.
- **CA Inventory:** Create root CAs and subordinate CAs and enroll them to the AppViewX PKIaaS certificate authority.
- **Custodian Management:** Custodians are responsible for approving any action performed in PKI+. You can add or delete custodians from this page.

  On completing custodian onboarding, you can add your root CAs and subordinate CAs to PKI+.
- **Settings:** Use this page to configure PKI+ settings.
- **Validation Authority:** Certificate authorities use Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) to obtain the revocation status of x.509 digital certificates.

- Getting Started with PKI+
- Dashboard
- Settings
- Custodian Management
- CA Inventory

- Validation Authority
- Validating Certificate Authority
- Certificate Group
- Certificate Authority Policy
- Certificate Enrollment
- Application Connector
- Pushing Certificate to Device

Getting Started with PKI+

You can use this page to:

1. **Configure Mail Server:** Configure SMTP mail server for Custodian Management by clicking the link provided on the Web page for instructions.
2. **Add custodians:** Add custodians for approving actions performing in PKI. See Onboarding Custodians.
3. **Create CAs:** Add root and subordinate CAs. See sections under CA Inventory.
4. **Set up Cloud Connector:** Enable connectivity with the Enterprise's private network by clicking the link provided on the Web page for instructions.

Dashboard

This page gives a quick summary of all the root and the intermediate CAs created via AppViewX PKIaaS.

The following widgets are displayed on this page:

- **CA Summary:** This widget displays the number of CAs created via AppViewX PKIaaS. This contains the root and intermediate CAs. Click the graph to redirect you to the CA inventory for the selected CAs.
- **CA by Status:** This widget displays the CA count based on the status in the CA inventory. Click the graph to redirect you to the CA inventory for the selected CAs.
- **CA Expiration:** This widget displays the CA count based on the expiry date. Click the graph to redirect you to the CA inventory for the selected CAs.

Settings

You can use this page to set the value for the data center, which is reflected on the AppViewX PKIaaS Certificate Authority page. You can also configure key ceremony administrators who can control the actions on the **Custodian Management** page.

1. Go to (**Menu**) icon **> PKI+ > Settings.**
   The **Settings** page appears.
2. Enter the fields as described in the table.

Fields for General Settings section

Field	Description
***Data Center**	Select a data center from the dropdown list to establish connection with PKIaaS.
***Default Region**	Select a region from the dropdown list.
Email IDs for PKI+ Alerts	Enter email IDs of users who can receive PKI+ alerts. You can add more than one user email ID using a comma (,) as a separator. The service connectivity and each CA status are monitored periodically. When there is a failure, an alert is triggered and an email is sent. Reach out to saashelp@appviewx.com for help. The maximum duration for which you can receive alerts is 30 days.
Key Ceremony Admins	Select two key ceremony admins. **Note:**

Field	Description
	• Only the default admins can add key ceremony admins. • If key ceremony admins are configured, only they can add/ delete custodians, but key ceremony admins cannot be added as custodians. • SSO users cannot be key ceremony admins.
Note: Fields marked with red asterisk (*) symbol are mandatory.	

3. Click **Save.**

What to do next:

Onboarding Custodians

Custodian Management

Custodians are responsible for approving any action performed in PKI+. Any admin can add custodians from the **Custodian Management** page if the key ceremony admins are not configured. The first custodian is auto-approved and the approval flow gets triggered from second custodian.

- Onboarding Custodians
- Deleting Custodians
- Filtering Custodians

Onboarding Custodians

Prerequisite

Configure SMTP mail server for Custodian Management by clicking the link provided on the **Getting Started with PKI+** Web page for instructions.

To onboard custodians:

1. Go to (**Menu**) icon **> PKI+ > Custodian Management.**
2. Enter the following fields:

Field Description for Custodian Management page

Field	Description
***Quorum Value**	By default, the quorum value is set to 51%. The quorum value represents the minimum number of approvals required to add or delete custodians and also to approve CA creation. For example: If there are three custodians, then the minimum approval required is rounded off to two. If there are six custodians, then the minimum approval required is four.
***Approval Link Validity**	By default, the approval link is valid for 30 minutes. Minimum value is 10 minutes while maximum value is 7 days.

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

3. Enter the following fields in the **Add Custodian** section:

Field Description for Add Custodian section

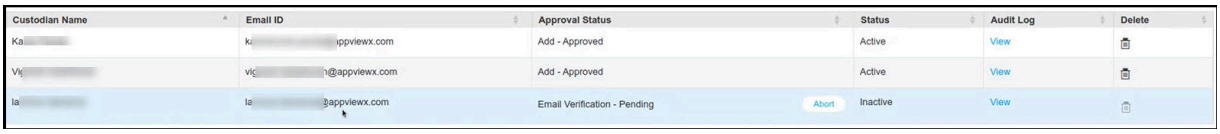
Field	Description
First Name	The first name of the custodian being added. Custodian must have login access to AppViewX.
Last Name	The last name of the custodian being added.
Email ID	The email address of the custodian to which the approval link and notification messages are sent.

4. Click **Save.**

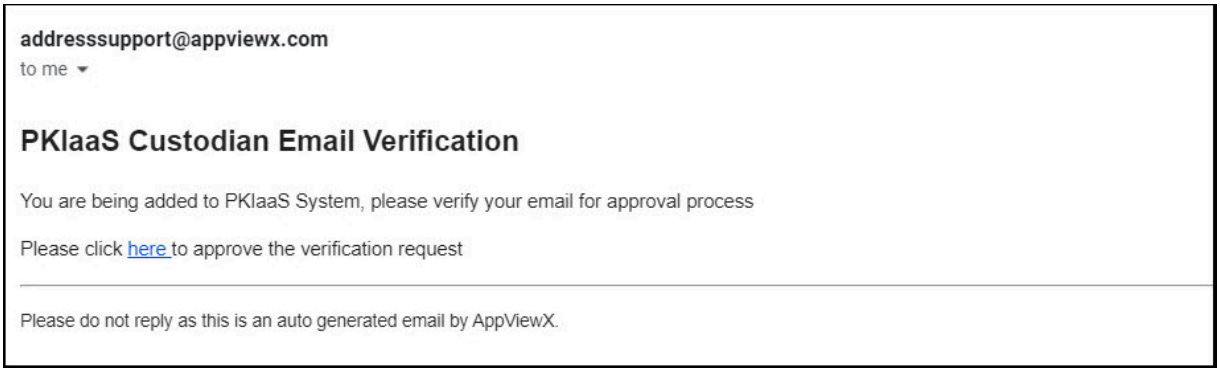
Note: If the custodian being added is not part of the AppViewX users, then the following confirmation screen appears. Click **Save and Continue** to proceed as an SSO user.

The first custodian is automatically approved.

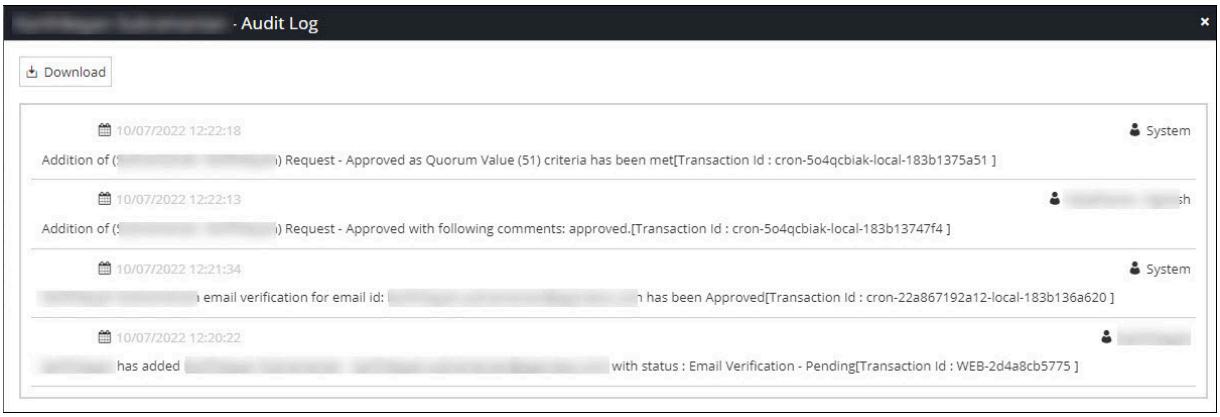
Details of the newly added custodian are populated in a table along with *Email Verification - Pending* approval status and *Inactive* status as shown. If you want to abort the action, click **Abort.** Any workflow triggered and in progress is killed from the Request page prior to triggering any further actions.



5. The requester receives a notification email. Click the **here** hyperlink to be directed to the AppViewX login page.



6. The requester must log into the application using their credentials and approve the request by going to **Menu > Requests > All requests.**
7. Enter the comments and click **Approve.**
8. Refresh the custodian table to see the approval status changed to *Add - Approval Pending* and the status as *Inactive.*
9. All active custodians (whose status are *Active*) also get an email from AppViewX PKIaaS for approval.
10. The active custodians click the **here** hyperlink in the email to be redirected to the AppViewX login page. On successfully logging in, go to **Menu > Requests > All requests** where the approval request is displayed with the **Approve** and **Reject** buttons.
11. Enter the comments and click **Approve.** If the request is rejected for any reason, then the approval status changes to *Email Verification - Rejected* and the status to *Inactive*.
    A confirmation popup window appears if you want to submit the request.
12. Click **OK.** Once the approval count reaches the minimum approval as set by the quorum number, the custodian is approved.
13. Click the  (**Refresh**) icon in the custodian table to see the approval status as *Add - Approved* and the status as *Active.*
14. [Optional] Click **Audit Log** against each custodian for more information about the request and the response count along with comments, if any, from other approvers. You can also download the audit log by clicking the **Download** button on the Audit Log view page. The audit log is exported in the .xls format. Once the audit log is fully loaded, the **Loading** button will turn to **View.** Refresh the page to see the **View** button.



When adding the second custodian, the second custodian gets an *Email Verification - Pending* notification message. After the email verification is done, an approval link is sent to the first custodian. On approval, the second custodian gets into the active state.

Important:

- If any of the approvals is in the pending state, then no new action on the CA or the Custodian Management pages are allowed until the current one is either approved/rejected/ aborted.
- At least two custodians must be added to perform the m(n) approvals in PKI+.

15. To add consecutive custodians, follow the aforesaid steps. Successful addition of custodians depends on the approval of active custodians per the quorum value set.

Deleting Custodians

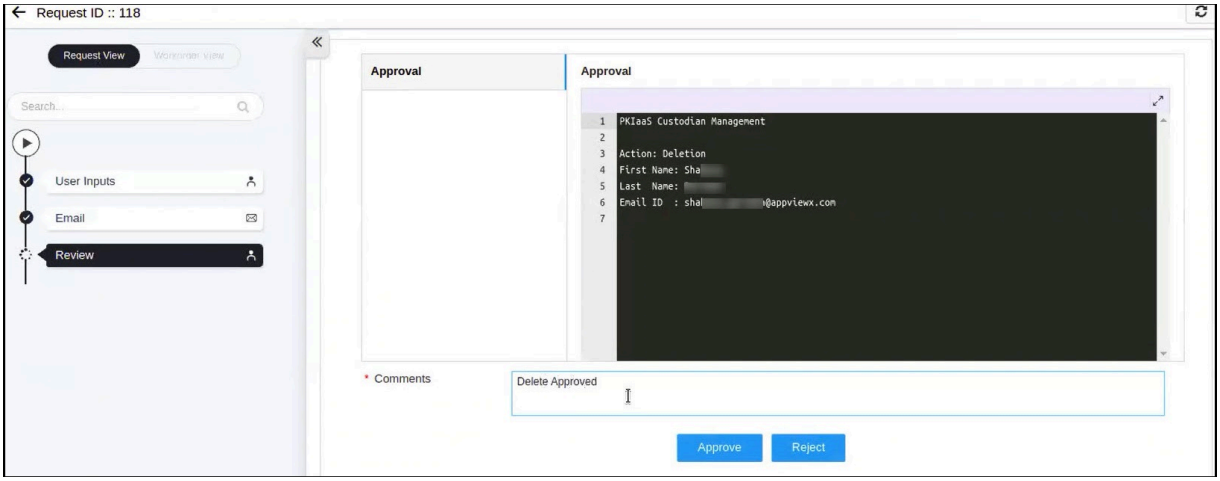
Attention: Deletion of custodians can be done by any administrator -OR- by key ceremony administrators, if configured. Minimum custodians must be available per the quorum value for m(n) approval.

To delete custodians:

1. Go to (**Menu**) icon **> PKI+ > Custodian Management.**
   The **Custodian Management** page appears.
2. Click the (**Delete**) icon against the custodian you want to delete.

A deletion mail is sent to all active custodians. The approval status changes to *Delete - Approval Pending.*

3. Click **Approve** to delete the custodian.



A confirmation popup window appears.

4. Click **OK** to confirm.

Once the approval count reaches the minimum approval as set by the quorum number, the custodian is deleted from the table. On successful approval, the approval status changes to *Delete - Approved* and the status changes to *Inactive.* If the deletion request is rejected, then the approval status changes to *Delete - Rejected* and the status changes to *Active.*

Filtering Custodians

You can currently apply filters to custodians based on their status using the **Filter By Status** option. The default filter includes both active and inactive selections. Clearing the filter allows you to view all entries.

CA Inventory

You can use this page to create your root CAs and subordinate CAs. There are two types of subordinate CAs: PKIaaS and external. PKIaaS subordinate CAs have their root CAs in the AppViewX system; external subordinate CAs are intermediate CAs whose root CAs are outside the AppViewX system.

- Creating Certificate Authority

Creating Certificate Authority

- To create AppViewX PKIaaS CA, see Configuring AppViewX PKIaaS Certificate Authority
- To create a root CA, see Creating Root CA.
- To create a subordinate CA from PKIaaS root CA, see Creating Subordinate CA from PKIaaS Root CA.
- To create a subordinate CA from external root CA, see Creating Subordinate CA from External Root CA.

Important: PKIaaS must not be used with the default policy; instead, have a specific policy for PKIaaS CA for creating certificates.

Complimentary CA

A complimentary CA is provided to all CERT+ customers. Customers using this CA cannot create a root CA but can create a subordinate CA that is signed by the AppViewX root CA as explained in Creating Subordinate CA from External Root CA. Once the CSR is downloaded, reach out to saashelp@appviewx.com. The complimentary CA can be deleted and re-created as required.

Configuring AppViewX PKIaaS Certificate Authority

To configure AppViewXPKIaaS Certificate Authority:

1. Go to **CERT+ > Administration > Certificate Authority.**

   The **Certificate Authority** page appears.

2. Select **AppViewX PKIaaS** from the list on the LHS of the panel and click **Configure Now.**
3. Enter the following fields:

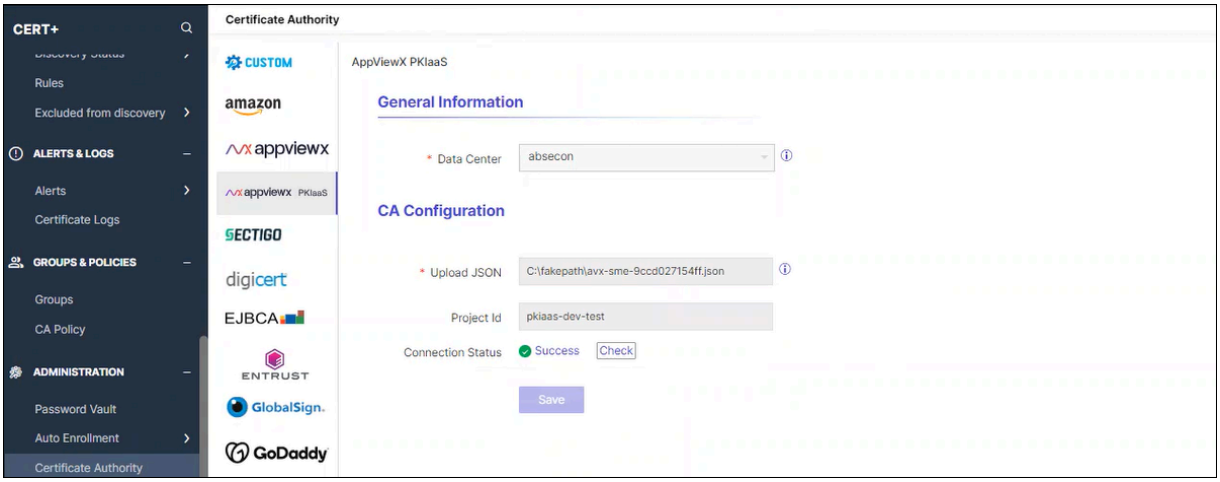
Field Description for AppViewX PKIaaS CA page

Field	Description
General Information	
***Data Center**	Select the data center through which the communication must happen.
CA Configuration	
***Upload JSON**	JSON credentials will be provided by AppViewX.
Project Id	This is automatically populated.

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

The uploaded credentials are validated for required permissions. Upon successful validation, the credentials are used for rotating the keys and new key is used for the CA creation.

4. Click **Check** to see if the connection is successful.



CA communication is validated and the connection status is shown as either Success or Failure.

5. Click **Save.**

Creating Root CA

Note: Customers using the complimentary CA can click the **+Create CA** button to directly create subordinate CA for external CA as explained in the Section, Creating Subordinate CA from External Root CA. The complimentary root CA is considered as an external CA in this case. The complimentary CA can be deleted and re-created as required.

To create root CA:

1. Go to **PKI+ > CA Inventory.**

   The **CA Inventory** page appears.

2. Click **+Create CA** on the top-right corner of the page.

   The **Create CA** page is displayed.

3. Enter the fields as described in the table.

Field Description for PKIaaS Management page

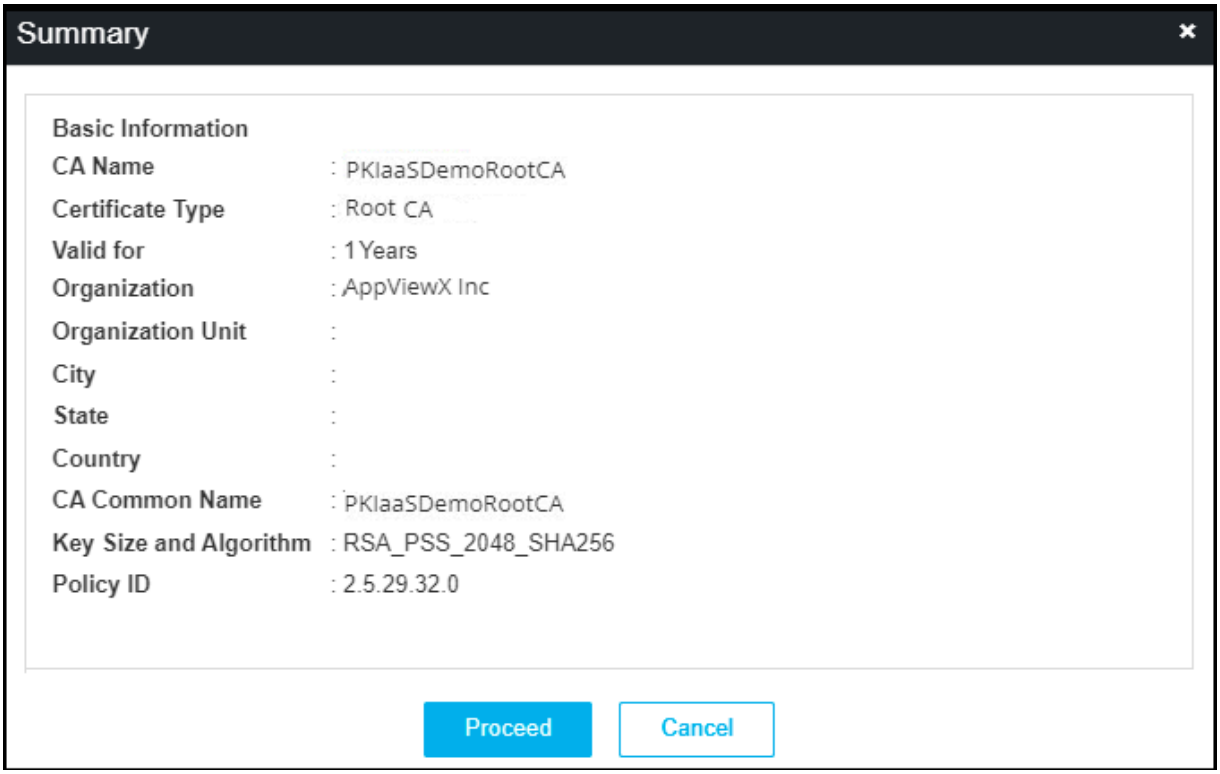
Field	Description
Select CA Type	
***CA Name**	Provide a friendly name for reference.
Certificate Type	Select **Root CA.**
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***Organization**	Enter the organization name owning the CA.
Organization Unit	Enter the business unit for CA operations.
City	Enter the city name.
State	Enter the state name.
Country	Enter the country of the organization.
***CA Common Name**	Enter the root CA subject name.
Configure CA Key Size and Algorithm	
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.

Field	Description
Configure CA Artifacts	
***Policy ID**	You can either select the CA policy ID from the dropdown list or key in the policy ID. By default, the value is 2.5.29.32.0.

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

4. Click **Save.**

   A window with the summary of values entered appears.



5. Click **Proceed** to trigger the approval flow.

   The newly created CA appears in the table with the approval status as *Create - Approval Pending* and the status as *Awaiting Approval* until all the necessary approvals are completed. If you want to abort the action, then click **Abort.**

An email from AppViewX is sent to all the active custodians for approving the CA.

addresssupport@appviewx.com
to me

Approval Request

Basic Information

Name	PKIaaSDemoRootCA
Type	Root CA
Validity	1 years

Subject

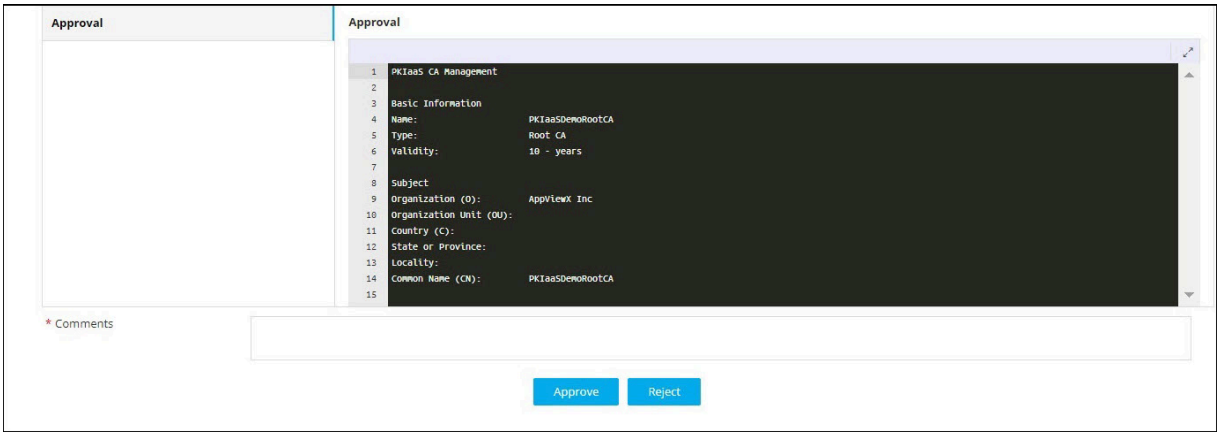
Organization (O)	AppViewX Inc
Organization Unit (OU)	
Country Code (C)	
State or Province	
Locality	
Common Name (CN)	PKIaaSDemoRootCA

Please click here to approve the request

Please do not reply as this is an auto generated email by AppViewX.

6. Click the **here** hyperlink in the email to be redirected to the AppViewX login page.

   On successfully logging in, the approval request is displayed with the **Approve** and **Reject** buttons.



7. Enter the comments and click **Approve.**

   A confirmation popup window appears if you want to submit the request.

8. Click **OK.** Once the approval count reaches the minimum approval as set by the quorum number, the custodian is approved.

   The approval status changes to *Create - Approved* and the status to *In Progress* until the CA is created and is enabled.

9. Click the  (**Refresh**) icon to see the status as *Active* once the CA is activated. Click **Resubmit** if the action fails for any reason.

   Certificates can be issued from this CA. CRLs are generated for this CA.

10. [Optional] Click the **Audit Log** against the CA to view the audit log details. You can also download the audit log by clicking the **Download** button on the Audit Log view page. The audit log is exported in the .xls format.

    Note: Once the audit log is fully loaded, the **Loading** button will turn to **View.** Refresh the page to see the **View** button.

11. [Optional] Click the **Approval Status** column value link to check the update on approvals.

    Note: The PKI CA thus created cannot be modified but can be viewed from the **PKI+ > CA Inventory** page.

What to do next:

- Creating Subordinate CA from PKIaaS Root CA -OR-
- Creating Subordinate CA from External Root CA

Creating Subordinate CA from PKIaaS Root CA

To create subordinate CA from PKIaaS root CA:

1. Go to  (**Menu**) icon **> PKI+ > CA Inventory.**
   The **CA Inventory** page appears.
2. Click **+Create CA** on the top-right corner of the page.
   The **Create CA** page is displayed.
3. Enter the fields as described in the table.

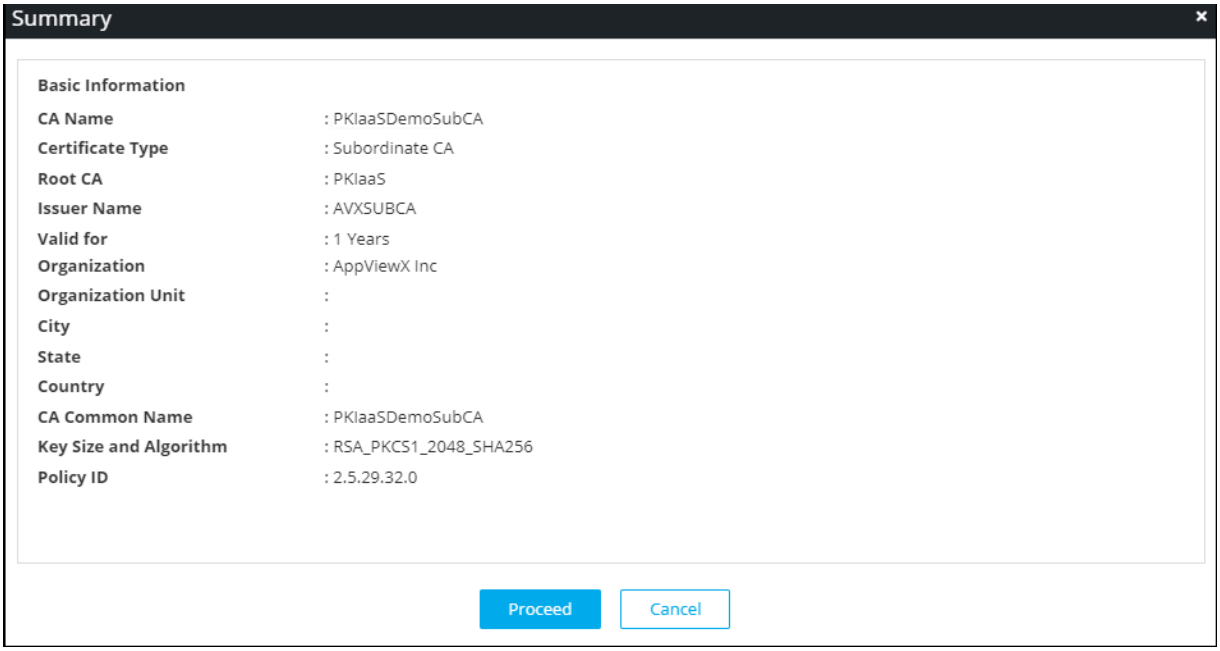
Field Description for PKIaaS Management page

Field	Description
Select CA Type	
***CA Name**	Provide a friendly name for reference.
Certificate Type	Select **Subordinate CA.** On clicking **Subordinate CA,** you see **Root CA** field with **External** and **PKIaaS** options.
Root CA	This field appears only on selecting **Subordinate CA.** Select **PKIaaS** if root CA is already in the AppViewX system. **Note:** Subordinate CAs need to activated and shows status as *Create - Approval Pending* until they are approved by the active custodians.
***Issuer Name**	This field appears only on selecting **Subordinate CA** as *PKIaaS*. Select an issuer name from the dropdown list.
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***Organization**	Enter the organization name owning the CA.
Organization Unit	Enter the business unit for CA operations.
City	Enter the city name.
State	Enter the state name.
Country	Enter the country of the organization.
***CA Common Name**	Enter the root CA subject name.
Configure CA Key Size and Algorithm	
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.

Field	Description
Configure CA Artifacts	
***Policy ID**	You can either select the CA policy ID from the dropdown list or key in the policy ID. By default, the value is 2.5.29.32.0.

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

4. Click **Save.**
   A window with the summary of values entered appears.



5. Click **Proceed** to trigger the approval flow.
   The newly created CA appears in the table with the status as *Create - Approval Pending.*

   An email from AppViewX is sent to all the active custodians for approving the CA. If you want to abort the action, then click **Abort.**
6. Click the **here** hyperlink in the email to be redirected to the AppViewX login page.
   On successfully logging in, the approval request is displayed with the **Approve** and **Reject** buttons.
7. Enter the comments and click **Approve.**
   A confirmation popup window appears if you want to submit the request.

8. Click **OK.** Once the approval count reaches the minimum approval as set by the quorum number, the custodian is approved.
9. Click the  (**Refresh**) icon on the **PKIaaS Management** page to see the *Active* status. Click **Resubmit** if the action fails for any reason.
   Once the PKIaaS subordinate CA is activated, the status changes to *Active*.
10. [Optional] Click the **Audit Log** against the CA to view the audit log details. You can also download the audit log by clicking the **Download** button on the Audit Log view page. The audit log is exported in the .xls format.

> **Note:** Once the audit log is fully loaded, the **Loading** button will turn to **View.** Refresh the page to see the **View** button.

11. [Optional] Click the **Approval Status** column value link to check the update on approvals.

Creating Subordinate CA from External Root CA

> **Note:** If you are using the complimentary root CA created in AppViewX, then you can create subordinate CA from external root CA as explained here.

To create subordinate CA from external root CA:

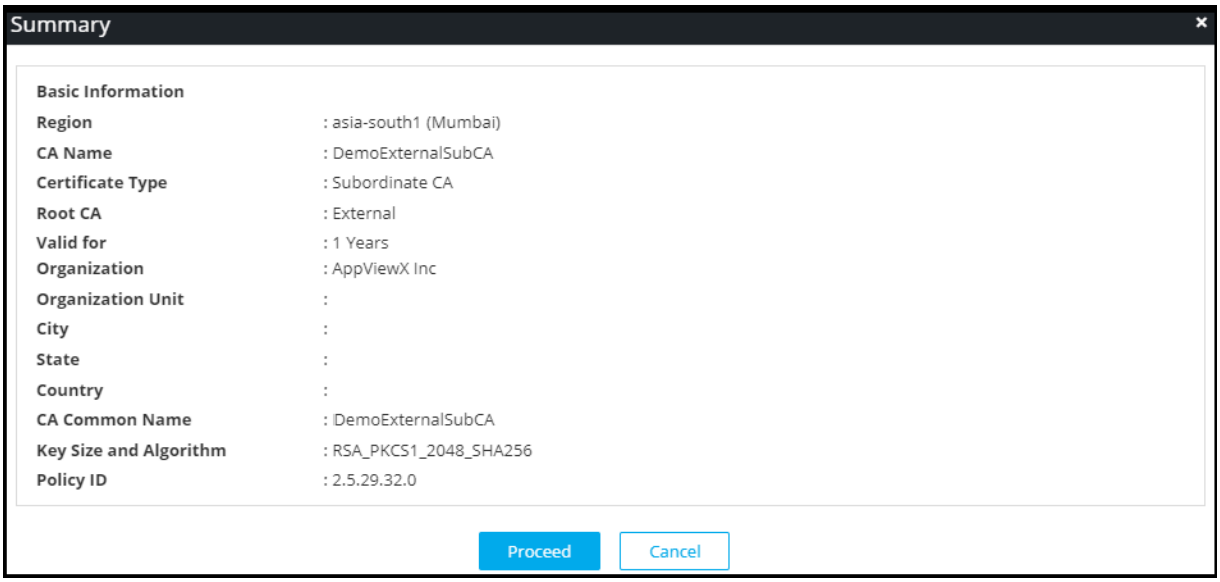
1. Go to (**Menu**) icon **> PKI+ > CA Inventory.**
   The **CA Inventory** page appears.
2. Click **+Create CA** on the top-right corner of the page.
   The **Create CA** page is displayed.
3. Enter the fields as described in the table.

Field Description for PKIaaS Management page

Field	Description
Select CA Type	
***CA Name**	Provide a friendly name for reference.
Certificate Type	Select **Subordinate CA.** On clicking **Subordinate CA,** you see **Root CA** field with **External** and **PKIaaS** options.

Field	Description
Root CA	This field appears only on selecting **Subordinate CA.** Select **External** if root CA is outside of the AppViewX system.
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***Organization**	Enter the organization name owning the CA.
Organization Unit	Enter the business unit for CA operations.
City	Enter the city name.
State	Enter the state name.
Country	Enter the country of the organization.
***CA Common Name**	Enter the root CA subject name.
Configure CA Key Size and Algorithm	
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.
Configure CA Artifacts	
***Policy ID**	You can either select the CA policy ID from the dropdown list or key in the policy ID. By default, the value is 2.5.29.32.0.
Note: Fields marked with red asterisk (*) symbol are mandatory.	

4. Click **Save.**
   A window with the summary of values entered appears.



5. Click **Proceed** to trigger the approval flow.
   The newly created CA appears in the table with the status as *Create - Approval Pending.* If you want to abort the action, then click **Abort.**

   An email from AppViewX is sent to all the active custodians for approving the CA.
6. Click the **here** hyperlink in the email to be redirected to the AppViewX login page.
   On successfully logging in, the approval request is displayed with the **Approve** and **Reject** buttons.
7. Enter the comments and click **Approve.**
   A confirmation popup window appears if you want to submit the request.
8. Click **OK.** Once the approval count reaches the minimum approval as set by the quorum number, the custodian is approved.
9. Click the  (**Refresh**) icon.
10. Click **Activate.** Until the signed certificate is uploaded, the status of the external subordinate CA remains as *Pending Signed Certificate.*
    The **Certificate Authority Activation** window appears.
11. Click **Download CSR.**
12. Once the CSR is downloaded, sign with valid root CA and click **Upload.**

> **Note:** Copy and paste or upload the complete certificate chain, ordered from leaf to root, starting with the subordinate certificate authority being activated.

Once the external subordinate CA is activated, the status changes to *Active*. Click **Resubmit** if the action fails for any reason.

13. [Optional] Click the **Audit Log** against the CA to view the audit log details. You can also download the audit log by clicking the **Download** button on the Audit Log view page. The audit log is exported in the .xls format.

    Note: Once the audit log is fully loaded, the **Loading** button will turn to **View.** Refresh the page to see the **View** button.

14. [Optional] Click the **Approval Status** column value link to check the update on approvals.

Actions

You can perform the following actions from the **Actions** menu of the **PKIaaS Management** page:

- Disable
- Enable
- Delete
- Filter

Disable

You can disable a root CA or a subordinate CA. No certificates can be issued from a disabled CA. CRLs will still be generated.

To disable CA:

1. Go to (**Menu**) icon **> PKI+ > CA Inventory.**
   The **CA Inventory** page appears.
2. Select the checkbox against the CA Name you want to disable.
3. Click **Actions** and select **Disable** from the dropdown menu.
   The approval status of the CA changes to *Disable - Approval Pending* and the status remains as *Active.* If you want to abort the action, then click **Abort.**
4. An email from AppViewX PKIaaS for approval is sent to all active custodians. Once the approval meets the quorum value, the CA is disabled. The approval status of the CA changes to *Disable - Approved* and the status to *Disabled.* If the request if rejected, then the approval status changes to *Disable - Rejected* and the status remains as *Active.* Click **Resubmit** if the action fails for any reason.
   You can follow the aforesaid steps to disable CAs.

Enable

You can enable a root CA or a subordinate CA. Certificates can be issued from this CA. CRLs are generated for this CA.

To enable CA:

1. Go to (**Menu**) icon **> PKI+ > CA Inventory.**
   The **CA Inventory** page appears.
2. Select the checkbox against the CA Name you want to enable.
3. Click **Actions** and select **Enable** from the dropdown menu.

   The approval status of the CA changes to *Enable - Approval Pending.* If you want to abort the action, then click **Abort.**
4. An email from AppViewX PKIaaS for approval is sent to all active custodians. Once the approval meets the quorum value, the CA is enabled. The approval status of the CA changes to *Enable - Approved* and the status changes to *Active.* If the request is rejected, then the approval status of the CA changes to *Enable - Rejected.* Click **Resubmit** if the action fails for any reason.

   A message that the operation is performed successfully appears.

   You can follow the aforesaid steps to enable CAs.

Delete

You can delete a root CA or a subordinate CA. Once the CA has been deleted, no new certificates can be issued from this CA and no new CRLs will be generated.

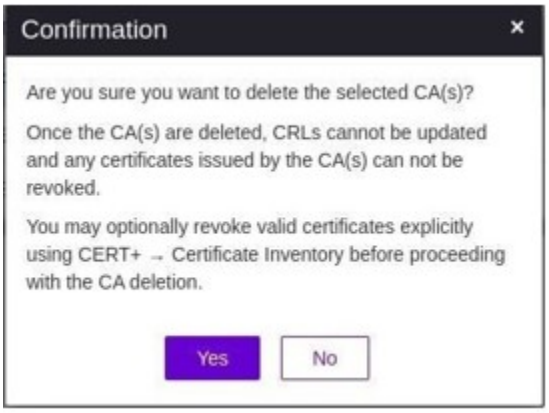
Before you begin:

- Deletion action will affect any auto-enrollment settings, policies, or workflows that are using the CA to issue or revoke certificates.
- Check for any unrevoked and unexpired certificates that may have been deleted from the AppViewX inventory by running a CA discovery to get all the valid certificates issued by that CA for revocation.
- To continue uninterrupted OCSP operations, replace the active OCSP certificate issued by the CA by going to **PKI+ > Validation Authority**.
- You can delete the root CA only after deleting all the subordinate CAs associated with it.

To delete CA:

1. Go to (**Menu**) icon **> PKI+ > CA Inventory.**

   The **CA Inventory** page appears.
2. Select the checkbox against the CA you want to delete.
3. Click **Actions** and select **Delete** from the dropdown menu.



Note:

- You can delete root CA only after deleting its subordinate CAs.
- If you are deleting a PKIaaS root CA or a subordinate CA, then you get a message, *Are you sure you want to delete the selected CA(s)?* irrespective of whether there are valid certificates issued by the CA or not.
- If the CA was enabled at least once, then you get a message, *Once the CA(s) are deleted, CRLs cannot be updated and any certificates issued by the CA(s) can not be revoked (AND) You may optionally revoke valid certificates explicitly using CERT+ → Certificate Inventory before proceeding with the CA deletion.*

4. Click **Yes** to proceed.

   The delete workflow is triggered. The approval status of the CA changes to *Delete - Approval Pending.* If you want to abort the action, then click **Abort.**
5. An email from AppViewX PKIaaS for approval is sent to all active custodians. Once the approval meets the quorum value, the approval status of the CA changes to *Delete - Approved* and the status changes to *Deleted.* If the request is rejected, then the approval status of the CA changes to *Delete - Rejected.* Click **Resubmit** if the action fails for any reason.

   A message that the operation is successful appears.

Note: If deletion fails, reach out to saashelp@appviewx.com.

Filter

You can currently apply filters to certificate authorities based on their status using the **Filter By Status** option. The default filter includes statuses such as enabled, disabled, pending, and others. Clearing the filter allows you to view all entries.

Note: The **Others** option in the filter encompasses different stages of workflow approval, including awaiting approval, rejected among others. Aborted entries are also displayed when Others option is selected.

Validation Authority

Certificate authorities use Online Certificate Status Protocol (OCSP) to obtain the revocation status of x.509 digital certificates. When a user requests the validity of a certificate, an OCSP request is sent to an OCSP server to check the specific certificate with a trusted certificate authority. The OCSP server then sends a *good, revoked, or unknown* response.

Prerequisites

- OCSP URL must be published in the AIA field of the certificate with the AppViewX OCSP server URL.
- **Plugins required:** OCSP Server and OCSP Generator must be deployed for OCSP to work.

You can then proceed to select one or more certificates from the inventory and click **Actions > Revocation Check** to perform revocation validation. Once validated, the certificate status is updated in the color code of the Common Name column.

- OCSP Profiles
- Creating OCSP Signing Certificate

OCSP Profiles

You can create the following OCSP profile by going to **PKI+ > Validation Authority > OCSP:**

OCSP Signing: By default, an OCSP signing certificate is created along with a new CA creation. Clicking this field lists all the valid OCSP signing certificates available in the AppViewX PKIaaS inventory along with common name, serial number, issuer common name, extended key usage, and status.

Note: Only one OCSP signing certificate is active at any given point of time.

- If you want to activate a selected OCSP signing certificate, you can do it from **Actions > OCSP Signing.** The OCSP configuration is updated with the selected certificate.

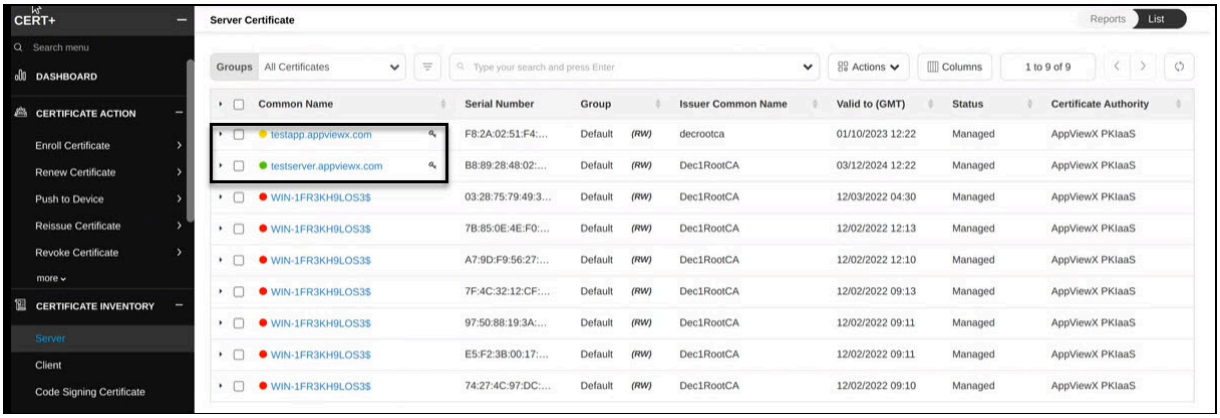
> **Note:** An OCSP signing certificate can be revoked only on deleting the CA. If an OCSP signing certificate is revoked or deleted from the **CERT+ > Certificate Inventory > Server** page, then the OCSP responder will not work. To remediate this action, you can create a new OCSP signing certificate by going to **CERT+ > Certificate Action > Enroll Certificate** and following the procedure explained in the Section, Creating OCSP Signing Certificate.

Creating OCSP Signing Certificate

To create an OCSP signing certificate:

1. Go to **CERT+ > Certificate Action > Enroll Certificate.**
   The **Enroll Certificate** page is displayed.
2. Select the **Certificate Authority** as *AppViewX PKIaaS.*
3. Select the **Certificate Profile** as *OcspSigning.*
4. Fill out the other fields as explained in the Section, Adding/Enrolling Certificate.

   The OCSP signing certificate appears on the **CERT+ > Certificate Inventory > Server** page as shown with a key symbol beside the common name.

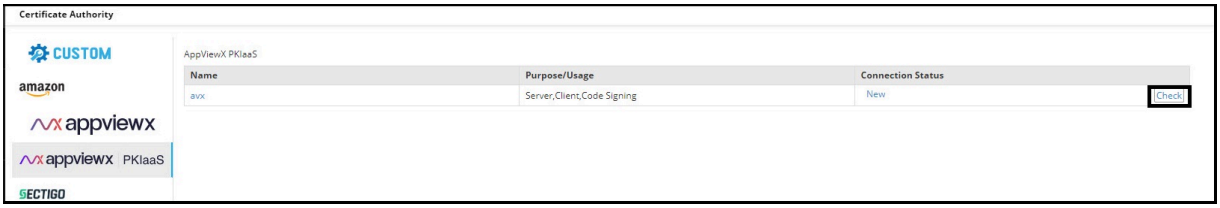


Validating Certificate Authority

Once the **AppViewX PKI+** settings are added, you need to validate to check if the connection between AppViewX and **AppViewX PKI+** is properly configured.

To validate the **AppViewX PKIaaS CA**:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Certificate Authority** from **Administration** on the LHS pane.
3. Click **AppViewX PKIaaS**.
   The Certificate Authority home page appears.



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

   CA communication is validated and the connection status is shown as either Success or Failure.

Certificate Group

Before you Begin

Before starting **Certificate Groups** configuration:

- **Certificate Groups** are used to categorize the certificates according to various **business units.**
- In some organizations, **Certificate Groups** are also used to assign access permissions. Only privileged users (inherits from Resource > User Group) can view the respective **Certificate Groups**.
- Users should be assigned to a **Role** (inherited from Role > User Group) that has access to perform the below actions,
  - View a group
  - Assign a group
  - Unassign a group
- With these actions, users can assign a group during **Certificate Discovery** to avoid movement of certificates post-discovery.

- Along with the view, assign, and unassign options, administrators should be assigned to a **role** that has access to additional actions,
  - Create/ modify a group
  - Delete a group
  - Edit Default group

Adding Certificate Group

To create a certificate group:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Groups** from **Groups & Policies** on the LHS pane.
3. Click **+ Create.**

   The **Create Group** page is displayed.
4. In the **Group Details** section, enter the following details:

Field Description for Group Details section

Field	Description
***Select Group Hierarchy**	From the list of group hierarchies, select the parent group of the new group.
***Group Name**	Enter a unique name.
Application ID	Enter an ID specific to your organization.
Description	Enter detailed information regarding the group stating the purpose.

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

5. In the **Other Details** section, provide the following details about the certificate group:

Field Description for Other Details section

Field	Description
Contact Name	Enter the name of the person to be contacted in case of any changes.

Field	Description
Line of Business Name	Enter the name of the business unit.
Email	Enter the email address of the contact person.
Environment Name	Enter the name of the environment.
Phone Number	Enter the phone number of the contact person.
Inventory Number	Enter the number related to the inventory.
Cost Center/ Hierarchy	Enter the cost center code/ label.
Push Certificate Automatically	To associate the certificate automatically with its device, select the **Push Certificate Automatically** checkbox.
Renew Automatically	To enable automatic renewal of the certificates under this group, turn on the Renew Automatically toggle. **Note:** If you enable the automatic renewal, two more details have to be entered: • **Start Renewing:** Enter a number between 1 to 90 to denote the number of days. The system will renew the certificate before expiry. • **Approval required:** To enable the requirement for approval, select this checkbox. **Warning:** If you change the group associated with the certificate, the number of renewal days will be overwritten as per the new group.
Associated Policy	From the list of CA policies, select the required **Associated Policy.**

6. Click **Create** to add the certificate group to the system.

Note: You can search for the required group and add the frequently used keywords as favorites. You can also create a certificate group for Server, Client, and Device certificates by clicking the **Group** () icon from the respective tabs under **Certificate Inventory.**

Editing Certificate Group

To modify a certificate group:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Groups** from **Groups & Policies** on the LHS pane.

   The group inventory page appears.
3. Click the name of the certificate group you want to edit.
4. On the Modify screen that appears, make whatever changes you want to the content.
5. Click **Update** to save your edits.

Deleting Certificate Group

To delete a certificate group:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Groups** from **Groups & Policies** on the LHS pane.

   The group inventory page appears.
3. Select the group you want to delete and click **Delete.**
   A **Confirmation** popup window appears.
4. Click **Yes**.
   The group is deleted from the inventory.

Assigning or Unassigning Group to Certificate

To assign a group to a certificate from within the Inventory module:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. From **Certificate Inventory,** click **Common Name** of the certificate whose CSR you want to download and click **Assign Group.**

   -OR-

On the certificate list, select the checkbox beside the certificate that you want to assign a group to. Click **Actions** and select the **Assign Group** option from the dropdown.

The **Assign/Unassign Certificates** screen appears.

3. Select the group you want to assign to the certificate.
4. Click **Assign**.

> **Note:** You can follow the same steps selecting **Unassign Group** to unassign. You cannot unassign a certificate from the Default group. If you unassign a certificate from the assigned group, it is assigned to the Default group.

Certificate Authority Policy

The CA policy defines rules and templates to ensure certificate attributes comply with the organization.

• Adding Certificate Authority Policy

Adding Certificate Authority Policy

The CA policy defines rules and templates to ensure certificate attributes comply with the organization.

To create a CA policy:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **CA Policy** from **Groups & Policies** on the LHS pane.
3. Click **+ Create** in the command bar to configure certificate practice standards for business unit.

   The **Policy Details** page is displayed.
4. Enter the details as described:

Field Description for Policy Details section

Field	Description
***Policy Name**	Enter a unique name for the certificate policy.
Description	Enter the policy information.

Field	Description
Policy Enforcement Type	Choose any of the options: • **Strict:** While adding or updating the Certificate Authority (CA) connector, values provided as part of the Certificate Signing Request (CSR) information should match the values provided in the policy. If the values do not match the policy, you cannot save the CA connector details. • **Suggestive:** While adding or updating the Certificate Authority (CA) connector, values provided as part of the Certificate Signing Request (CSR) information do not have to be an exact match to the values provided in the policy. You can modify the values provided, but the certificate is then considered to be non-compliant.
Certificate Requests Need Approval?	Enable proper control through appropriate approvals for various actions performed on the group of certificates to which this policy is applicable.
Enable Access to Private Key?	Enable the option to allow private keys of the certificates to be exported.
Enable certificate push-bind access for read-only user	Enable the option to allow certificate push, bind and rollback operations from the holistic view for the user who got only read permission on the certificate group.
Validate issuer and root certificate for compliance?	Enable the option to check if issuer and root of the certificate are compliant to the standard defined in the policy.
Email Address mandatory for Client Certificate	Enable the option to set email address as mandatory during the client certificate enrollment.

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

5. In the **CA details** section, enter the following information:

Field Description for Create CA Policy section

Field	Description
***CA Accounts**	Select the CA to associate with the policy. Based on the CA selected, fields are populated.

Field	Description
Certificate Issuance From	By default, Issuer Name is selected.
***Issuer Location**	Select a location from the dropdown list.
***Issuer Name**	Select issuer name from the dropdown list. This field appears only on selecting **Issuer Name** in the **Certificate Issuance From** field.
***Validity**	Enter a value and press Enter.
***Bit Length-Key Type**	Select a value from the dropdown list.
***ECDSA curve**	Select a value from the dropdown list.
***Hash Function**	Select a value from the dropdown list.

6. [Optional] **Certificate parameters** section can be used later to help distinguish between multiple policies within the system.

Field Description for Certificate parameters section

Field	Description
Restrict Wild Card Certificate	Enable this option to restrict wild card certificates.
***Host Name**	Enter a host name. Host name must not start or end with a period (.).
***Allowed Domain Names**	Type a domain name and press **Enter.**
Common Name	The fully qualified domain name (FQDN) or common name that exactly matches your web browser.
Organization	The name of the organization requesting the certificate.
Organization Unit	The division of the organization requesting the certificate.
Locality	The location of the organization requesting the certificate.
State	The state in which the organization is located.
Country code	The country and the country code in which the organization is located.
Email	The email contact details of the person responsible for maintaining the certificate.

Field	Description
Subject Alternative Name	Any additional hostnames, such as alternative websites, IP addresses and so on that have to be protected with the single SSL certificates.

7. Click **Save Details.**
   The added CA account is displayed in the table. You can view the CA account details, edit, or delete the CA account using the options provided.
8. Under the **Group selection** section, select the group(s) you want to include in the policy or create a new group to which the policy must be assigned.

> **Note:** You can search for the required group and add the frequently used keywords as favorites.

9. Under the **Compliance check** section, you can turn on the **Perform Compliance Check** toggle button to check the compliance for the defined rules and certificates attributes of the inventoried certificates.
10. Click **Create Policy.**

> **Note:** If you want to make any changes to the policy in the future, you can select the policy and make the respective changes. If you want to completely reset the policy data, click **Reset** beside the CA name on the right pane.

Certificate Enrollment

A typical certificate enrollment process involves the requester generating a key pair (one public, and one private key), sending only the public key to a CA along with a CSR (Certificate Signing Request), and then receiving a CA-signed certificate that can be installed on an endpoint.

- Adding/Enrolling Certificate
- Uploading Key
- Post-Enrollment Usage of Certificates

Adding/Enrolling Certificate

To enroll a certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Enroll Certificate** from **Certificate Action** on the LHS pane.
3. Select **Server**, **Client,** or **Code Signing Certificate** depending on the type of certificate(s) you want to enroll.

   The **Enroll Certificate** page appears.
4. In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list.
5. In the **CA Details** section, enter the details as follows:

Field Description for CA Details section

Field	Description
***Certificate Authority**	Select **AppViewX PKIaaS**.
***Regenerate Automatically**	Select the toggle button to On or Off. • When the toggle is enabled, the **Start Regenerating** option is enabled. • Enter the number of days to regenerate the certificate automatically before expiry.
***CA Account**	The account to which the enrollment request is submitted. By default, it is *pkidev.*
Certificate Profile	Select the profile from the dropdown list. While enrolling server certificate, you get the option of *OcspSigning* as well in the dropdown list. For more information, see **CERT+ > Administration > Certificate Profiles.**
***Issuer Location**	Select an issuer location from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate from the dropdown list.
***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. By default, it is *AppViewX PKIaaS CA connector.*
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.

Field	Description
	• **AppViewX:** Private key and CSR are created in AppViewX based on CSR parameters given. • **Upload CSR:** Uploaded CSR is taken as a source to populate CSR parameters and submit to CA.

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

6. In the **CSR Parameters** section, enter the details as follows:

Field Description for CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of the Certificate Signing Request (CSR) to be present on the certificate. For example, <appviewx>. **Note:** No special characters allowed except period(.), hyphen (-), and underscore (_).
Subject Alternative Name	Select the subject alternative subject name from the dropdown list. You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. **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 is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The organization unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Field	Description
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present on the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter a 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 controlled by the group's policy.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***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.

7. In the **Attachments** section, there is an optional field where the user/admin wants to keep any relevant attachment for the certificate enrollment, such as an approval email.

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

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

Field Description for 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 to upload a file.

8. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example: cost center. Inventory can be filtered based on these attributes as well. If the Certificate Attributes are added under **Administration > Certificate Attributes,** it is reflected in the enrolment page.
9. In the **Generic Fields** section, enter the **Device Name** and the **Application IP Address**.
10. In the **Vendor specific details** section, the **Certificate ID** is auto-populated based on the value entered in the **Common Name** field.
11. Click **Add.** Once the details are added, it will redirect you to the page where you 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.
12. Click the **Submit** button to trigger the request.
    Once the submit action is triggered, the Submit popup window appears. Add comments if needed, and then click **Yes.** If the approved option is enabled in CA Policy, the request goes to the Approve and Implementation stages.
13. Click **Approve**.
14. The **Approve** pop-up window appears. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.
15. Enter the comments in the field.
16. Click **Yes**.
    Once approved, you can see the Implement option in a holistic view.
17. Click **Implement.**
18. The **Implement** pop-up window appears. Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.
19. Enter the comments in the field.
20. Click **Yes**.

What to do next

CSR Submission to CA is in progress.

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

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

If auto-approval is disabled in the targeted CA, the user has to be logged into CA and approve the request.

Once the certificate is issued successfully, the certificate is retrieved to AppViewX.

Uploading Key

To upload a certificate key for the CSRs and certificates generated outside AppViewX:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Select the type of certificate you want to upload key for from the **Certificate Inventory.**
3. In the list of certificates, click the common name of the certificate for which you want to upload a certificate key.
   The certificate topology appears.
4. Hover the mouse over (**More**) icon on the server certificate and click **Upload Key.**
5. If the key you want to upload is password-protected, a popup screen appears asking you to enter the associated password.
6. Click **Submit.**
7. On the screen that pops up, navigate to the key you want to upload and click **Open.**

> **Note:** If the key you are trying to upload does not match the certificate, an error message that the *Certificate and key do not match* appears.

If everything is correct, the key is uploaded to the certificate.

Post-Enrollment Usage of Certificates

Once a requester obtains a digital certificate signed by a CA, they can install this certificate onto an endpoint, which becomes a trusted network entity (it is assumed that the third party possesses the CA's public key in order to do this – the root CAs of leading CAs are installed on all major browsers).

As part of the standard TLS handshake process, any third party that interacts with the certificate owner will proceed to review the validity of the issued certificate by decrypting the digital signature provided by the CA.

The third party contrasts the decrypted hash function against the hash obtained by hashing the digital certificate. A match indicates integrity of the certificate. The communicating third party can then retrieve the public key from the digital certificate and proceed to establish a secure encrypted connection.

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 it will provision certificates from on-premises infrastructure.

- Adding Application Connector to Certificate

Adding Application Connector to Certificate

To add an application connector to a certificate:

1. Go to  (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Server** or **Client** from **Certificate Inventory.**
3. In the Certificate list view page, click the **Common Name** of a certificate to add an application connector.
4. In the Certificate topology page, click **Add connector** or click **Connector actions > +Add App Connector.**

   The **Add Connector** is displayed.
5. In the **General Information** screen:
   - Select the device type from the **Category** dropdown list.
   - Select the device vendor from the **Vendor** dropdown list.

- In the **Connector Name** field, enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
- Enter a description for the connector. This description shows up when you hover the mouse over the connector within the Certificate topology.

> **Note:** Applicable only for Citrix application type] The SNI-enabled virtual server option is displayed. When this checkbox is selected, the virtual servers whose SNI are enabled are listed. You can also enable SNI for the virtual server by selecting Enable SNI push for Certificate and Enable SNI in Virtual Server.

6. From the list of available devices, click **Add to List** () button beside each device you want to select.
7. In the **Certificate Details** section:
   - From the **Certificate Type** dropdown, click the type of certificate to be used with the connector.
   - From the **Certificate File Name** field, enter the name of the certificate. The file format of the selected certificate type is automatically displayed.
   - In the **Key File Name** field, enter a name for the key file.
   - Select the **Push Root and Intermediate Certificates** to be pushed to the device.
8. In the **Push Details** section:
   - In the **Script location** field, specify whether the **Pre - Push** script and **Post - Push** script file is in AppViewX or target device.
   - Enter the script location that must be executed before and after the push in the Pre – Push script and Post - Push script fields.
   - Select the **Overwrite** checkbox to overwrite existing certificates with the new certificate.
   - Select **Push automatically** checkbox to push certificates to the device automatically.

> **Note:** [Applicable for F5 application type] The Secure push checkbox is selected by default. This option encrypts certificates while pushing them to a device. You can uncheck this option if you have the necessary permissions.

9. Click **Save** to add the application connector to the certificate topology.

Pushing Certificate to Device

The push to device option allows you to push the certificate to the load balancer or server device and associate it to a profile, template, or virtual server.

If the **Push automatically** field is selected while adding application connectors to a new certificate, then the certificate is automatically pushed to the device when it is retrieved. In such case, you need not complete the process manually.

Prerequisites

Prior to pushing the certificate to a device, ensure that you have necessary role-based access controls and workflow access pertaining to the template and request.

To push a certificate to a device:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Select **Push to Device** from **Certificate Action.**
   The **Server Certificate** page appears.
3. Search for the certificate in the inventory and click the **Common Name** of the certificate to view the holistic view.
4. Click **Push to device.**
5. In the **Confirmation** popup window, enter comments and click **OK.**
   A request ID and work order ID are generated automatically and the work order status is displayed beside the connector in the topological view.
6. Click **Approve.** The work order status displayed beside the connector updates to *Push-Review In Progress.*

   On the **Approve** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.
7. Click **Implement.**
8. On the **Implement** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.
9. Click (**Refresh**) at the top of the page until the topology updates.

   After the push action is completed, the status is updated to *Completed.*

   The topological view follows a color-coding scheme to identify certificate statuses.

Color Coding for Certificate Statuses

Color	Certificate Status
Green	Certificate is available and valid.
Red	Certificate has expired.
Gray	Certificate push action failed.
Blue	Certificate will expire in 90 days.
Yellow	Certificate will expire in 90 days.
Orange	Certificate will expire in 90 days.
Black	Certificate will expire in 90 days.
Mid Purple	Certificate associated with profiles is manually removed.

Chapter 4: Certificate Chain of Trust

Overview

The widgets in the dashboards contain reports that provide consolidated statistics for the list of all accessible certificates by extracting its data from the certificate inventory and record the key value indicators for expiry and compliance use cases.

There are three types of certificates in CERT+:

- Server Certificate
- Client Certificate
- Code Signing Certificate

Certificate chain (or chain of trust) is made up of a list of certificates that start from a server's certificate and end with the root certificate. If your server's certificate is to be trusted, its signature has to be traceable back to its root CA. In the certificate chain, every certificate is signed by the entity that is identified by the next certified along the chain.

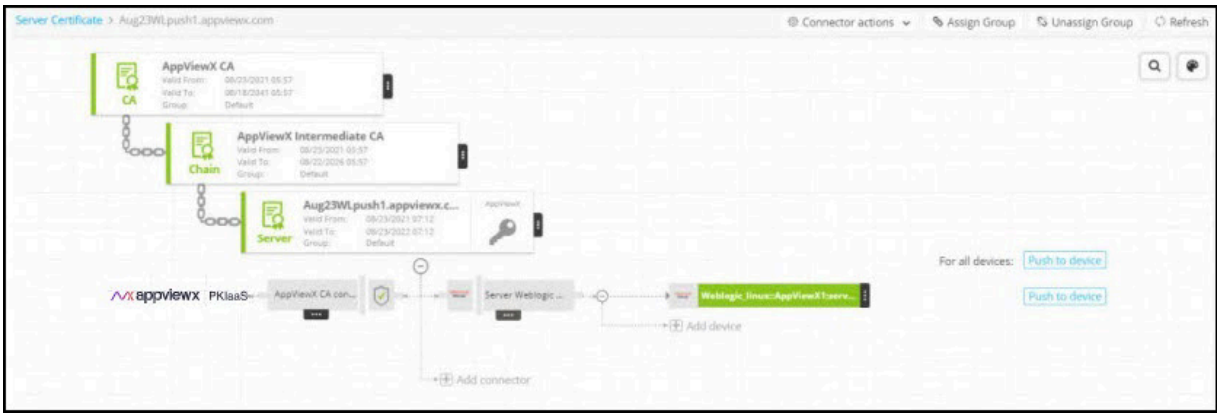
Viewing Certificate Topology

To view the topology that a server or client certificate belongs to:

1. Go to (**Menu**) icon **> CERT+.**

   The **CERT+** left navigation pane appears.
2. Click **Certificate Inventory** and select the type of certificate you want to view**.**
3. On the list that appears on the screen, click the **Common Name** of the certificate.

   The screen refreshes and displays the topology of the corresponding certificate.



Note: For certificates that are reissued, renewed, or regenerated, the certificate has a history, which is denoted by an H symbol beside its name.

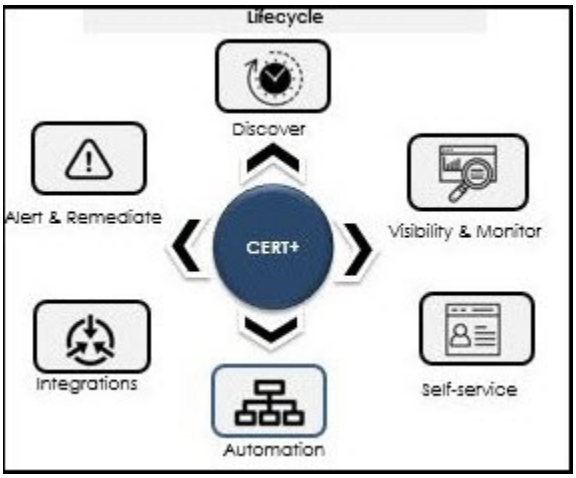
4. Click (**Refresh**).

   A **Certificate History** screen pops up with details corresponding to the selected certificate.

Chapter 5: Certificate Lifecycle Management

What is Certificate Lifecycle Management (CLM)?

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



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

- **Certificate 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.

Inventoried Certificate Actions

Important: Configure policy first before performing any of the certificate actions.

The following actions can be performed on certificates:

- Downloading Certificate
- Uploading Certificate
- Exporting Certificate
- Renewing Certificate
- Regenerating Certificate
- Revoking Certificate
- Generating CSR for Certificate
- Submitting CSR to Certificate Authority
- Downloading CSR
- Suspending Certificate
- Changing Status of Certificate
- Deleting Certificate
- Revocation Check - OCSP

Downloading Certificate

Note: This functionality is available only for server, client, device, code signing, intermediate, and root certificates.

You can download a certificate from the Certificate page and the topology page within AppViewX.

Download from Certificate Inventory

To download a certificate as a .PEM file that is designed to be safe for inclusion in ASCII or rich-text documents such as emails:

1. Go to (**Menu**) icon **> CERT+.**

   The **CERT+** left navigation pane appears.
2. Click **Download** from the **Certificate Inventory** after selecting the type of certificate you want to download.
3. Switch to the **List** toggle button on the top right corner of the certificate page.
4. Select the check box for the certificate that you want to export.

   Note: Client certificates cannot be downloaded directly from the Certificate page; they can only be downloaded from the certificate topology screen. For more details, see the Section, *Download from Certificate Topology*.
5. Click **Actions,** and select **Download Certificates.**
6. In the **Download Certificate** popup window, select **Certificates Only.**
7. You can also enable/disable the **Download Trust Store Certificates** option.

   Note: If you have permission to view the restricted content mentioned in Step 6, the certificate details are then downloaded inside a zip file. If you do not have the necessary permissions, the system creates and downloads an empty zip file to the destination you specify.
8. Click **Download.**
9. To view details of the certificate, unzip the file, and open the security certificate file. Click **Details.**

Download from the Certificate Topology

1. Go to (**Menu**) icon **> CERT+.**

   The **CERT+** left navigation pane appears.
2. Click **Download** from the **Certificate Inventory** after selecting the type of certificate you want to download.
3. Switch to the **List** toggle button on the top right corner of the certificate page.
4. From the **Common Name** certificate list, select the certificate that you want to download.
5. Hover the mouse over on the certificate and click **Download Certificate.**
6. In the **Download certificate** pop-up window, select the file format.

- For PEM and DER certificate types, you can enable/disable the **Download Trust Store Certificates** option along with the end certificates.
- For PEM and DER certificate types, you can enable/disable the **Download Trust Store Certificates** option along with the end certificates.

7. Click **Yes.**

Uploading Certificate

To upload a certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Upload** from **Certificate Inventory.**

   The **Upload Certificate** screen is displayed.
3. Select the **Certificate Group** into which the uploaded file must be mapped in CLM.
4. Choose the certificate file and click **Open.**
5. Click **Upload.**
   Once uploaded, go to the selected certificate group in inventory to see the uploaded certificate-keys.

Exporting Certificate

You can export all the certificates in the inventory or select only specific certificates and export. You export certificate details in the form of columns and values. The output can be exported in <.xls> or <.csv> format. This can be used for reporting or making another inventory.

To export the server certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click the **Certificate Inventory** and select the type of certificate you want to export.
   The **Certificate** screen is displayed.
3. Switch to the **List** toggle button on the top right corner of the certificate page.
4. In the **Common Name** column certificate list, select the check box against the certificate that you want to export certificate to.
5. Click **Actions**, and then select **Export Certificates** from the list.
   The **Export** popup window appears.

6. Select the desired **Options** and **Format** in the **Export** pop-up window.
   The selected certificate is exported to your local machine.

Renewing Certificate

Note: Only certificates having CSR/private keys can be renewed. Click **Renew Certificate** to renew certificates with existing keys; click **Regenerate Certificate** to renew certificates with new keys.

Enable **Renew Automatically** to avoid doing it manually. It is recommended to renew certificates with new keys.

From Holistic View

To renew a certificate from the holistic view:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Renew Certificate** from **Certificate Action.**
3. Click **Server, Client,** or **Process Explorer** depending on the type of certificate you want to renew.
4. Switch to the **List** toggle button on the top right corner of the page.
5. In the **Common Name** column certificate list, select the certificate that you want to renew.
6. Hover the mouse over (**More**) icon and click **Renew.**
   You are redirected to the **Certificate** page.
7. In the **Vendor Specific Details** section, enter a new **Certificate ID** and click **Renew.**
   In the Renew popup window, enter comments and click Yes. A request ID and work order ID are then generated automatically and the work order status is displayed beside the certificate in the topological view. The work order status displayed beside the connector updates to *Renew Certificate renewal request In Progress.*
8. Click **Approve.**
9. On the **Approve** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.

   The work order status displayed beside the connector updates to *Push-Review In Progress.*
10. Click **Implement.**
11. On the **Implement** screen that pops up:

- Click **Now** or **Schedule Later** button in the **Implement** field.
- If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
- Enter comments and click **OK**.

12. Click  (**Refresh**) icon on the top of the page until the topology updates.
    After the renewal action is completed, the status is updated to *Completed.*
13. On the **Renew Certificate** popup window, select the type of certificate renewal as **Now** or **Set auto-renew**.
14. Select **Submit**.
    The status of the trigger can now be monitored under process explorer.

> **Note:** Alternatively, you can go to **Certificate Inventory** and select the check box against the certificate name you want to renew and click **Actions > Renew Certificate** from the command bar.

Regenerating Certificate

> **Note:** The regenerate option allows you to create a new certificate with a new key and with similar parameters to an existing certificate so that you can host it on a different type of web or application.

To regenerate a certificate:

1. Go to  (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Switch to the **List** toggle button on the top right corner of the page.
3. In the **Common Name** column certificate list, select the certificate that you want to regenerate.
   The Certificate page is displayed.
4. Hover the mouse over  (**More**) icon on the certificate, and click **Regenerate.**
5. In the **Vendor Specific Details** section, enter a new **Certificate ID** and click **Regenerate.**
6. Click **Approve**.
7. On the **Approve** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.
8. Click **Implement.**

9. On the **Implement** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Manual Implementation** field to choose the mode of implementation.
   - If you select **Schedule Later**, set the date and time that you want the certificate implementation to occur.
   - Enter comments and click **Yes**.

   A request ID and work order ID are generated automatically. The work order status is displayed beside the certificate on the topological view.
10. Click  (**Refresh**). The work order status is displayed beside the certificate.
    After the regenerating action is completed, the status is updated to *Completed.*

Revoking Certificate

If you have the necessary permission, you can submit a request to the issuer of a certificate to revoke it. As soon as the certificate is revoked, the certificate is no longer considered to be trusted. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.

Note: Revoke old certificates after renewing and provisioning new keys.

To revoke a certificate:

1. Go to  (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Switch to the **List** toggle button on the top right corner of the page.
3. In the **Common Name** column certificate list, select the certificate that you want to revoke.
4. Hover the mouse over  (**More**) icon on the certificate, and click the **Revoke** option.
5. Select a reason for revoking the certificate.
6. Click **Yes.**
   A request ID and work order ID are generated automatically and the work order status is displayed beside the certificate on the topological view.
7. Click **Approve**.
8. On the **Approve** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.

9. Click **Implement.**
10. On the **Implement** screen that pops up:
    - Click **Now** or **Schedule Later** button in the **Implement** field.
    - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
    - Enter comments and click **OK**.
11. Click  (**Refresh**). The work order status is displayed beside the certificate.

> **Note:** Alternatively, you can go to **Certificate Inventory** and select the check box against the certificate name you want to revoke and click **Actions > Revoke Certificate** from the command bar.

After the regenerate action is completed, the status is updated to *Completed.*

• Performing Revocation Check

Performing Revocation Check

For CAs (both external and AppViewX), you can check the most recent status of the certificate even if it is moved to the inventory for the first time. This check is performed automatically twice a day and the user can check for the revoked certificates anytime.

To perform a revocation check:

1. Go to  (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Server, Client, Device, or Code Signing** depending on the type of revoked certificates you want to view.
3. In the certificate list, select certificates for which you want to view the status.
4. Click **Actions,** and select **Revocation check** option from the dropdown.

   The **Revocation Check** dialog box appears.
5. Click **OK.**
   Once validated, the status certificate is updated in the color code of the **Common Name** column.

Generating CSR for Certificate

To generate a manual CSR for the certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **Generate CSR** from **Certificate Action.**
3. Click **Server** or **Code Signing Certificate.**

   The **Generate CSR** page appears.
4. In the **Group details** section, select the **Assign Group** from the dropdown list where you want to assign a CSR to the desired group of certificates.

Field Description for Group details section

Field	Description
***CSR Selection**	Select an option.
***Common Name**	Common name is one of the key values of the Certificate Signing Request (CSR) to be present on the certificate. For example, <appviewx>. **Note:** No special characters are allowed except period (.), hyphen (-), and underscore (_).
Subject Alternative Name	Select the alternative subject name from the dropdown list. You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. **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 is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Field	Description
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present on the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
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 matches with the Challenge Password.
***Hash Function**	The hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***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: Fields marked with red asterisk (*) symbol are mandatory.

5. In the **Attachments** section, enter the details as follows:

Field Description for 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 to upload a file.

6. Click **Add** to generate the CSR and add it to the intended group.

Submitting CSR to Certificate Authority

After you have generated a CSR, you must submit it to the respective certificate authority (CA) for signing.

To submit CSR to CA:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. On the Certificate list view, locate the CSR you generated and click the Common Name of the certificate.

   The certificate topology screen opens.
3. Add a CA connector to the certificate topology as explained in the Section, Add Certificate Authority Connector to Certificate.
4. Click **Submit** to trigger the request.

   Once the submit action is triggered, the Submit popup window appears. Add comments if needed, and then click **Yes.** If the approval required option is enabled in CA Policy, the request goes to Approve and Implementation stages.
5. Click **Approve**.
6. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.
7. Enter the comments in the field.
8. Click **Yes**.
   Once approved, you can see the Implement option in the holistic view.

9. Click **Implement.**

   The **Implement** pop-up window appears.

   - Click the **Schedule later** button if the workflow request has to be implemented automatically in the future.

10. Enter the comments in the field.
11. Click **Yes**.
    CSR Submission to CA is in progress.
12. Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

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

    If auto-approval disabled in the targeted CA, the user has to be logged into CA and approve the request.

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

Downloading CSR

To download a certificate signing request (CSR) for a certificate:

From holistic view:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. From **Certificate Inventory,** click **Server** or **Code Signing Certificate.**
3. On the certificate list view, click the **Common Name** of the certificate to view the topology.
4. Hover over (**More**) icon on the certificate and click **Download CSR**.

> **Note:** Alternatively, you can go to **Certificate Inventory** and select the check box against the certificate name you want to download CSR and click **Actions > Download CSR** from the command bar.

Suspending Certificate

If you have the necessary permission, you can suspend a certificate. As soon as the certificate is suspended, it is revoked. The suspended certificates are listed on the Certificate Revocation List (CRL) maintained by each certificate authority.

To suspend a certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Switch to the **List** toggle button on the top right corner of the page.
3. Click **Server, Client,** or **Device** tab depending on the type of certificate you want to suspend.
4. In the **Common Name** column certificate list, select the certificate that you want to suspend.
   The certificate topology appears on the screen.
5. In the **Comments** field, enter the reason for suspending the certificate.
6. Click **Yes.**

Changing Status of Certificate

Before changing the status of a certificate, the user should plan for the impact that might have on existing work orders.

To change the status of a certificate:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click **CA Switch** from **Certificate Action** and select the type of certificate for which you want to change status.
3. On the **Change Status** pop-up screen that appears, select **Managed** (to create, renew, or revoke actions on those certificates) or **Monitored** (to only alert) from the Change status to dropdown.
4. [Recommended] In the **Comments** field, enter the reason for changing the status.
5. Click **Yes.**

What to do next:

Note: Alternatively, you can go to **Certificate Inventory** and select the check box against the certificate name you want to renew and click **Actions > Change Status** from the command bar.

Deleting Certificate

To delete a certificate or policy:

1. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
2. Click the type of certificate you want to delete from **Certificate Inventory** list.
3. From the certificates inventory, select the check box beside the certificate or policy you want to delete.
4. Click **Actions,** and select **Delete** from the dropdown list.

> **Note:** This functionality is available only for server certificates and policy.

5. Click **Yes** to confirm.
   The certificate or policy is then removed from the list and deleted from the AppViewX system.

Revocation Check - OCSP

Certificate authorities use Online Certificate Status Protocol (OCSP) to obtain the revocation status of x.509 digital certificates. When a user requests the validity of a certificate, an OCSP request is sent to an OCSP server to check the specific certificate with a trusted certificate authority. The OCSP server then sends a *good, revoked, or unknown* response.

Prerequisites

- OCSP URL must be published in the AIA field of the certificate with the AppViewX OCSP server URL.
- **Plugins required:** OCSP Server and OCSP Generator must be deployed for OCSP to work.

You can then proceed to select one or more certificates from the inventory and click **Actions > Revocation Check** to perform revocation validation. Once validated, the certificate status is updated in the color code of the Common Name column.

Chapter 6: Windows Auto-Enrollment Proxy

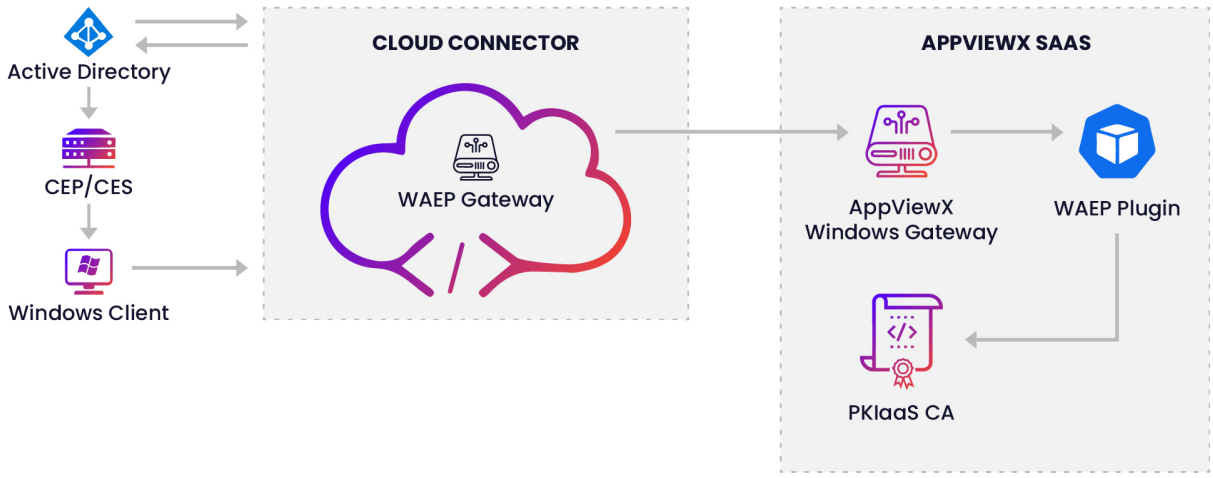
What is Windows Auto-Enrollment Proxy?

Windows Auto-Enrollment Proxy (WAEP) is a component developed by AppViewX that helps users/devices connected to the Microsoft domain to enroll or migrate from their existing certificates automatically to AppViewX PKIaaS.

Salient Features

- Use the Lift & Shift feature to migrate Microsoft Windows-issued certificates easily to Cloud.
- Control the number of duplicate certificates issued.
- View the WAEP dashboard for the enrollment status of all certificates.

How WAEP works



1. The Certificate Enrollment Policy (CEP) server publishes the certificate template information, the CA information, and the enrollment link to all Windows clients and users.
2. The Windows client sends the request directly to the Cloud Connector (CC) via Certificate Enrollment Web Service (CES) for enrolling a certificate.
3. The CC queries for the agent settings along with other details such as AD configuration and global catalog server configuration. With the CC IP address and the port making a unique combination, there will be only one agent settings based on this combination of business keys.
4. The WAEP module then fires an LDAP query using the agent settings fetched. It fetches the details from the global catalog servers and constructs the request.
5. The CC then forwards the CSR payload to the PKIaaS for issuing a signed certificate.
6. The signed response is then routed back to the client through the CC.

Prerequisites

1. Establish trust for all entities in the environment.
   - Trust anchor certificates to be published to all domain members from group policy -OR- you can run the following commands from AD:
     - For issuing CA:

       ```
       certutil –dspublish –f <PathToCertFile.cer> SubCA
       ```

     - For root CA:

       ```
       certutil –dspublish –f <PathToCertFile.cer> RootCA
       ```

2. Set up TLS connection in the AppViewX CC server.

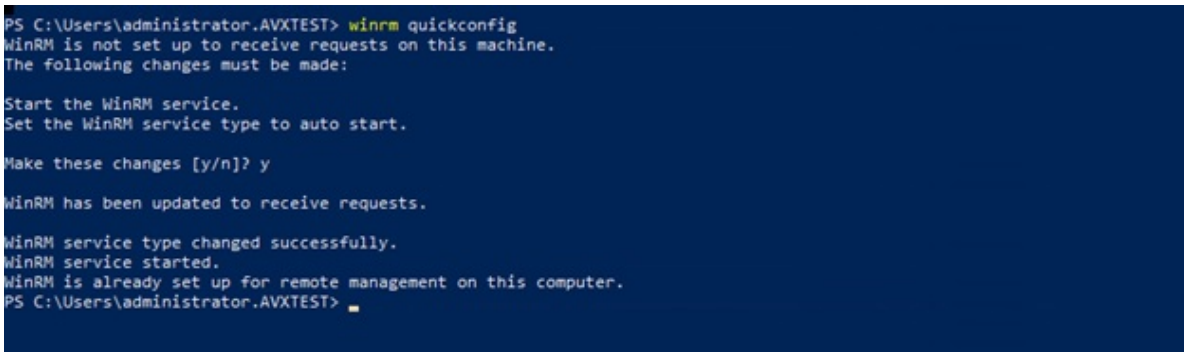
- Enable the ACME service during the setup of CC for WAEP to function.
- The AppViewX CC server must be configured with certificate TLS to handle connection between Windows clients and the CC server.
- The AppViewX CC server must be made available to use the Lift & Shift feature for SaaS deployments.

  The CC ships with a self-signed certificate but ensure to replace the default self-signed certificate with a signed certificate. You can choose to have the signed certificate from a trusted third-party CA depending on your organizational policies.

3. Ensure there is Internet access or provision to download the PKI CRL.
4. Create a service account: A domain service account that belongs to the Cert Publishers group and with access delegated for the policy server and the AD server. The service account must be a part of the local admin group in CEP/CES server. See Creating Service Account.
5. For the Lift & Shift feature to work, enable the WinRM service on the policy server (CEP/CES) and the AD servers configured in WAEP for global fetch configuration and publication of templates.

   To configure WinRM service (Applicable only for automatic upload of templates):

   a. Run *winrm quickconfig* on the PowerShell window as an administrator.
   b. Type *y* when prompted to start the WinRM service.

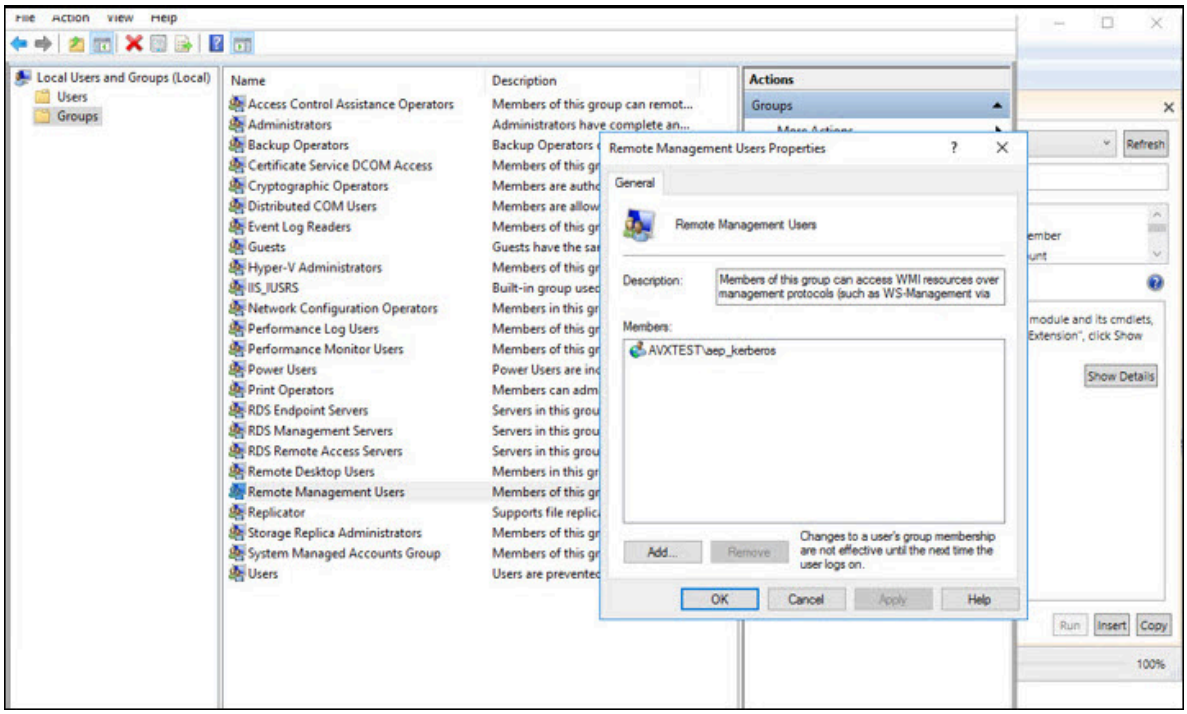


   The service account, for example: <waep_kerberos>, must be part of the **Remote Management Users** group.

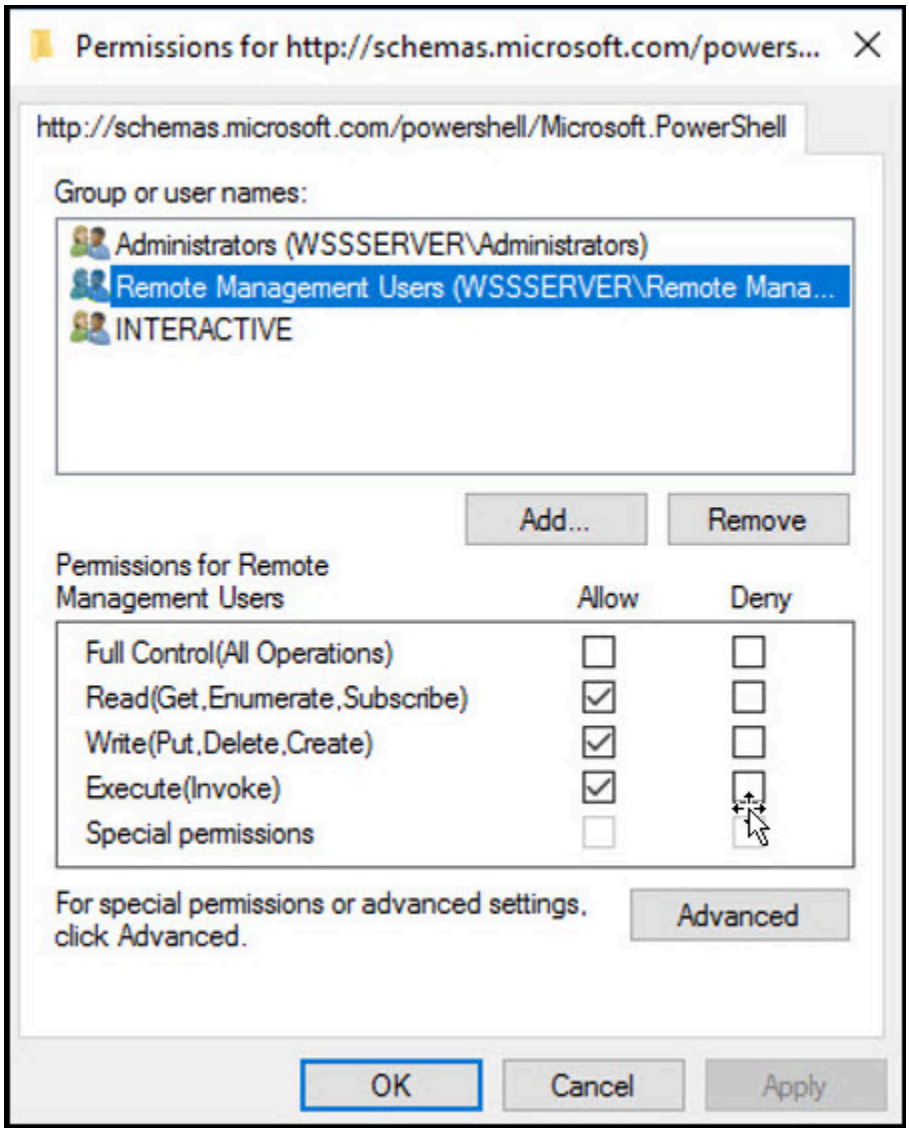
   c. To validate if the **Remote Management Users** group has permissions to execute the scripts, run the below command on the AD server and the policy server:

```
PS C:\Users\administrator.AVXTEST> Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell
```

   d. Add the service account (aep_kerberos) to the **Remote Management Users** group.



e. Assign **Read,Write, and Execute** permissions to the group.



f. Enable Credential Security Support Provider (CredSSP) authentication on the policy server (CEP/CES) and the AD servers by running the following command:

```
Enable-WSManCredSSP -Role Server
```

g. Once the server role is enabled, ensure the parameters, **Kerberos, Negotiate, CredSSP,** are set to **true** and **CbtHardingLevel** is set to **Relaxed** as shown.

```
cfg                 : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
lang                : en-US
Basic               : false
Kerberos            : true
Negotiate           : true
Certificate         : false
CredSSP             : true
CbtHardeningLevel   : Relaxed
```

h. Repeat the process to enable CredSSP authentication on the client side by running the following command:

```
PS C:\Users\Administrator> Enable-WSManCredSSP -Role Client
```

Note:

- Ensure that the parameters, **Kerberos, Negotiate, CredSSP,** are set to *true* and **CbtHardingLevel** is set to *Relaxed.*
- If Kerberos is not set to *true,* then run the following command:

```
winrm set winrm/config/Service/auth '@{Kerberos="true"}'
```

- If CredSSP is not set to *true,* then run the following command:

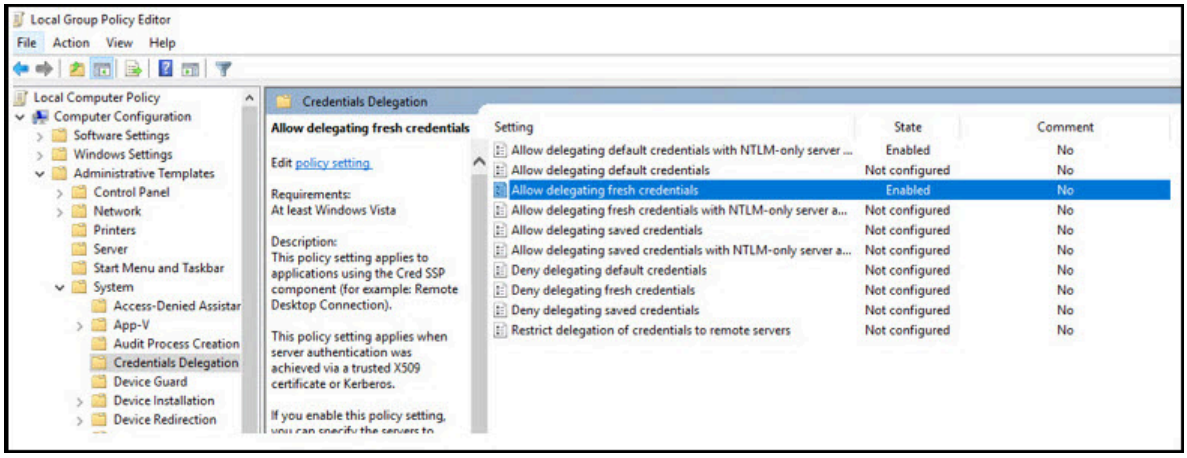
```
winrm set winrm/config/Service/auth '@{CredSSP="true"}'
```

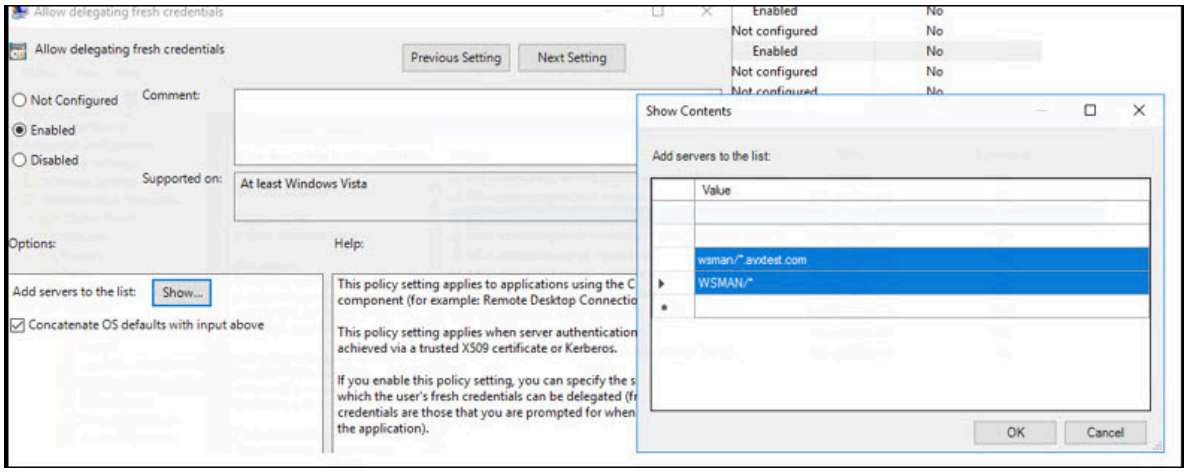
i. Add the policy server to the trusted hosts list by running the following command:

```
winrm s winrm/config/client '@{TrustedHosts="CSSSERVER"}'
```

Note: Here CSSSERVER is the hostname for policy server. Repeat the step for the AD server.

j. Allow credential delegation via the group policy editor.

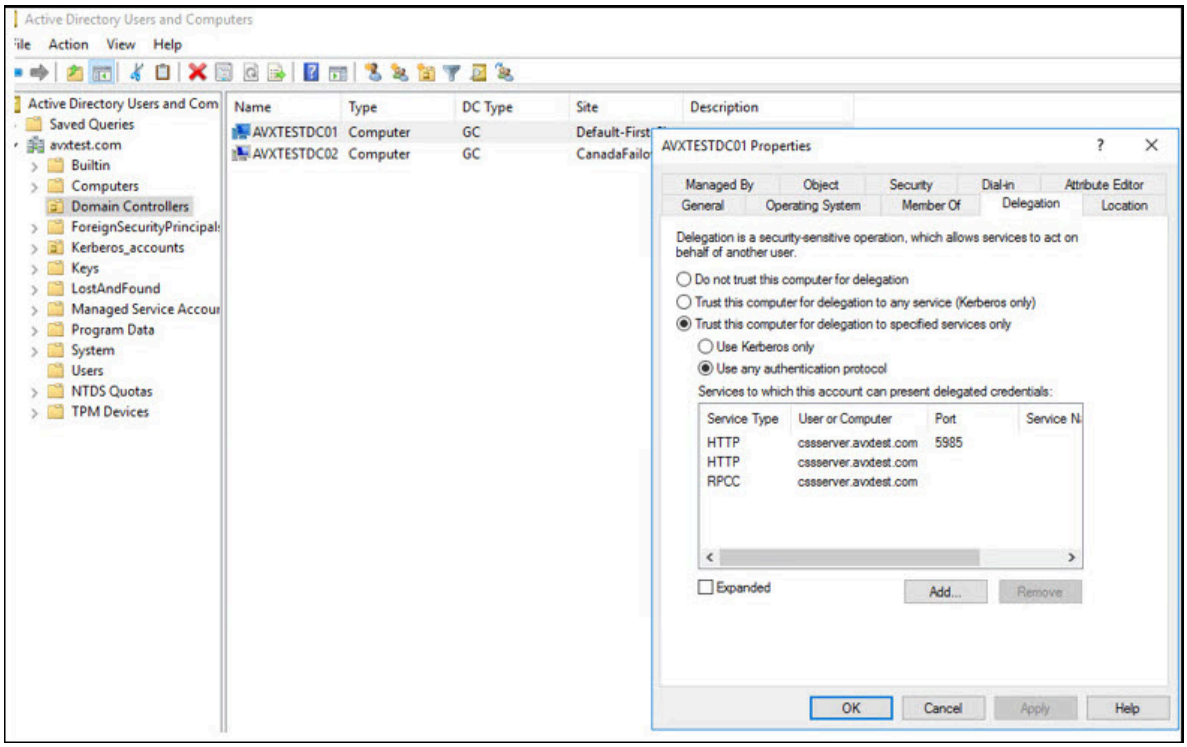




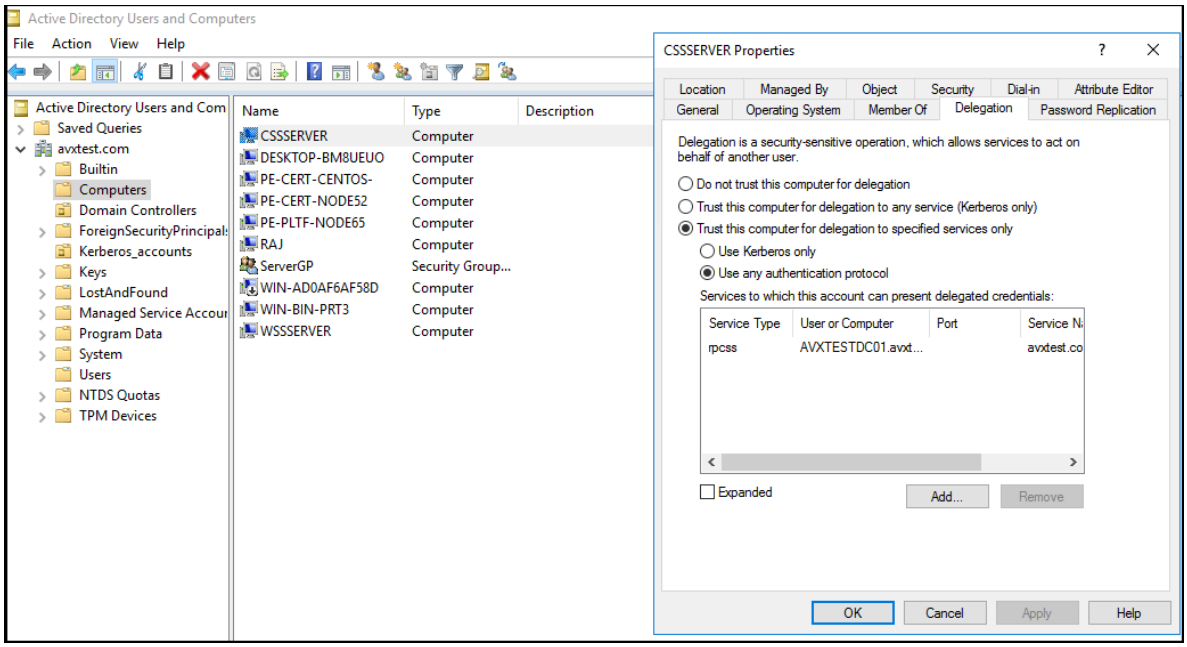
Note: Replace ***.avxtest.com** with your domain name.

Repeat the same procedure for the remote server, which would be the policy server.

k. Ensure that delegation is provided to the AD server that will be used for the connection.



Similarly allow delegation for the policy server as shown:



Note: For more information, refer to https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_troubleshooting?view=powershell-7.3

Server Requirements

The following lists the required servers, clients, and applications used in this guide.

Server Requirements

Server/Client	Requirements
Microsoft Active Directory Domain Services Server	Operating System: • Windows 2012 Server R2, Windows 2016 Server and later Server Roles: • Active Directory Domain Services • Service Accounts
Microsoft CEP/CES Server	Operating System: • Windows 2016 Server (Recommended) or later

Server Requirements (continued)

Server/Client	Requirements

	Server Roles:
	
	• Active Directory Certificate Services
	  • Certificate Authority
	  • Certificate Enrollment Web Service
	  • Certificate Enrollment Policy Web Service
	
	• IIS

WAEP Dependencies	• Enable the ACME service during the setup of CC for WAEP to function.
	• Replace the default certificate with a signed certificate on CC.
	• Internet access or provision to download the PKI CRL.
	• Windows Service account
	
	Trust anchor certificates to be published to all domain members from group policy -OR- you can run the following commands from AD:
	• For issuing CA: run
	`certutil –dspublish –f <PathToCertFile.cer> SubCA`
	• For root CA: run
	`certutil –dspublish –f <PathToCertFile.cer> RootCA`
	• Configure WinRM to use Lift & Shift feature

Microsoft Windows Client	Operating System: • Windows 10 or later

Cloud Connector Specifications	• Operating System
	  • Ubuntu version 20.04
	  • CentOS version 7.7 and 7.9
	• 4 vCPU
	• 8GB memory

Server Requirements (continued)

Server/Client	Requirements
	• 16GB disk space • x86 64-bit architecture

Step 1: Setting up Active Directory for WAEP

This section describes all the steps required for creating and setting up Active Directory for WAEP and its dependent components:

- Roles and Permissions
- List of Commands
- Creating Service Account
- Adding Hosts to DNS Service

Roles and Permissions

The following server roles must be installed or configured; all the related actions described below must be executed by a member of the Domain/Enterprise Administrator group:

- Active Directory Domain Services (ADDS) administrator
- Active Directory Certificate Services (ADCS) administrator
- Certificate Enrollment Policy Web Service (CEP) administrator
- Certificate Enrollment Web Service (CES) administrator

List of Commands

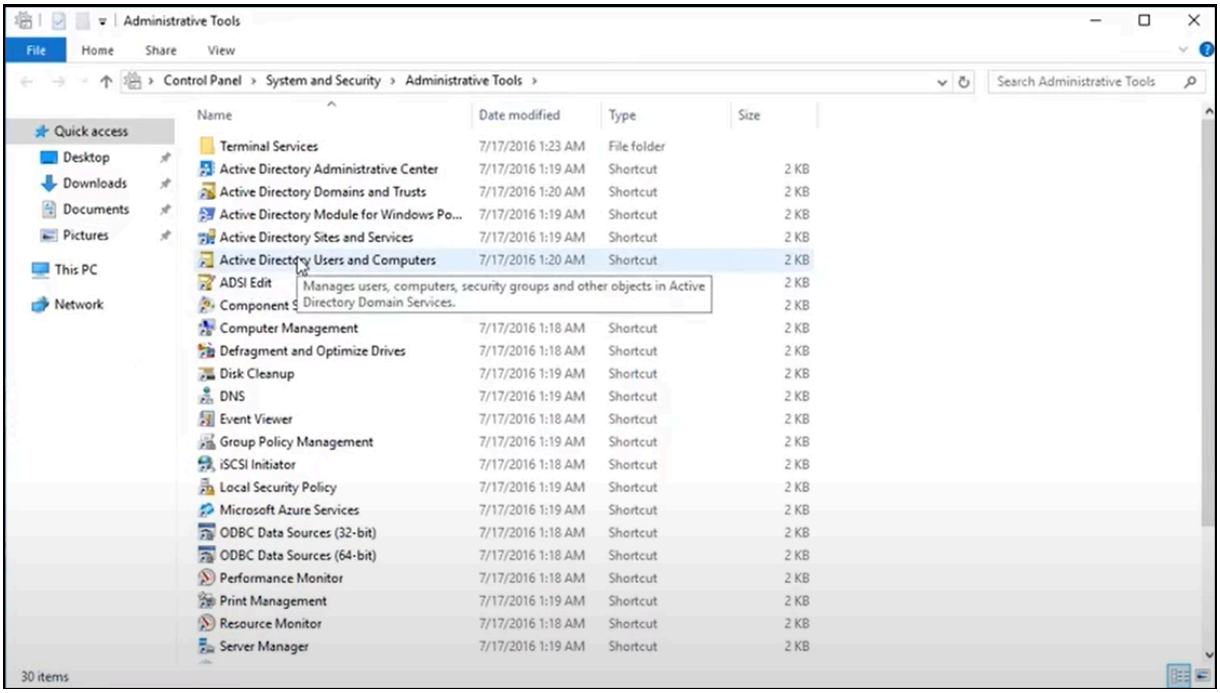
Command	Description
`Certutil -adtemplate -v | select-string distinguishedName,msPKI-Cert-Template-OID,pKIExpirationPeriod,pKIOverlapPeriod`	This command fetches AD templates from AD server during automatic fetch in WAEP configuration.
`(Get-ADForest).Domains | %{ Get-ADDomainController -Filter * -Server $_ } | Where-Object { $_.IsGlobalCatalog -eq 'True'}`	This command is executed in the policy server to fetch Global Catalog from AD. This is executed

Command	Description
	during automatic global catalog fetch on the WAEP Settings page.

Creating Service Account

To create a service account:

1. Open the **Server Manager** by going to **Start Menu > Server Manager.**
2. Select **Tools > Activate Directory Users and Computers.**



3. Go to **<yourcompany.com>** and select **Users.**
4. Click **Action > New > User** and add a service account with user login name (waep-service or a name of your choice) and set the password to never expires. This account will be used for Certificate Enrollment Services and for WAEP to make a bind to AD.
5. Add the account (waep-service) as a member of the Cert Publishers group.

Note: Use the single service account if performing this installation with a single service account on a single host.

Adding Hosts to DNS Service

Create a new host type for the CEP/CES server on the DNS server.

Step 2: Installing and Configuring Microsoft CA and CEP/CES Roles

The following sections describe how to install and configure the Microsoft Certification Authority and CEP/CES roles:

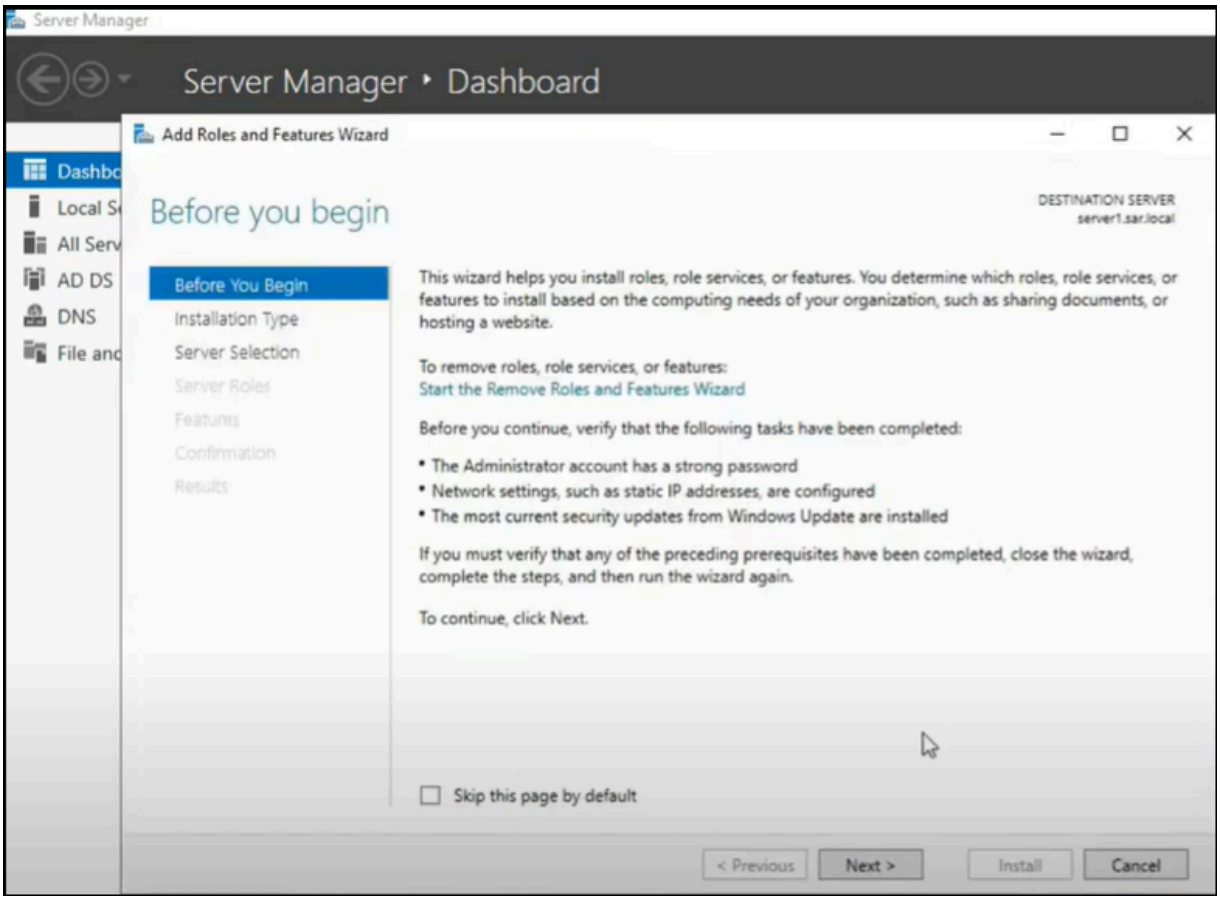
- Installing Active Directory Certificate Services
- Configuring Active Directory Certificate Services
- Installing Certificate Enrollment Services
- Configuring Certificate Templates
- Configuring Certificate Enrollment Services
- Configuring IIS
- Setting up Service Account

Installing Active Directory Certificate Services

To install Active Directory Certificate Services (ADCS):

1. Assign a static IP address for this host.
2. Give an appropriate computer name for the host, for example: <winaepserver>.
3. Add the host member of the domain (yourcompany.com) using an account that belongs to the Domain/Enterprise Admin group.
4. Open the **Server Manager.**
5. Click **Add roles and features**.

   The **Add Roles and Features Wizard** opens.

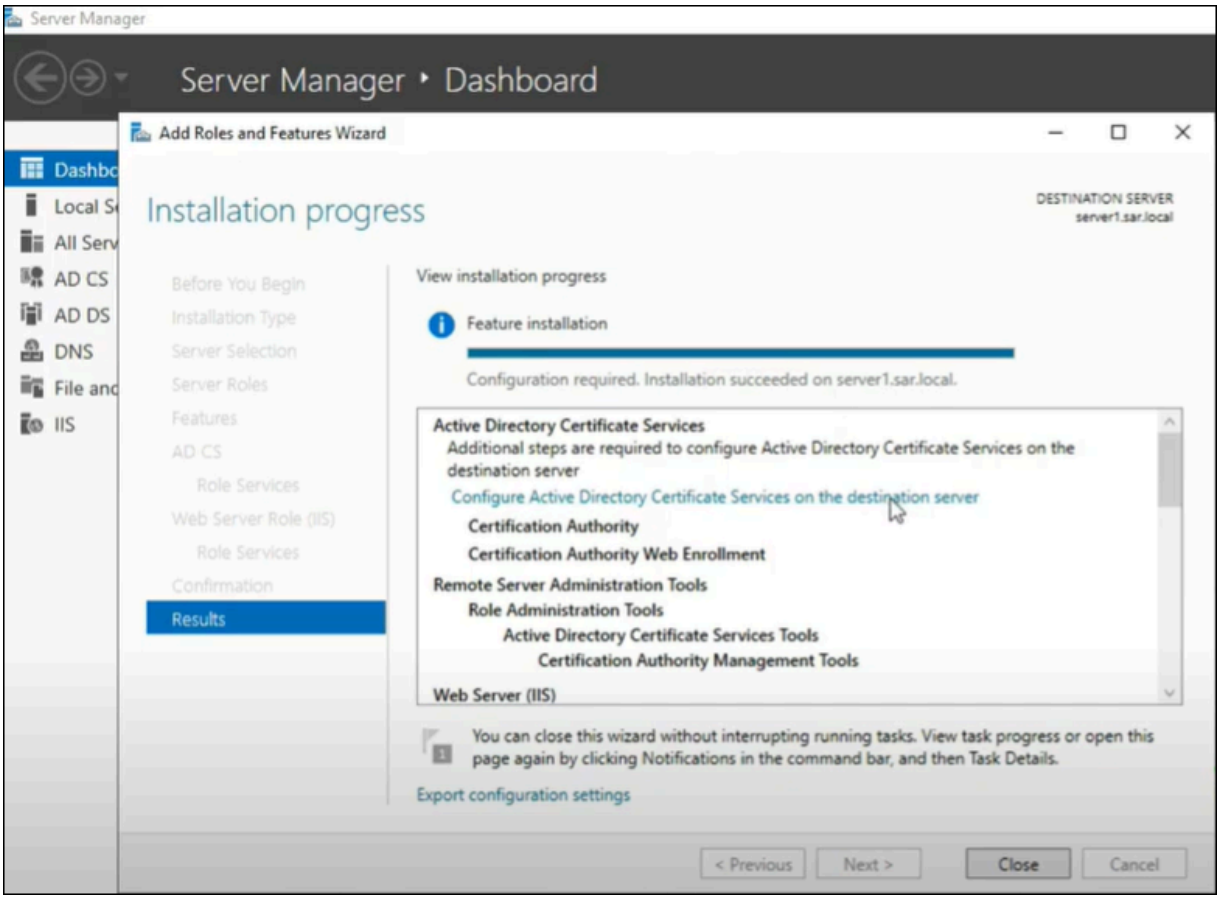


6. Click **Next.**
7. In **Installation Type,** select **Role-based or feature-based installation,** and click **Next.**
8. In **Server Selection,** select **Select a server from the server pool,** and click **Next.**
9. In **Server Roles,** select **Active Directory Certificate Services.**
10. Click **Add Features** when prompted to add required features.
11. Keep the default selections and keep clicking **Next** until you reach the **Role Services** page.
12. Select **Certification Authority** and **Certification Authority Web Enrollment.**
13. In the popup that appears, click **Add Features** to add IIS and its corresponding features.
14. Click **Next** until you reach the **Confirmation** page, and click **Install.**
15. Click **Close** when installation is complete.

Configuring Active Directory Certificate Services

To configure Active Directory Certificate Services:

1. Click **Configure Active Directory Certificate Services on the destination server** in the Server Manager notifications.



2. Click **Change** besides the **Credentials** box.
3. Enter an account that belongs to the Domain/Enterprise Admin group, click **OK,** and then click **Next.**
4. Configure **Certification Authority** and **Certification Authority Web Enrollment** by selecting role services, and click **Next.**
5. Select **Enterprise CA,** and click **Next.**
6. Select **Root CA,** and click **Next.**
7. Select **Create a new private key** and click **Next.**
8. Set the Cryptography provider to **RSA#Microsoft Software Key Storage Provider.**
9. Set the Key Length to **4096** bits.
10. Set the hash algorithm to **SHA256,** and click **Next.**
11. Enter a unique name for the CA such as <MSCA-Proxy> and then click **Next.**
12. Set the validity period **25** years.
13. Configure the location for the certificate database and certificate database logs.
14. Click **Next.**
15. Click **Configure,** and click **Close.**

Installing Certificate Enrollment Services

To install the Certificate Enrollment Services on the CEP/CES server:

1. Open the **Server Manager.**
2. Click **Add Roles and Features,** and click **Next.**
3. Select **Role-based or feature-based installation,** and click **Next.**
4. Choose **Select a server from the server pool,** and click **Next.**
5. Expand the **Active Directory Certificate Services,** select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service,** and click **Next.**
6. Proceed until the **Confirmation** page, and click **Install.**
7. Reboot the server after the roles have been installed.

Configuring Certificate Templates

Note: This section is applicable only if you choose to manually upload the templates on AppViewX.

To configure certificate templates on ADCS:

1. Type `certsrv.msc` in the command prompt to open the Certificate Authority Manager.
2. Expand the selection for your CA.
3. Right-click **Certificate Templates** and click **Manage.**
4. Ignore the create the object identifier list warning and click **OK,** and then click **Refresh.**
5. Right-click the **Computer** template, select **Duplicate Template** and specify the following:
   a. Under **Compatibility Settings,** specify Certification Authority **= Windows Server 2012** and Certificate recipient **=Windows 8/Windows Server 2012.**
   b. Click the **General** tab, and change the Template display name to **AppViewX_computerautoenroll** or any name of your choice.
   c. Click the **Security** tab, and give Domain Computers permissions to **Enroll** and **Autoenroll.**
   d. Select the **Subject Name** tab, and change the Subject name format to DNS Name.
   e. Select **DNS Name,** or **SPN,** or **both** per requirement in the subject alternative name.
   f. Under the **Request Handling** tab, clear **Allow private key to be exported.**
   g. Click **OK** to go back to the template list.
6. Right-click the **User** template and select **Duplicate Template** and specify the following:

a. Under **Compatibility Settings,** specify Certification Authority **= Windows Server 2012** and Certificate recipient **= Windows 8/Windows Server 2012.**
b. Click the **General** tab, and change the Template display name to **AppViewX_userautoenroll** or any name of your choice.
c. Select the **Security** tab, and give Domain Users permissions to **Enroll** and **Autoenroll.**
d. Select the **Subject Name** tab, and change the Subject name format to **Common name.**
e. Clear **Include email name in subject name** and clear **Email name in the subject alternative name.**
f. Select **User principal name (UPN)** or **email** per requirement.
g. Under the **Request Handling** tab, clear **Allow private key to be exported.**
h. Click **OK** to go back to the template list and then close the **Certificate Templates Console** window.

7. Return to the Certificate Authority manager, right-click **Certificate Templates,** specify the following and then click **OK:**
   a. Select **New > Certificate Template to Issue.**
   b. Select the new templates created.
8. Delete templates that are not required from the **Certificate Templates** section except for the new templates created.

   To force existing users to enroll from the new templates ensure to supersede the respective old templates to the new ones. For example, if the old user template is UserV1 include this under the superseded section of the new template **AppViewX_userautoenroll.**

Configuring Certificate Enrollment Services

To configure Certificate Enrollment Services on the CEP/CES server:

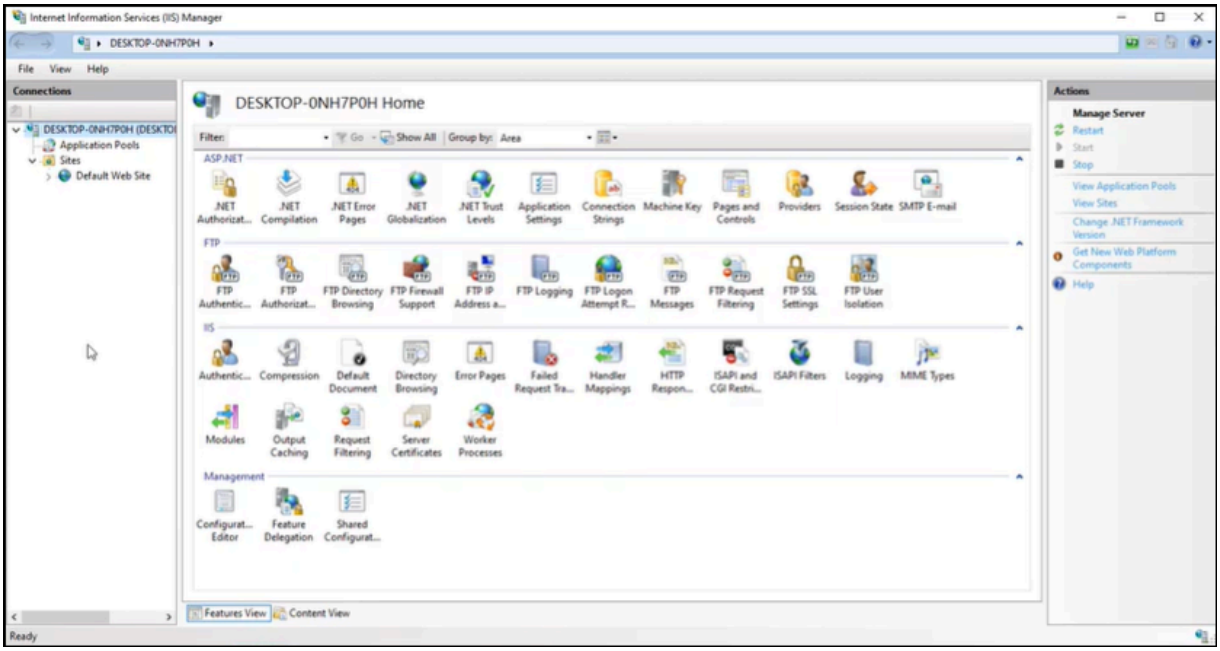
1. Click the new task shown in the Server Manager notifications: **Configure Active Directory Certificate Services on the destination server.**
2. In the credentials panel shown, click **Change.**
3. Enter an account that belongs to the Domain/Enterprise Admin group, click **OK** and then click **Next.**
4. Select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service** and click **Next.**
5. Select the CA Name.
6. Click **Select** and select the Microsoft CA that will be issuing the certificates using certificate enrollment web service, click **OK** and then click **Next.**
7. For CES authentication type, select **Windows Integrated Authentication** and then click **Next.**
8. For CES service account, select **Specify service account** and then click **Select.**

9. Specify the service account <waep-service> and credentials and ensure to use the single service account created if using a single service account.
10. Click **OK** and then click **Next.**
11. For CEP authentication type, select **Windows Integrated Authentication** and then click **Next.**
12. For Certificate authentication, select **Choose and assign a certificate for SSL later** and click **Next.**
13. Review the confirmation page and click **Configure.**
14. When the installation completes, click **Close.**

Configuring IIS

To configure the Internet Information Services (IIS) on ADCS:

1. Type `InetMgr.exe` in the command prompt to open the Internet Information Services (IIS) Manager.
2. Click your server name on the left-hand side.
3. Expand the selection for your server and click **Application Pools.**



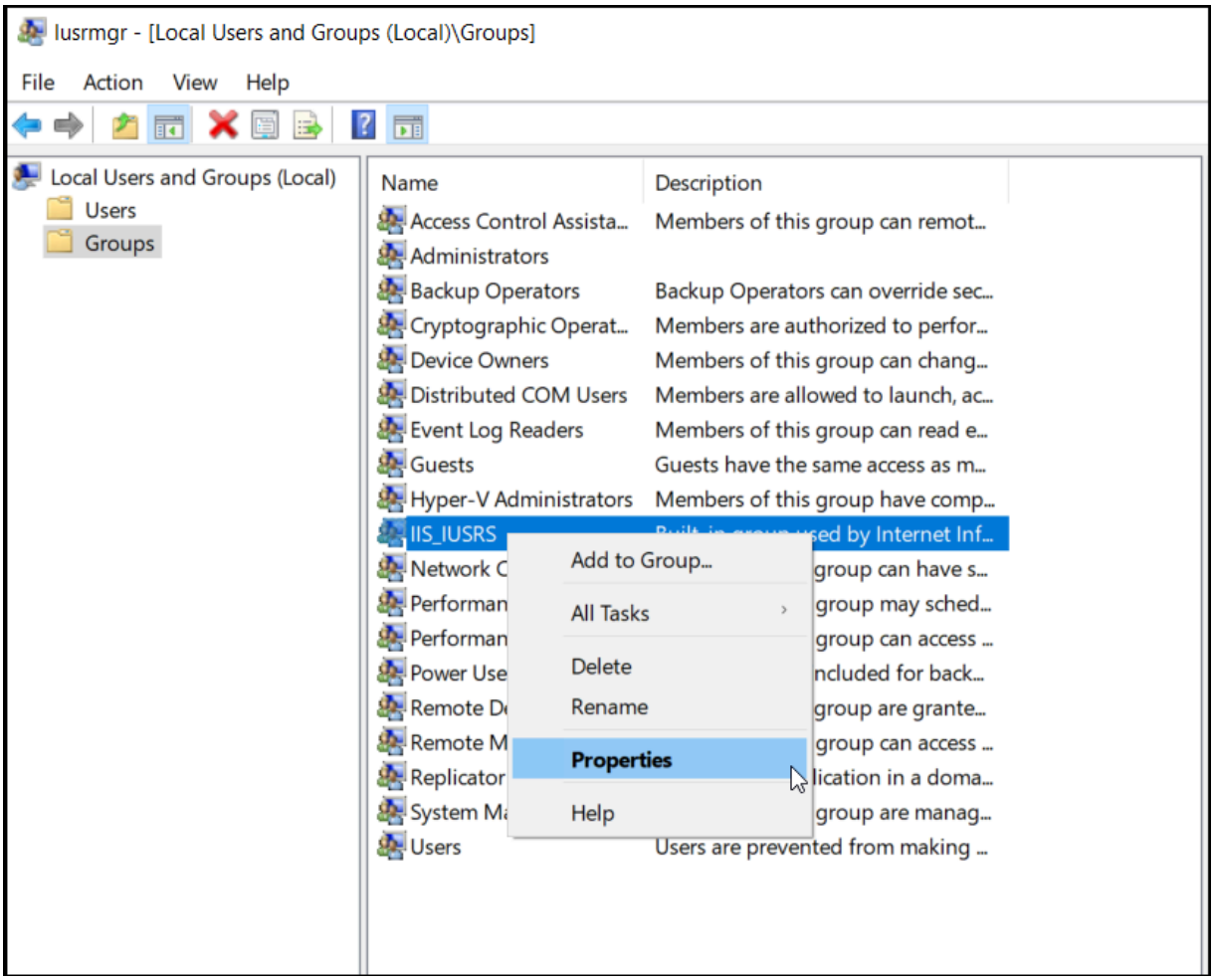
4. Right-click **WSEnrollmentPolicyServer,** and select **Advanced Settings.**
5. Edit **Identity.**
6. Select **Custom account** in the panel that appears, and click **Set.**
7. Enter the username and credentials for **<yourcompany\waep-service>.**
8. Click **OK** and expand **Sites** in the **Connection** menu on the left-hand side.
9. Click **Default Web Site** and then click **Bindings** on the right-hand side.
10. Edit the https site binding.

11. From **SSL certificate,** select the CS Server's SSL certificate **winaepserver.yourcompany.com,** click **OK** and then click **Close.**
12. Expand the **Default Web Site** option on the left-hand side.
13. Click **ADPolicyProvider_CEP_Kerberos** and open **Application Settings.**
14. Edit the entry name **FriendlyName** and set the value to **AppViewX_Enrollment.** This is a name that clients will see only when manually requesting certificates.
15. Click **Add** and create a new entry with the name **RetryIntervalMs** and value **300000.**
16. Click on the URI and copy the URI so that it can be used for group policy update.
17. Restart IIS by clicking on the server name and then click **Restart** on the right-hand side.

Setting up Service Account

To set up the service account on Active Directory Certificate Services:

1. Create Service Account as mentioned in the Section, **Create Service Account.**
2. Type `lusrmgr.msc` in the command prompt to open the **Local Users and Group** manager.
3. Click **Groups.**
4. Right-click the **IIS_IUSRS** group and select **Properties.**



5. Right-click the **Administrators** group and select **Properties.**
6. Click **Add,** and enter <YOURCOMPANY\waep-service> in the **Enter the object names to select** text box, and click **OK.**
7. Enter an account that belongs to the Domain/Enterprise Admin group, and click **OK.**
8. Open the command prompt with Admin permissions.
9. Set the service principal name for the service account by running the following command as admin:

```
setspn -s HTTP/<winaepserver or server name>.yourcompany.com <waep-service>
```

Make sure to replace the server **<FQDN>** and account names with your own configuration.

Note:

- If you are using a single service account and performing this installation on a single host (the waepserver host), ensure to run only the *setspn* command once.
- If you have a service account created that is part of the domain, then ensure that it has access to the Cert Publishers group and they are a member of the local admin group on the CEP/CES or policy server.

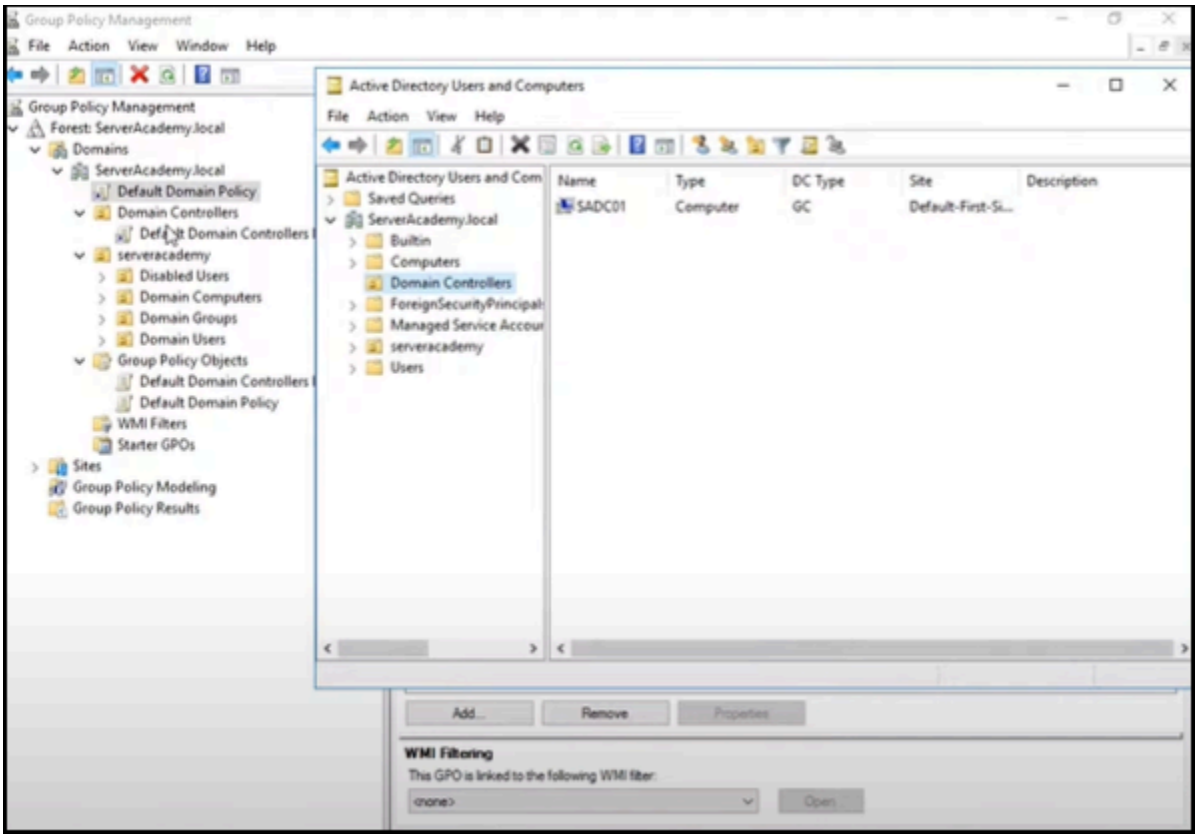
Step 3: Validating Configuration

The following sections describe how to validate the configuration:

Configuring Group Policies on AD Server

To configure group policies on the AD server:

1. Open the **Group Policy Management** console.
2. Expand your domain forest > Domains > your domain name, and select **Default Domain Policy.**



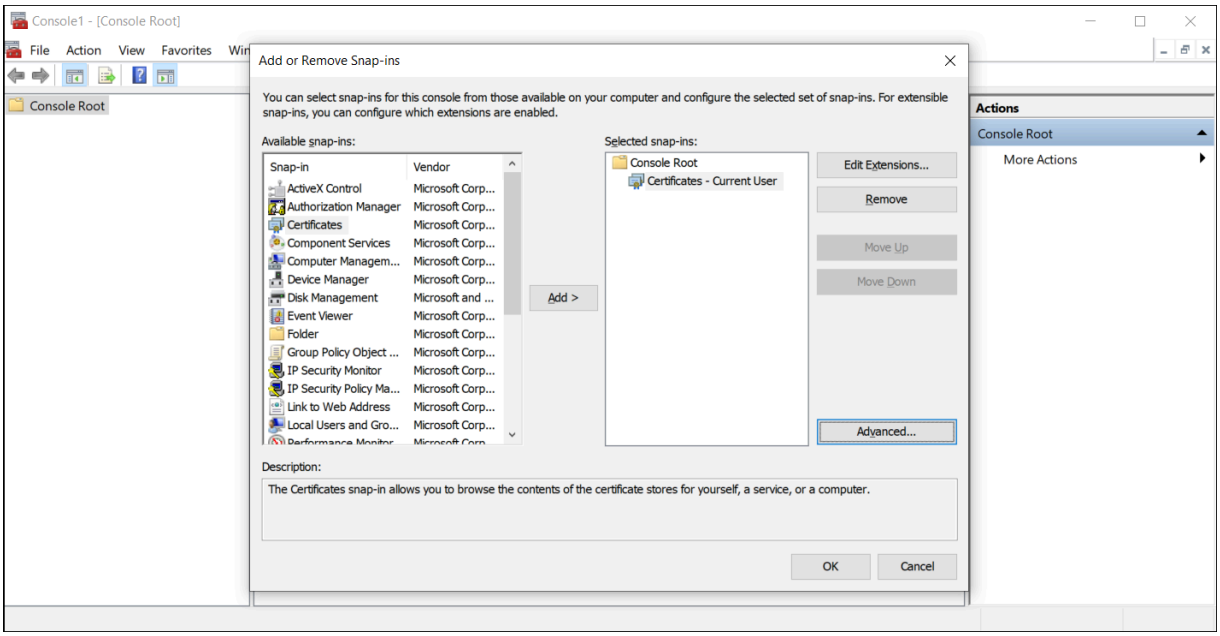
3. Right-click **Default Domain Policy** and select **Edit.**
4. Expand **Computer Configuration,** and select **Policies > Windows Settings > Security Settings > Public Key Policies.**
5. Edit **Certificate Services Client – Auto-Enrollment** according to the following and then click **OK.**
   a. Change **Configuration Model** to *Enabled*.
   b. Select **Update certificates that use certificate templates.**
6. Expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.**
7. Edit **Certificate Services Client – Auto-Enrollment** according to the following and then click **OK.**
   a. Change **Configuration Model** to *Enabled*.
   b. Select **Update certificates that use certificate templates.**

[Optional] Testing Auto-Enrollment

Do the following steps on the Windows Client machine to ensure auto-enrollment policy works:

1. Add the Windows Client host member of the domain **(yourcompany.com).**
2. Log in as user member of the **Domain Admins** group.

3. Type `mmc.exe` in the Run command to open the Microsoft Management Console.
4. Click **File > Add/Remove Snap-in** and select **certificates** for both **user** and **local computer.**



5. Verify that the user certificate was generated (Current User/ Personal/ Certificates).

   Make sure that the user certificate in the personal store is generated by the Windows CA using your duplicated template.

6. Verify that the computer certificate was generated. (Local Computer/ Personal/ Certificates requires Admin privileges to check the local computer certificate store.)

   Make sure that the computer certificate in the personal store is generated by the Windows CA using your duplicated template.

Step 4: Configure Windows Auto-Enrollment Proxy

Prerequisite

- **Generate CSV file (Applicable only for manual upload of templates)**

To generate CSV file:

1. Run **Windows PowerShell.**
2. To extract information of the certificate name, certificate template OID, validity period, and renewal period from the templates published on the ADCS server, run the command on the ADCS server:

```
Certutil -adtemplate -v | select-string distinguishedName,msPKI-Cert-Template-OID,pKIExpirationPeriod,pKIOverlapPeriod
```

3. Copy the certificate name, certificate template OID, validity period, and renewal period for **Computer_Auto_enrollment** template and **User_autoenrollment** template as shown:

```
distinguishedName = User
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.1
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = UserSignature
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.2
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = SmartcardUser
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.3
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = ClientAuth
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.4
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = SmartcardLogon
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.5
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = EFS
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.6
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = Administrator
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.7
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
distinguishedName = EFSRecovery
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.10260412.10212111.6898619.9178819.425121.217.1.8
```

Note: The **Computer_Auto_enrollment** template is used to enroll devices while the **User_autoenrollment** template is used to enroll users.

4. Open a spreadsheet and create three column headings:
   - **templateName:** In this column, add entries as **Computer_Auto_enrollment template** and **User_autoenrollment.**
   - **templateOID:** In this column, paste the OIDs copied in Step 3 against the respective template.
   - **validityPeriod:** In this column, enter the value as 365, which is the default value of the validity period.
   - **validityPeriodUnit:** In this column, enter the value as *days, weeks, months, or years*.
   - **renewalPeriod:** In this column, enter the value as 30, which is the default value of the renewal period.

Note: The renewal period must be less than the validity period.

   - **renewalPeriodUnit:** In this column, enter the value as *hours, days, weeks, months, or years*.
5. Once done, save the file in .xls, or .xlsx, or csv format.

To configure Windows auto-enrollment proxy:

1. Log on to the AppViewX application using your credentials.
2. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
3. Expand **Administration** menu and select **Auto Enrollment > WAEP.**
   The **Windows AEP** auto-enrollment page is displayed.
4. Click **+New Setting** to add a WAEP auto-enrollment request.
   The **Windows AEP : New Setting** page is displayed.
5. Enter the following fields:

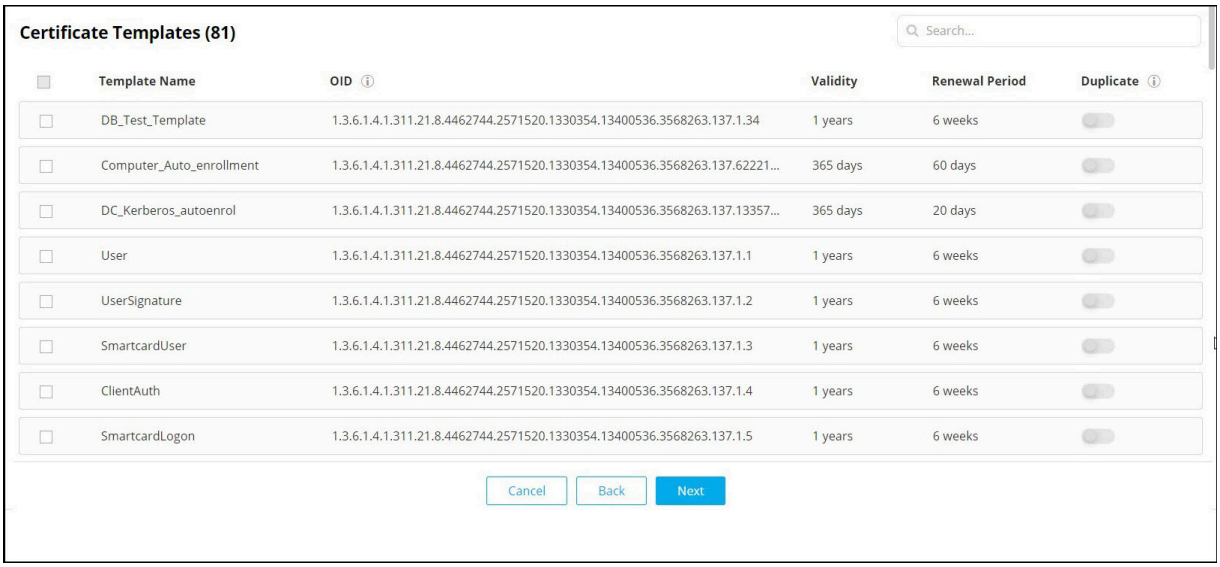
Field Description for Windows AEP : New Setting page

Field	Description
Endpoint Details	
***Name**	Provide a unique name for the WAEP setting. **Note:** Only alphanumeric and the following special characters are allowed: period (.), hyphen (-), and underscore (_). The name cannot begin with a special character.
***Cloud Connector**	Select the hostname based on the domain.
***Data Center**	Field is auto-populated based on the Cloud Connector hostname.
Active Directory Configuration	
***Policy Server**	Provide the IP address or the hostname of the **Certificate Enrollment Policy Web Service (CEP)/ Certificate Enrollment Web Service (CES)** or policy server used to execute the remote Windows PowerShell scripts.
***LDAP Server**	Select or enter the hostname of the AD/LDAP server.
***Service Account with Base**	Provide the service account created for bind. For example: cn=test_service, ou=Kerberos_accounts, dc=avxtest, dc=com
***Service Account Password**	Provide the service account password.

Field	Description
Active Directory Sync	This field is optional for manual import of templates.Enable this toggle button to fetch all the global catalog servers in your forest.
Global Catalog Configuration	
***Global Catalog Server IP**	If Active Directory sync is enabled, then this field lists all the global catalog servers in your forest as a dropdown list. To enable the auto features for on-premise environment, install the cloud connector as an additional component.
***Port**	Port 3268 is the MS default port for global catalog.
***LDAP Base DN**	If AD sync is enabled, the LDAP base DN is auto-populated based on the IP address of the global catalog server selected from the dropdown list.
Validate Account	Click the button to validate connection of the global catalog server with your service account credentials. If the validation is successful, you see *Success* displayed next to the button. If it fails, then check the service account credentials, or permissions to global catalog server, or verify the global catalog server IP and try again.
Import Templates	
***Type**	By default, **Manual** is selected. It is recommended that you select the **Auto** option to automatically fetch your templates from your AD. If you have selected **Manual,** then drag and drop your template that you created or browse to the location it is saved.
Fetch Templates	The templates are fetched and populated in the **Certificate Templates** screen.

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

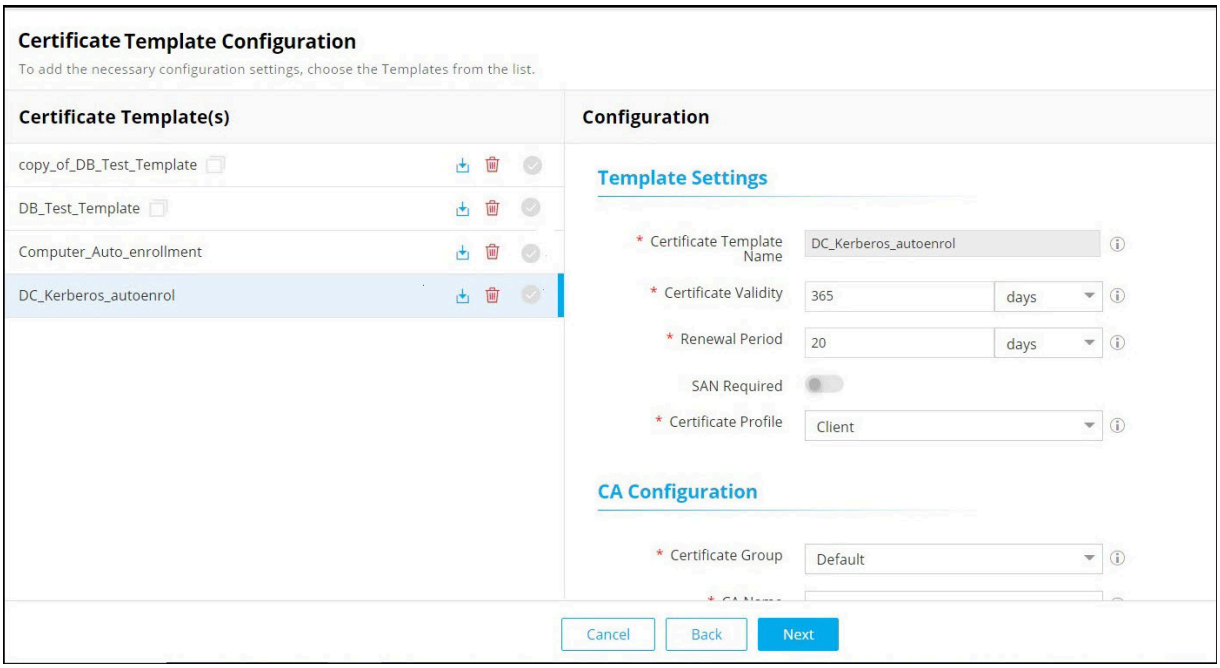
6. Click **Next.** A message that templates are imported successfully appears.
   The **Certificate Templates** page appears along with all the fetched templates along with the details populated in the table as shown.



7. Select the templates you want to configure and click **Next.**
   The **Certificate Templates Configuration** page appears.

> **Note:** [Applicable only if you have chosen automatic upload of templates] If you want to make a copy of an existing template, then select the checkbox against that template and slide the toggle button under the **Duplicate** column. The duplicated template name appears with the prefix: *copy_of_* along with the template name on the next page. For example, if you made a duplicate of the *DB_Test_Template* template, then the duplicate template appears with the name, *copy_of_DB_Test_Template*, which you can edit on the next page.

8. Click the template you want to configure and fill out the details in the **Configuration** page that appears on the RHS of the page.



9. Enter the following fields:

Field Description for Certificate Template Configuration page

Field	Description
Template Settings	
***Certificate Template Name**	Enter the name of the certificate template if you created a copy of it.
***Certificate Validity**	Enter the expiry time limit for certificates.
***Renewal Period**	Enter the renewal time limit for the template.
SAN Required	This is disabled by default.
Subject Alternative Names	This field appears only when you select the **SAN Required** checkbox. Select from the following values: • DNS • Email • User Principal Name • Service Principal Name **Note:** You can either choose DNS/Email or both, or customized SAN such as User Principal Name/Service Principal Name or

Field	Description
	both. For example, if you select DNS/Email or both, you cannot select User Principal Name/Service Principal Name and vice versa.
***Certificate Profile**	Select the profile configured to set the Key Usage and EKU. **Note:** This profile must match the Key Usage values and EKU as seen in the actual on-prem Microsoft template in case of manual fetch.
CA Configuration	
***Certificate Group**	Select the certificate group for managing the certificates.
***CA Name**	Select a CA for WAEP to communicate for certificate enrollment.
***CA Account**	The field values are listen only when account is added to CA settings.
***CA Certificate**	Select issuer certificate. It is recommended to select intermediate CA certificates to sign all the client certificates.
***Issuer Name**	Select the issuer name for the certificate.
***Issuer Location**	Select the issuer location for the certificate.
***CA Connector Name**	By default, this is **CA Connector.** If you created a CA connector manually, then provide that name here.

On completion, you get a message that the template is saved successfully and a blue tick mark appears across the configured template.

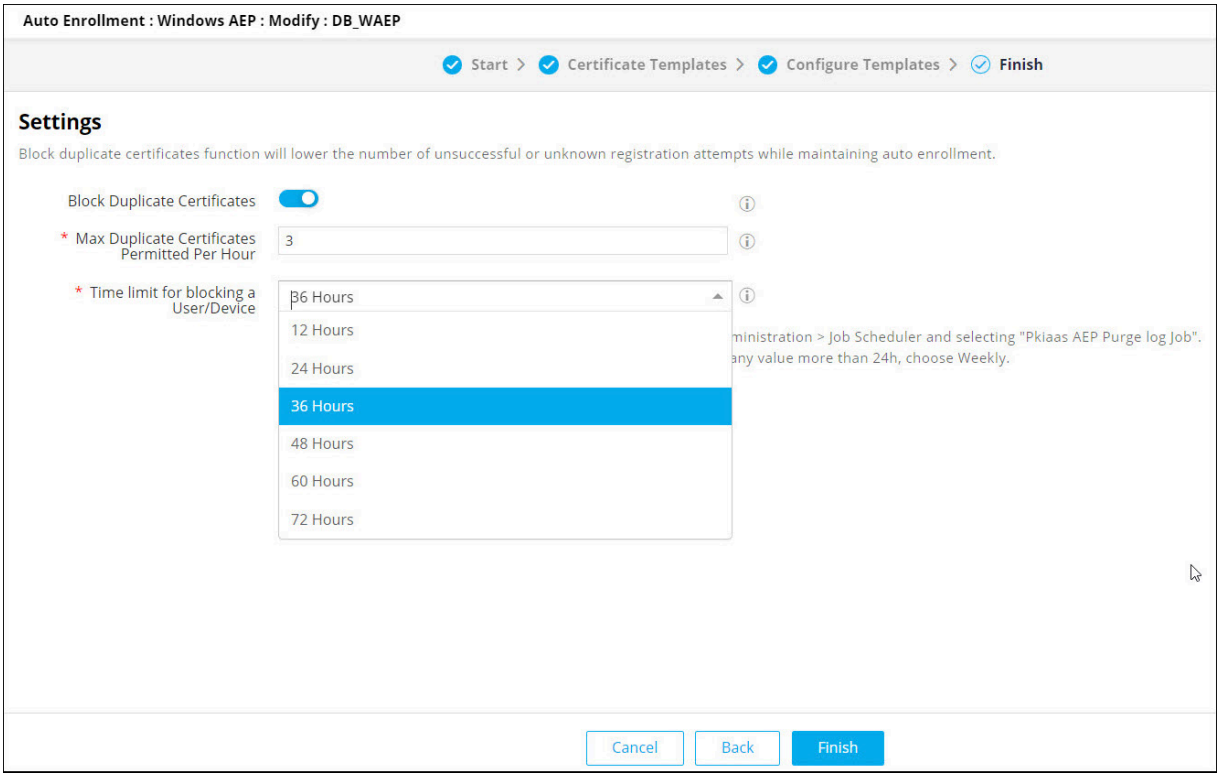
Note:

- You can select or clear the templates by going back to the previous page.
- You cannot click **Next** until all the selected templates are configured.
- Click the (**Download**) icon to download a selected template (appears only if you have chosen automatic upload of templates) or click the (**Delete**) to delete a selected template.

10. Click **Next.**

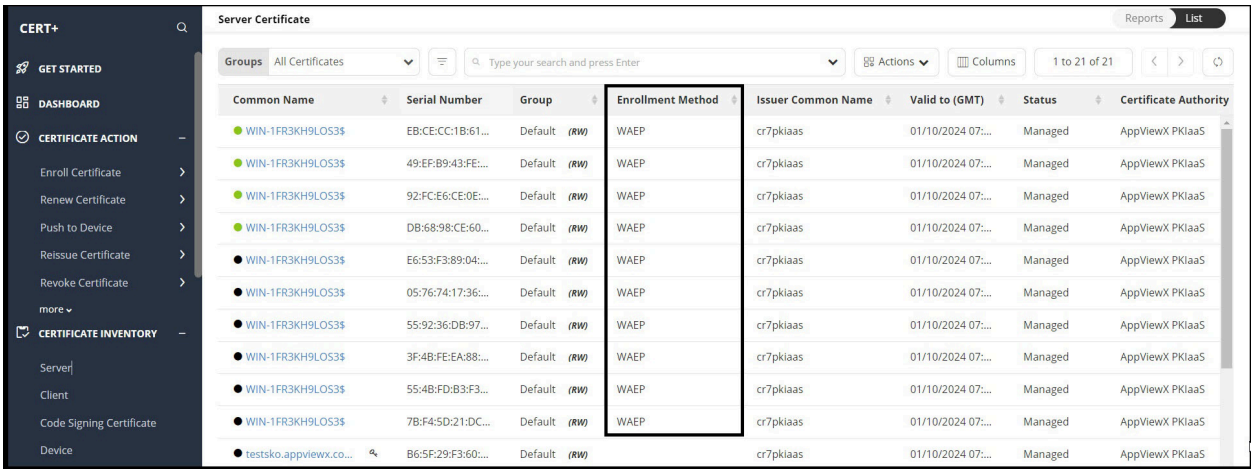
The **Settings** page appears. By default, the **Block Duplicate Certificates** toggle button is disabled. If you enable it, you can customize the values for blocking the maximum number of duplicate certificates in an hour and the time limit to block a user/device issuing the certificates.

Note: By default, the time limit for a user/device is 24h. If you change this value, ensure to update the **Occurrence Type** by navigating to **CERT+ > Administration > Job Scheduler** and selecting **Pkiaas AEP Purge log Job.** If you have set the time limit as 12h or 24h, then choose **Occurrence Type** as **Daily.** For values more than 24h, choose **Occurrence Type** as **Weekly.**



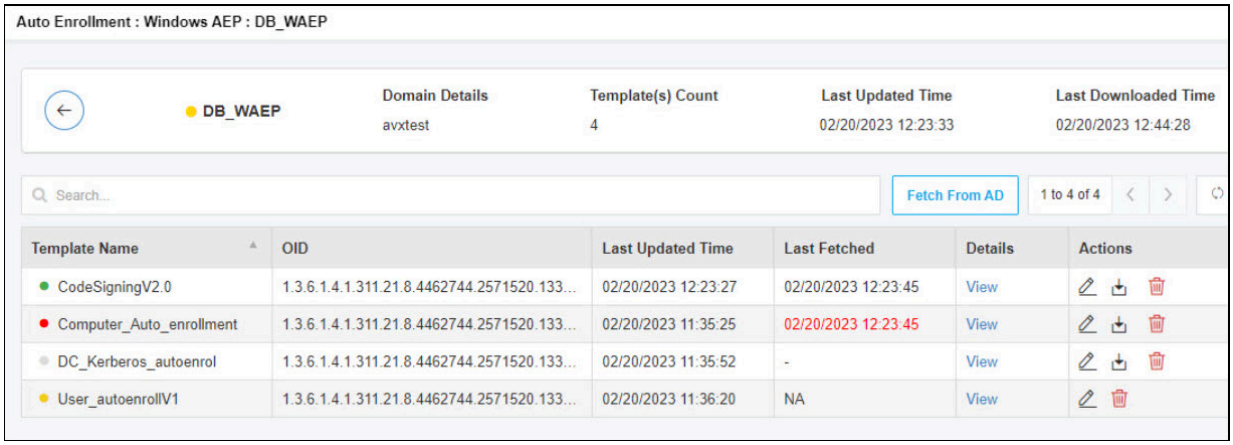
11. Click **Finish.**
    A message that the WAEP settings is saved successfully appears.

The AppViewX PKIaaS certificates that are auto-enrolled via WAEP appear on the **Cert+ > Certificate Inventory** page as shown. You can filter the AppViewX PKIaaS certificates using the WAEP enrollment method.



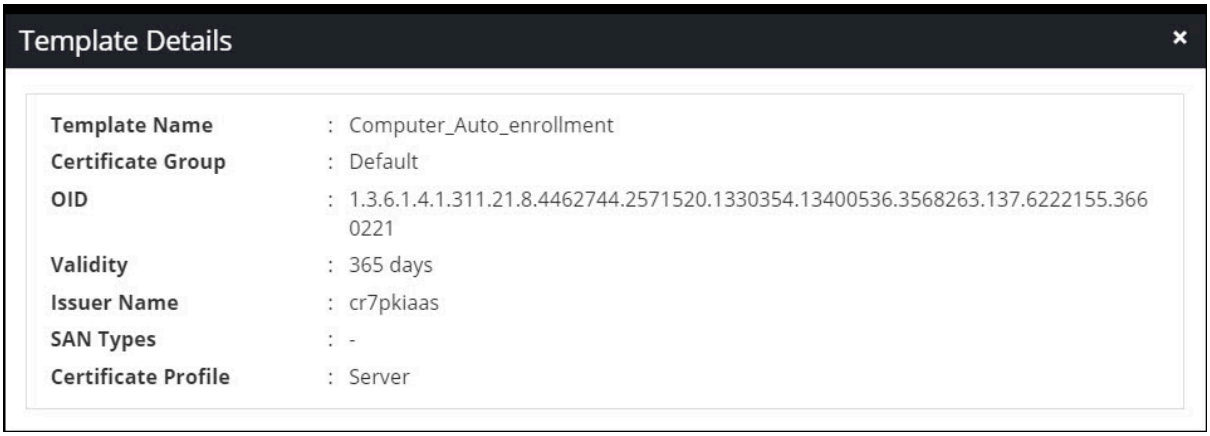
What to do next:

- [Applicable only if you have chosen automatic upload of template] Click **Download** to download the entire set of configured certificate template scripts and the runnable files to publish on your active directory.
- Click **Go to Inventory** to view the added WAEP setting on the dashboard.
- Click the **Endpoint Setting** hyperlink on the dashboard to view details of the configured certificate template.



- Once the templates are fully configured, click **Fetch from AD** to fetch the templates from the active directory. A message, *Template sync triggered successfully,* appears. Here are the color codes against the templates:
  - **Green:** indicates the templates were fetched successfully along with the last fetched time.
  - **Amber:** indicates the templates are partially configured. The last fetched time will be NA.
  - **Gray:** indicates the templates were not found in the AD or the templates not yet published. The last fetched time will be empty for these.
  - **Red:** indicates the templates were deleted along with the last fetched time.

- Click **View** to get the certificate template details.



- Click the (**Edit**) icon to edit configuration of the certificate template.
- Click the (**Download**) icon to download a selected template, or click the (**Delete**) to delete a selected template.

- Downloading Certificate Template Scripts
- Viewing the added WAEP Setting on the Dashboard

Downloading Certificate Template Scripts

Note: This section is applicable only if you have used the Lift & Shift feature.

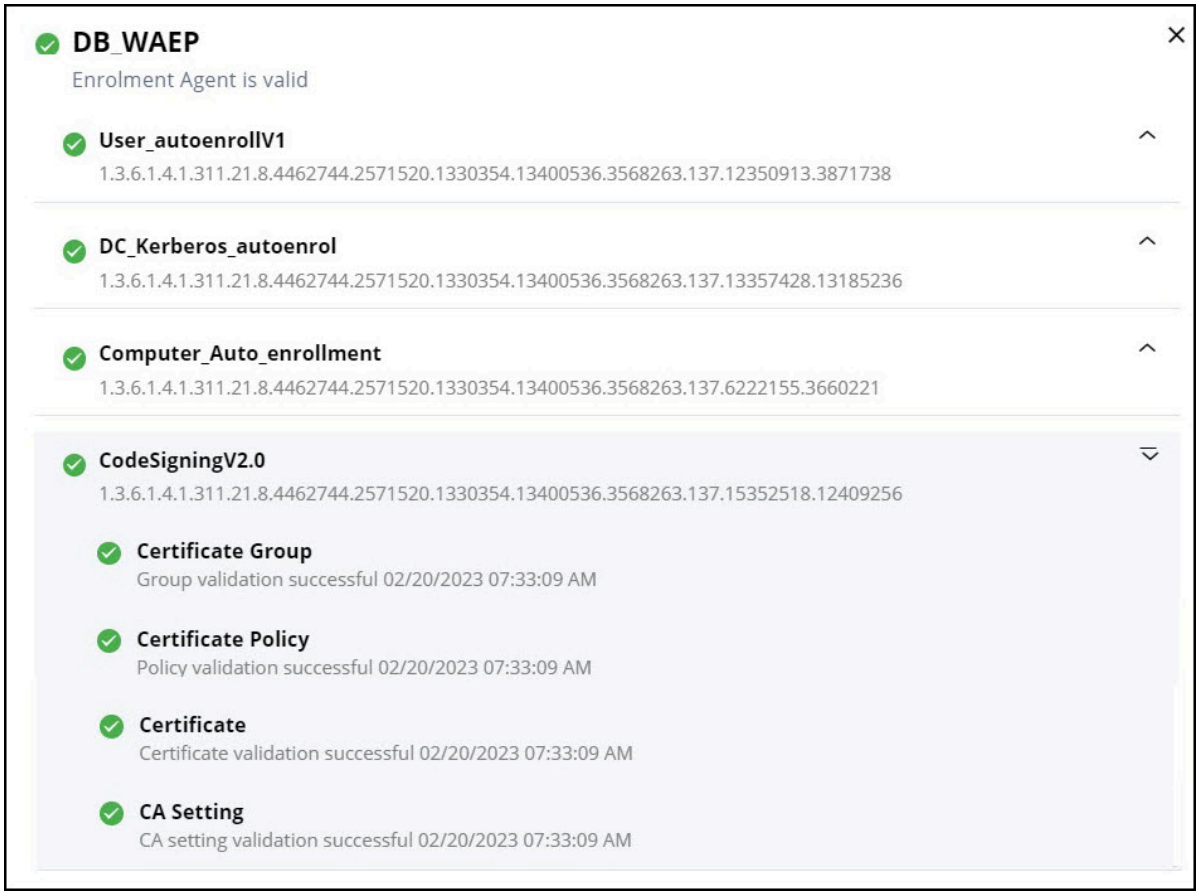
1. Click **Download** to download the entire set of configured certificate template scripts and the runnable files.
2. To publish the downloaded files on your active directory:
   a. Unzip the downloaded files.
   b. Open PowerShell and run the waep script as an administrator by typing *y* at the prompts as shown:

Viewing the added WAEP Setting on the Dashboard

To view the newly added WAEP setting on the dashboard:

1. Click **Go to Inventory** to view the added WAEP setting on the dashboard.
2. From this page, you can do any of the following actions:
   - Click **Check** to check if the certificate template configuration is successful. If the certificate template configuration is successful, the status changes to *Valid,* else it turns to *Invalid*. For incomplete template certificate configuration, the status shows as *Incomplete.* To complete the WAEP configuration, click the (**Edit**) icon.

     You can also expand to view the validation attributes and status of the connection separately for each of the certificate templates as shown.



   - If the certificate is found in the enrolled Windows client machine, then the enrollment is successful and the **Success Requests** tab on the dashboard is incremented by 1. If it is unsuccessful, then the count in the **Failed Requests** tab is incremented by 1.

- If you have enabled the **Block Duplicate Certificates** on the **Settings** page, then based on the value set for the permissible duplicate certificates in an hour further auto-enrollment requests are blocked for the day with a log entry, *Duplicate Certificate request - Certificate entry with this Common Name, Certificate Template and SAN value has already been issued.* The user/device is automatically unblocked after the set time limit has elapsed.

  The administrator can manually enable the blocked user/device from the WAEP page by clicking **View** in the **Blocked Users** tab, selecting the checkbox against the user name to unblock, and clicking **Unblock.**

  Click the **Audit Log** to get details on the unblocked user/device. The details include the device/user name, domain, date and time on when it was blocked and unblocked, and who unblocked it. You can also download the audit log in the CSV format.

- Click the  (**Edit**) icon to edit the WAEP configuration.
- Click the  (**Download**) icon to download the bundled templates of WAEP configuration, or click the  (**Delete**) to delete the WAEP configuration.

Step 5: Updating Windows Auto-Enrollment Server URL

Note: This section is applicable only if you choose to manually upload templates to AppViewX.

To update the Windows Auto-Enrollment Server URL on ADCS:

1. Open a command prompt on the Windows Auto-Enrollment Server <winaepserver or server name>.
2. To get the current URL, run the command:

```
certutil -config <winaepserver or server name.yourcompany.com\MSCA-Proxy> -enrollmentserverurl
```

   Ensure to replace the server <FQDN> and <MSCACN> names with your own configuration.

3. To remove the existing enrollment server URL, run the command:

```
certutil -config <winaepserver or server name.yourcompany.com\MSCA-Proxy> -enrollmentserverurl https://<winaepserver or server
 name.yourcompany.com/MSCA-Proxy>_CES_Kerberos/service.svc/CES
delete
```

   Ensure to replace the server <FQDN> and <Enrollment Server URL> with your own configuration.

4. To add the new enrollment server URL, run the command:

```
certutil -config <winaepserver or server name.yourcompany.com\MSCA-Proxy> -enrollmentserverurl https://<AEP

URI:portnumber>/avxapi/msproxy/simpleenroll Kerberos
```

Ensure to replace the server <FQDN> and <Enrollment Server URL> with your own configuration.

5. To confirm, run the first command again to show the new updated URL.

Note:

- All connections are now routed to Windows Auto-Enrollment server so we recommend that you disable the MS root CA, which was created earlier, for security purpose.
- If you are already running Microsoft CA environment, we still recommend that you follow the afore-mentioned steps and plan for decommissioning your previous Microsoft CA environments once the migration of certificates is complete.

Step 6: Updating Group Policy for Certificate Enrollment

To update the Group Policy for Certificate Enrollment:

1. Type `gpmc.msc` in the Run command to access Group Policy Management on the AD Domain Services server.
2. Expand your domain forest > Domains > your domain name, and then select **Default Domain Policy.**
3. Right-click **Default Domain Policy** and select **Edit.**
4. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.**
5. Edit **Certificate Services Client – Certificate Enrollment Policy.**
6. Change **Configuration Model** to *Enabled*.
7. Remove the **Active Directory Enrollment Policy** from the Certificate Enrollment policy list, and click **Add.**
8. Enter the policy server URI: https://%3Cwinaepserver.yourcompany.com%3E/ADPolicyProvider_CEP_Kerberos/service.svc/CEP. Click **Validate Server,** and click **Add.**
9. Select **Default,** and click **Add.**
10. Expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.**
11. Edit **Certificate Services Client – Certificate Enrollment Policy.**
12. Change **Configuration Model** to *Enabled*.
13. Remove the **Active Directory Enrollment Policy** from the Certificate Enrollment policy list, and click **Add.**

14. Enter the policy server URI: https://%3Cwinaepserver.yourcompany.com%3E/ADPolicyProvider_CEP_Kerberos/service.svc/CEP. Click **Validate Server,** and click **Add.**
15. Select **Default,** and click **OK.**

Steps to replace the Default TLS Certificate with Signed Certificate in CC

WAEP uses MTLS to establish communication that requires a certificate to authenticate it. By default, AppViewX provides its own certificate that will perform authentication.

Note:

- The certificate must have the same IP address as the CC. If you are using a PKIaaS-issued certificate, then you must have a provision to download CRLs for all the end clients.
- If it is not AppViewX's default certificate, then you must update the **relative path of the certificates** in the *appviewx.properties* file in the `<Cloud_Connector_folder>/deps/` directory.

To update the certificate:

1. Copy the files (CRT and the private key) of the certificate and paste them in the `<Cloud_Connector_folder>/deps/` directory in the desired location.
2. Update the following fields in *appviewx.properties* file in the `<Cloud_Connector_folder>/deps/` directory by passing the relative paths of the respective files that were placed in the directory in during the previous step:
   - SERVER_ACCESS_CERT=<relativepath> after the `/deps` directory. For example, /externalcerts/externalcert.crt
   - SERVER_ACCESS_KEY=<relativepath> after the `/deps` directory. For example, /externalcerts/externalcert.key
   - TRUSTED_CA_CERTS=<relativepath> after the `/deps` directory. For example, /externalcerts/externalcert_trust.crt

   Note: If there is more than one trusted certificate (root, issuing), then separate them using a comma.

3. Move to the CC installation path and run the installation script to see the changes:

   `./deps/utils/gateway_upgrade.sh`

4. Once upgrade is done, the user must check whether the *avx-midserver-gateway* is restarted or not. If not, restart the mid-server-gateway.
   - Switch to `<Cloud_Connector_folder>/deps/tools` and run the following commands.
     - `./k3s kubectl get pods -n cc | grep avx-mid-server-gateway`

       Copy the complete pod name.
     - `./k3s kubectl delete pods -n cc <avx-mid-server-gateway-pod-name> --force`

Known Errors

Following are some of the known errors encountered on the WAEP Settings addition page and how to troubleshoot them:

- **CERT-ENROLLMENT-PROTOCOL-1009 : Agent name already added. Please enter a different name.**

  Probable Cause: Agent setting name is already added.

  Workaround: Use a different and unique agent setting name.
- **CERT-WAEP-ENROLLMENT-1010 : The provided agent Hostname is already added. Please provide different valid Hostname.**

  Probable Cause: The provided agent hostname is already added.

  Workaround: Try a different hostname.
- **CERT-WAEP-ENROLLMENT-PROTOCOL-1002 : Template with same name already exists on the WAEP Agent. Please change and add again.**

  Probable Cause: While renaming the template of the duplicate template, you may get this error.

  Workaround: Try a different and unique template name while configuring the certificate template.
- **WAEP Setting addition Page: Unable to establish connection with policy server.**

  Probable Cause: Check whether the policy server Remote Desktop Protocol (RDP) access is accessible from the CC.

  Workaround: Check whether the policy server is accessible from RDP.
- **Invalid Credentials provided for policy server**

Probable Cause: The C11 credential provided is incorrect or the NTLS authentication is not enabled for WinRM.

Workaround: Provide valid credentials and enable required authentication protocol for WinRM.

- **Windows machine responded with empty powershell response.**

  Probable Cause: PowerShell execution did not execute as expected.

  Workaround: Check if access is configured to connect via WinRM.

- **Unable to establish connection with LDAP server from policy server**

  Probable Cause: The policy server could not execute PowerShell script with the LDAP server via Remote Desktop Protocol (RDP).

  Workaround: Check the trust and RDP access between the LDAP and the policy server.

Following are some of the known errors encountered during WAEP enrollment and how to troubleshoot them:

- **CERT-ENROLLMENT-0012: AGENT_ID property not found to identify CC (Agent) for WAEP**

  Probable Cause: AGENT_ID property not configured on the CC.

  Workaround: Contact AppViewX CC support.

- **Error occurred while dynamically getting validity in days**

  Probable Cause: Validity conversion failed for the selected template.

  Workaround: Verify the configured validity on the WAEP configuration.

- **CERT-ENROLLMENT-011: Template settings is not found for this Template OID**

  Probable Cause: Template to be used for enrollment is not selected for the WAEP configuration.

  Workaround: Verify and add the selected template in the WAEP configuration.

- **CERT-ENROLLMENT-008: Certificate conversion failed**

  Probable Cause: Certificate conversion failed while downloading the certificate from AppViewX in the PEM format.

  Workaround: Contact AppViewX support.

- **CERT-ENROLLMENT-001: Agent settings is not found (or) invalid for this agent**

Probable Cause: WAEP configuration not found for the particular CC (Agent).

Workaround: Verify whether WAEP configuration is added for the particular CC hostname.

Chapter 7: Reporting and Monitoring

Overview

Once the certificates in the infrastructure are discovered in AppViewX, they can be monitored as the reports in the Dashboards. In the dashboards, the user can track the certificates expiry, compliance, security details as the reports in the dashboard.

Reporting and monitoring the certificates are essential for an administrator to get complete visibility of all the certificates across multiple vendors and data centers in one single window pane. Certificates have a finite life span and are set to expire at different dates and times. Due to advancements in cryptography, there are high chances that the infrastructure will carry the weaker algorithm certificates which will be vulnerable to several attacks which will cause business outages.

Using the dashboards and reports, the administrator can continuously monitor the status of the certificates in terms of expiry, security, compliance and so on.

Certificate Reporting

For more information, refer to the **Certificate Reporting** section in the CERT User Guide.

Dashboard Actions

This section explains how to create, export, import, and delete dashboards.

Viewing Certificate Reports

To view certificate reports:

1. Click **Certificate Inventory** and click the type of certificate for which you want to view the report.

   The Reports page is selected.

   Although each certificate report displays the data differently, the same set of data is used to generate each report.

2. 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.

Creating Dashboard

To create a dashboard:

1. Go to (**Menu**) icon **> CERT+**.

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

2. Click **Dashboard** in the left navigation pane.
3. Click the **Create (+)** icon in the command bar.

   The **Create dashboard/widget** window appears.

4. Enter the field information in the **Create dashboard/widget** window.

   The following table provides the field description to create a dashboard:

Field Description for Create dashboard/widget section

Field	Description
***Dashboard name**	Name of the dashboard.
***Select solution**	ADC is the select solution.
***Widget type**	Type of the widget. Options 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. When you choose this option, the **Choose widgets** option appears, which allows you to select the widgets.
***Select widget**	Customized widgets appear in the drop-down menu. Select the appropriate widget.
***Widget name**	Name of the widget.

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

5. To create a dashboard/widget, click **Create**.

Exporting Dashboard

For more information, refer to the **Exporting Dashboard Information** section in the CERT User Guide.

Importing Dashboard

For more information, refer to the **Importing Dashboard** section in the CERT User Guide.

Deleting Dashboard

For more information, refer to the **Deleting Dashboard** section in the CERT User Guide.

Chapter 8: 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

For more information, refer to the **Alerts and Logs** section in the CERT User Guide.

Chapter 9: PKI Standard Practices

Overview

This section outlines some of the 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 Organization 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

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

- Ensure 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

Issue Type	Revoke compromised/ counterfeit certificates	Revoke CA certificate	Replace all certs issued	Remove/ Revoke Root certificate
Impersonation	Yes	NA	NA	NA
RA compromise	Yes	NA	NA	NA
CA system compromise	NA	Yes	Yes	NA
CA key compromise	NA	Yes	Yes	NA
Root CA compromise	NA	NA	Yes	Yes

Chapter 10: Steps for Migration

Following are the steps to migrate:

- CA policy must have only issuer-based configuration.
- Reconfigure the RBAC configuration for PKI+.
- Ensure that there is no custodian or CA in the *in-progress* state.
- For on-premise deployments, the settings have to be configured. See Settings.