appviewx

PKI+ User Guide

Version: 2024.1.3.0

Copyright AppViewX, Inc.

Trademarks

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
4.0	Updated draft of document for the release 2024.1.3.0	Apr 2025
3.0	Updated draft of document for the release 2024.1.2.0	Mar 2025
2.0	Updated draft of document for the release 2024.1.1.0	Mar 2025
1.0	Initial draft of document for the release 2024.1.0.0	Mar 2025

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.

Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

For example,

- This document includes software details developed by VMware, Inc. (www.vmware.com.

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.

Convention	Description
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Introduction

What is AVX One Platform?

AVX One Platform refers to a unified solution offered by **AppViewX** designed to simplify and automate the management of various infrastructure components, such as **PKI (Public Key Infrastructure)**, **SSL/TLS certificates**, **load balancers**, and **application delivery controllers** (ADCs), among other network and security resources.

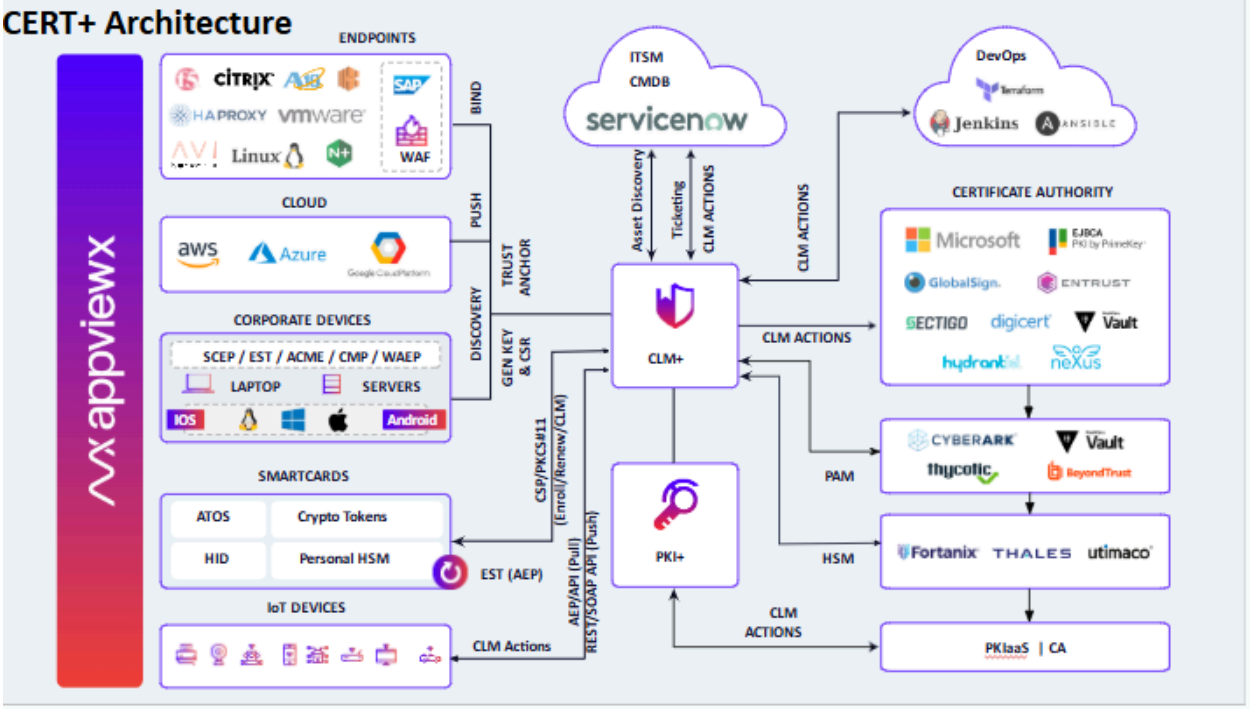
Key features of **AVX One Platform** include:

1. **Centralized Management:** AVX One provides a centralized platform for managing multiple components, including certificates, keys, and security policies, making it easier for organizations to maintain security across their infrastructure.
2. **Automation:** It offers automation capabilities for tasks such as certificate lifecycle management, certificate discovery, renewal, and revocation. This reduces manual errors and improves operational efficiency.
3. **Multi-cloud & Hybrid Cloud Support:** The platform supports both on-premises and cloud-based deployments, allowing organizations to manage their infrastructure across multi-cloud and hybrid cloud environments.
4. **PKI Management:** AVX One simplifies the deployment, configuration, and operation of **Public Key Infrastructure (PKI)**, enabling organizations to create, manage, and deploy certificate authorities (CAs), and handle certificate issuance, revocation, and validation.
5. **Security & Compliance:** The platform helps ensure compliance with various security standards and industry regulations, particularly related to encryption and certificate management.
6. **Integrations:** AVX One integrates with various third-party systems, including cloud services, load balancers, and network security appliances, offering flexibility for businesses with complex IT environments.

In summary, **AVX One Platform** is an integrated, scalable solution designed to streamline and secure the management of infrastructure resources, particularly focusing on PKI, certificates, and related security operations.

CERT Architecture

The following diagram illustrates the CERT architecture:



What is AppViewX PKI?

AppViewX PKI is a comprehensive solution for managing Public Key Infrastructure (PKI) and digital certificates within an organization's IT environment. It simplifies the entire lifecycle of digital certificates, providing tools for automated certificate management, secure key management, and ensuring compliance with security policies.

What is AppViewX PKIaaS Native CA?

AppViewX introduces its own Certificate Authority (CA)--AppViewX PKIaaS Native CA--for PKI initialization enabling the customers to take advantage of Post-Quantum Cryptography (PQC) capabilities, to ensure the infrastructure remains secure in the era of quantum computing.

Note:

PKI can be initialized using either the AppViewX CA backend (PKIaaS Native) or a Cloud CA backend (Standard).

Key Features

- **Post-Quantum Cryptography (PQC) support:** Supports NIST-standardized PQC algorithms and selected algorithms from the fourth round of NIST's post-quantum standardization process.
- **Customizable Certificate Templates:** Allows users to create tailored certificate authorities (CAs) with custom templates and offers pre-configured templates for different types of end certificates.
- **CA Key Storage Mechanisms:**
  - **CA Key with On-Prem HSM (BYOD):** Seamlessly integrates with external HSM vendors for cryptographic operations. HSMs supported by AppViewX PKIaaS Native CA are:
    - Fortanix with FIPS
    - Fortanix without FIPS
    - Thales DPOD
    - Thales GPN
    - Utimaco
    - Entrust
  - **CA Key with Cloud HSM (BYOD or AVX Provided):** Requires connectivity 443 to the external Cloud HSM Provider.
  - **AVX Managed Key:** This is a key management service provided by **AppViewX**, which is part of the **PKI** solution. The **AVX Managed Key** feature is designed to streamline and automate the generation, storage, and lifecycle management of cryptographic keys used in PKI, SSL/TLS certificates, and other security operations.
- **Enhanced Security – Airgapped Root CA:** Enhances security with offline Root CA deployment support.
- **Revocation List Management – Custom CRLDP & OCSP:** Provides customizable Certificate Revocation List Distribution Points (CRLDP) and Online Certificate Status Protocol (OCSP) services.
- **Auto-Enrollment Support:** Simplifies certificate enrollment with support for SCEP, EST, ACME, WAEP, and Microsoft Intune protocols.
- **Support for Short-Lived Certificates:** Short-lived certificates refer to SSL/TLS certificates that are issued with a very short validity period, typically ranging from a few days to a few months. With shorter validity periods, the use of automated tools (like **ACME protocol** for certificate management and many more MDM tools) becomes more common. This encourages the automation of certificate renewal, which reduces human errors and increases operational efficiency. They are more secure as attack surface is minimized because certificates are rotated more frequently. If a certificate is compromised, revocation becomes more effective because the certificate will expire quickly anyway.
- **PKI Dashboard:** Features an intuitive dashboard for streamlined certificate and CA management.
- **Security:** AppViewX PKIaaS Native CA provides Quantum-Resilient Security by implementing algorithms such as Dilithium, Falcon, and Sphincs Plus to protect data against quantum attacks.

Note:

AppViewX PKIaaS offers 99.5% availability by default as a multi-tenant SaaS solution.

Key Types, Hash Functions, and Key Sizes supported by AppViewX PKIaaS Native CA

Key Types	Hash Functions	Key Sizes
SPHINCS PLUS (SLH-DSA)	SHAKE256, HARAKA256, SHA256	256, 384, 512
DILITHIUM (ML-DSA)	SHAKE256	10496, 15616, 20736
FALCON (Beta)	SHAKE256	7176, 14344
EC	SHA160, SHA224, SHA256, SHA3-224, SHA3-256, SHA384, SHA512	160, 163, 191, 192, 193, 224, 233, 239, 256, 283, 320, 359, 384, 409, 431, 512, 521, 571
DSA	SHA160, SHA224, SHA256, SHA3-224, SHA3-256, SHA384, SHA512	1024, 2048
RSA	SHA160, SHA224, SHA256, SHA3-224, SHA3-256, SHA384, SHA512	1024, 2048, 3072, 4096, 7680, 8192

Chapter 2: Getting Started

Know your Deployments for PKI+

We support multiple deployment options to cater to various customer needs and infrastructure preferences. Our solutions can be deployed in On-Premises environments, Managed Kubernetes platforms such as EKS, AKS, GKE, and OpenShift and as a Software as a Service (SaaS).

SaaS Deployment (Highly Secure and Hassle-Free)

Our Software as a Service (SaaS) offering is designed for organizations that prioritize security, simplicity, and efficiency. In this deployment mode, we manage all aspects of application hosting, maintenance, and scaling, providing a worry-free experience for our customers. Our SaaS platform is built with cutting-edge security measures, including robust encryption, multi-factor authentication, and continuous monitoring to ensure your data and operations are protected at all times.

Choosing SaaS not only reduces the burden on your IT teams but also ensures that you benefit from the latest updates, features, and security enhancements without any additional effort. This option is ideal for organizations of all sizes, particularly those looking to quickly access our services with the assurance of enterprise-grade security and compliance. For additional information about saas deployment, click here.

On-Premises Deployment

On-Premises deployment enables organizations to install and operate our applications on their own infrastructure. This approach offers the highest level of control and customization, making it particularly suitable for organizations with strict security, compliance, or performance needs. It is best suited for enterprises with dedicated IT resources and the expertise to manage complex infrastructure. For additional information about on-premises deployment, click here.

- System Requirements
- Start your Onboarding Journey

System Requirements

System Requirements

Hardware

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

Deployment Requirements

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

Operating System

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

- RHEL 8.7
- RHEL 8.8
- RHEL 8.10
- RHEL 9.2
- RHEL 9.3
- RHEL 9.4

System Requirements (continued)

	• Ubuntu 20.04 • Ubuntu 22.04
Browser Requirements	• **Firefox:** v74.0.1 (64-bit) or later • **Google Chrome:** v85.0.4183.83 (64-bit) or later

Start your Onboarding Journey

Key Highlights of PKI Onboarding Trial Journey

1. **Seamless Module Navigation:** Users can easily transition from the trial version of CERT+ to explore the features of PKI. During this process, they have the option to designate specific user groups that will have access to PKI upon activation.

   Any CERT+ trial customers can click **Manage PKI** to enable the PKI product and designate/invite the users into AppViewX adding the user to a specific User group and assigning them to access the PKI.

2. **Guided Activation Experience:** Once PKI is activated, the super admin or designated users can fully explore the entire product. The experience is enhanced with a simplified guided navigation, ensuring that users can quickly understand and use all the available features.

   The journey begins by creating a PKI hierarchy which allows the user to create the Root Certificate Authority.

3. **Flexible PKI Hierarchy Setup:** Users have the ability to configure both classical Public Key Infrastructure (PKI) and Post-Quantum Cryptography (PQC) hierarchies. This flexibility allows organizations to choose the most suitable security framework for their needs.
4. **Streamlined PKI Hierarchy Setup and Certificate Issuance:** The setup process for creating a PKI hierarchy and issuing certificates is designed to be efficient. Users can achieve this with minimal input, ensuring that the security protocols such as custodian addition and key ceremonies are maintained without compromising on security standards.
5. **Collaboration and Access Sharing:** Users can invite others to join their designated user group, enabling them to experience the product firsthand. This feature promotes collaboration and allows teams to explore the product’s capabilities together.

The process for managing PKI differs between SaaS trial/new customers and existing customers as mentioned:

- **SaaS trial/New Customers:** Directed to the **CERT+** > **Insights** > **Summary** page, where a pop-up window appears outlining the Onboarding Journey.
- **Existing Customers:** Directly access the PKI page by going to (**Menu**) icon **> PKI+**.

Trial Journey

AppViewX offers its customers a free trial of PKI for its SaaS customers. The trial period is valid for 30 days. Explained below is how to get started on the trial journey:

1. Upon signing up for the free PKI trial, you will receive an email with the subject line, **Welcome to AppViewX Trial!**, at your registered email address.

   This email contains your username. Use this username to log into the AppViewX application. This is followed by another email with a Certificates Insights Report that provides valuable insights into the certificates discovered from Certificate Authority, along with detailed analysis on certificate management, security posture, and compliance status.

2. Click **Login Now** in the email to be redirected to the AppViewX application.
3. Set and confirm the new password to log in.

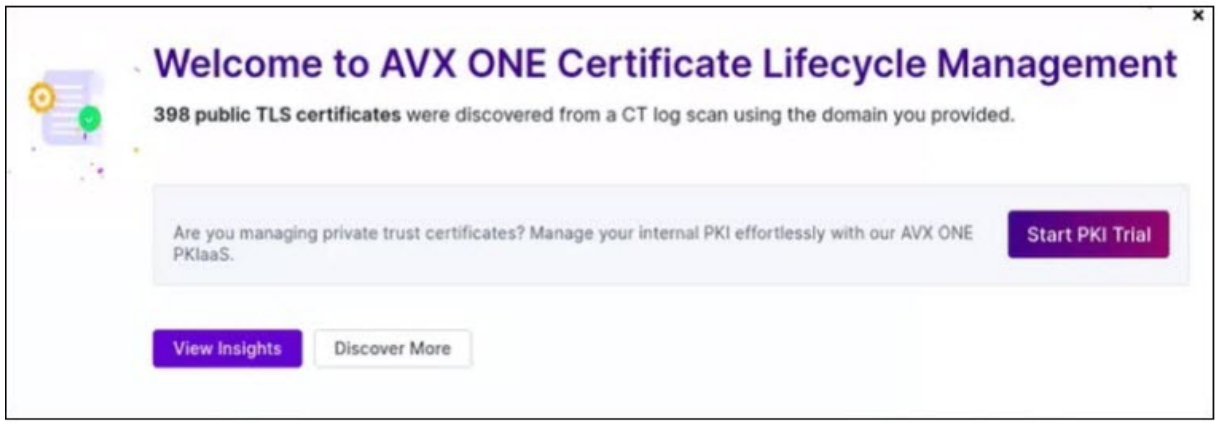
   Tip:

   Click the information icon for guidelines on creating a new password.

   The password is successfully saved to your Google Password Manager for future reference. An email that your password was changed successfully is sent to your inbox. An email follows with details of all the certificates expiring in the next 30 days.

4. On logging in, select the **I accept the terms and conditions** check box on the **Terms of Service** page to continue.

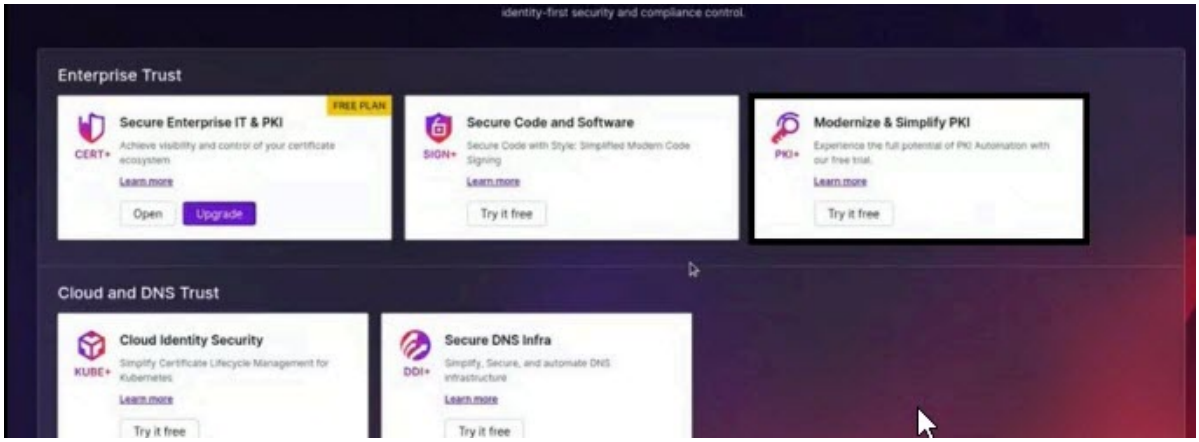
   The **Welcome to AVX ONE Certificate Lifecycle Management** window pops up.



5. Click **Start PKI Trial** to get started.

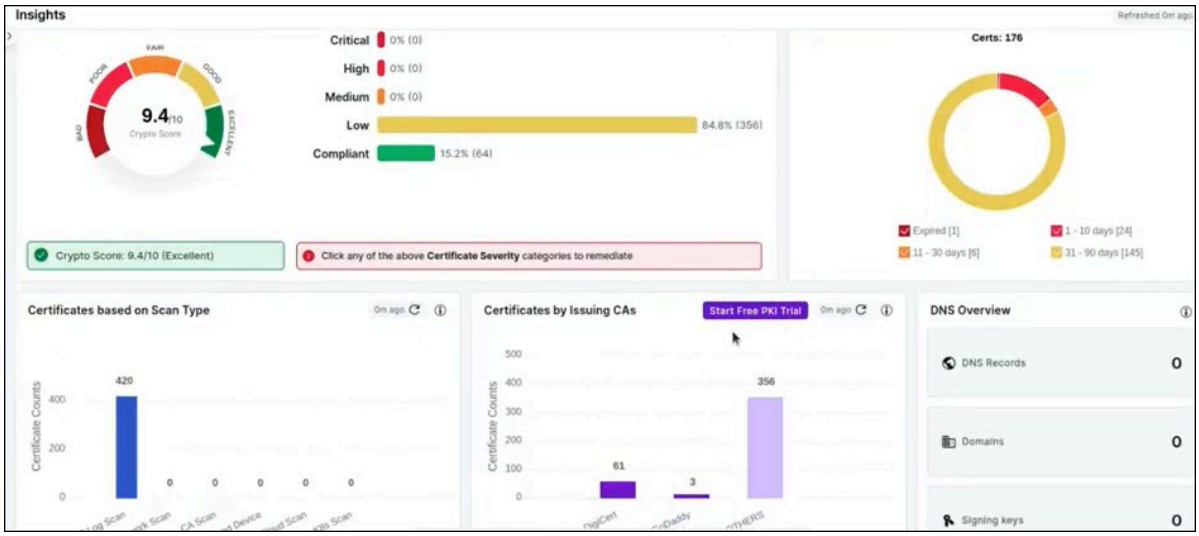
   Alternatively, you can access the PKI trial by any of the following ways:

   - Go to (**Menu**) icon **> All Products.** Click **Try it free** from **Modernize & Simplify PKI.**



   -OR-

   - From the **Insights > Summary** page, scroll down to **Certificates by Issuing CAs** and click **Start Free PKI Trial.**



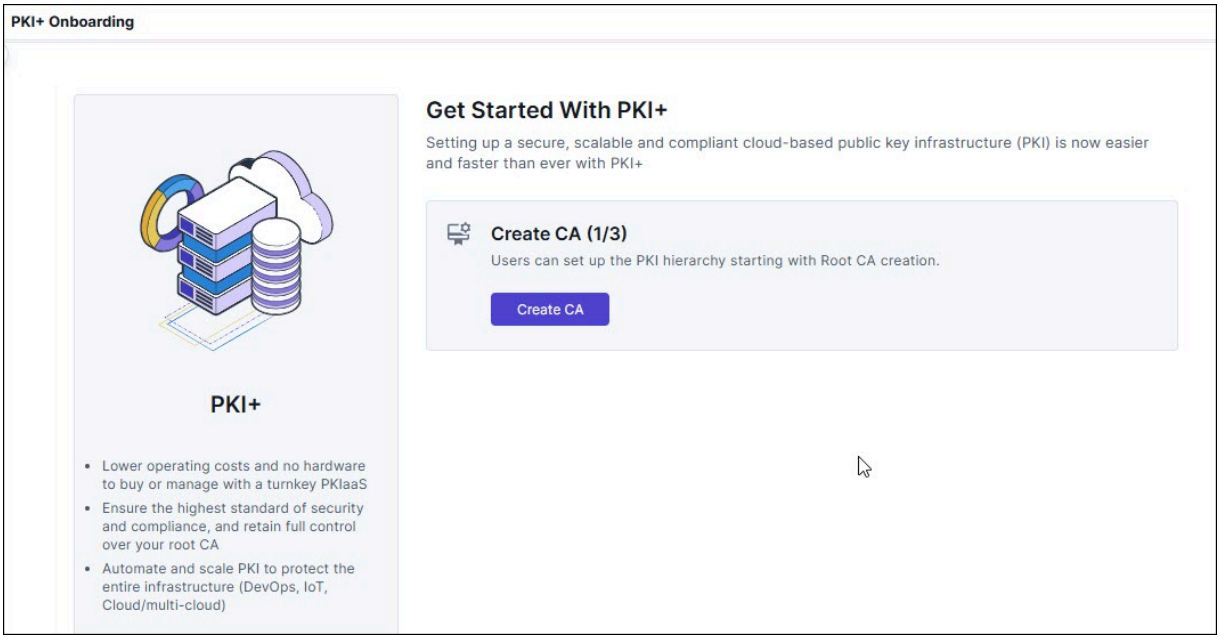
-OR-

- Click **Start PKI Trial** on top of the page. On clicking this button, the button name changes to **Manage PKI.**

A message, *Unboxing your free trial...exciting things are coming!* appears. A **Welcome to PKI+** page is displayed listing the functionalities included in your free trial.

6. Click **Continue.**

The **Get Started with PKI+** page appears.



7. Click **Create CA** to create a PKI hierarchy by creating the root certificate authority.

   The **Create Root CA** page appears.

   a. Enter the fields as described in the table.

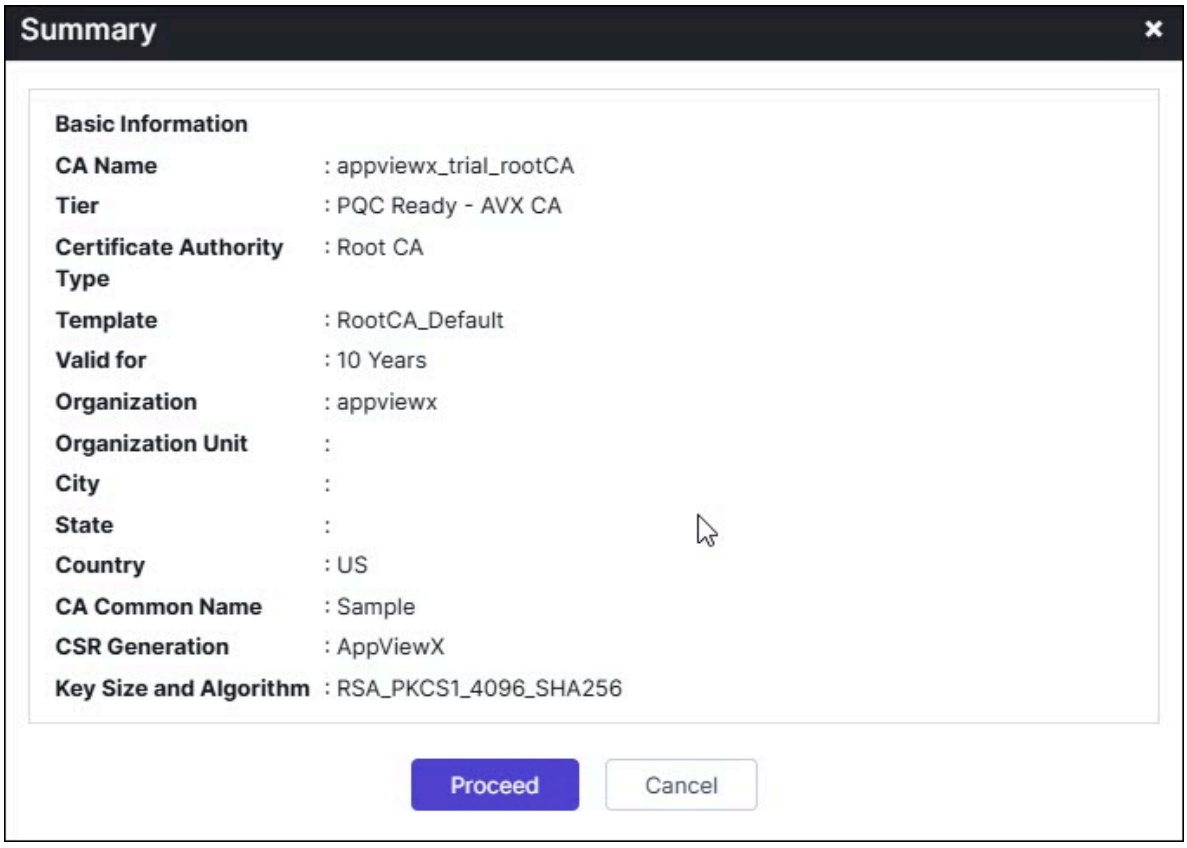
Field Description for Create Root CA page

Field	Description
Select CA Type	
***CA Name**	By default, the CA name is populated. You can edit this and provide a name with no special characters expect hyphen (-) and undescore (_).
***Valid for**	By default, the validity is set to 10 years.
Configure CA Subject DN Details	
***CA Common Name**	Enter the root 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.
Configure CA Key Size and Algorithm	
CSR Generation	You can only select AppViewX.
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.
Configure CA Artifacts	
Path Length Constraint	This is an optional parameter in an issuing CA certificate; it defines the number of sub CA chains created under that specific issuing CA certificate holding the path constraint value. By default, the value is None. This field can have any of these values: 0, 1, 2, 3, or none. For example, if it is set to **2**, it means that only two intermediate CAs are allowed between the end-entity certificate and this CA certificate. None indicates unlimited.

Field	Description
Custodian Settings	
Custodian	By default, the freemium customer (logged in user) is added as the custodian. Custodians are responsible for approving any action performed in PKI. Custodians are the individuals responsible for issuance of root and intermediate certificates. They approve or reject certificate requests, manage the lifecycle of certificates, and ensure auditability and compliance. To add more custodians, click **Manage.** To add a custodian, see Custodian Management. **Note:** • Quorum value is set to 50%, which means that if the custodian group has two members, then only one custodian is needed to approve any CLM action. • Quorum value is an editable field and can contain values ranging from 20 through 100. You can edit this per your organizational need. • Newly added custodians appear in the **Custodian** text box with an increment, for example, if one custodian is added, then the text box displays the default custodian +1.
Note: Fields marked with red asterisk (*) symbol are mandatory.	

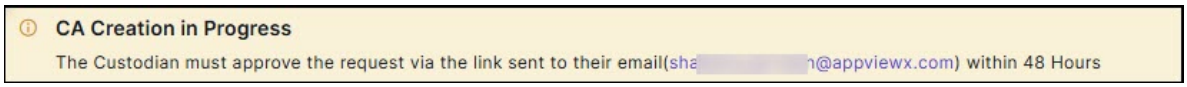
b. Click **Create.**

A window with the summary of values entered appears.



c. Click **Proceed.**

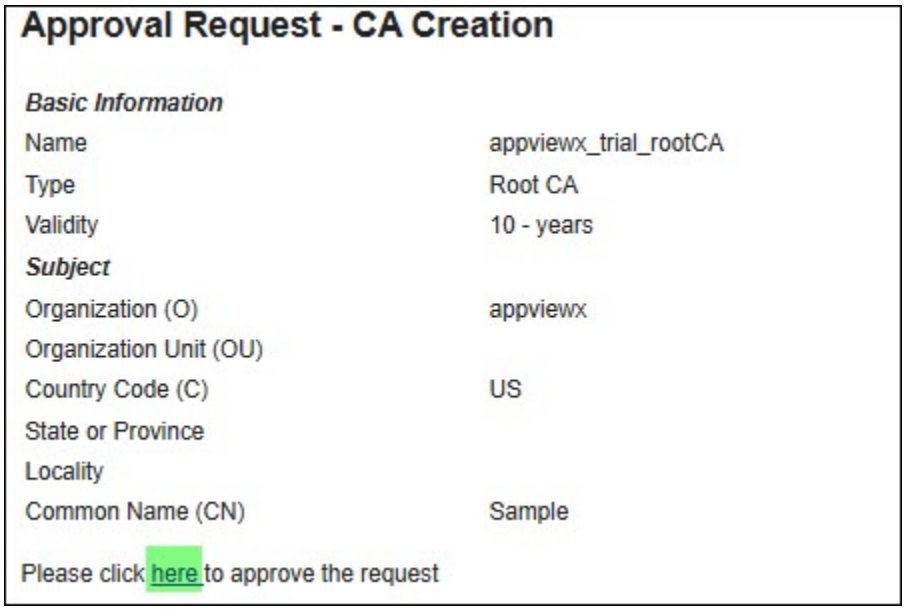
A message, *PKIaaS CA configuration added successfully,* appears on the top of the page while another message appears, *CA Creation in Progress.*



The custodian must approve the subordinate CA creation request via the link sent to their email address.

Note:

The approval link in the email is valid for 48 hours.



Approval Request - CA Creation

Basic Information

Name	appviewx_trial_rootCA
Type	Root CA
Validity	10 - years

Subject

Organization (O)	appviewx
Organization Unit (OU)	
Country Code (C)	US
State or Province	
Locality	
Common Name (CN)	Sample

Please click here to approve the request

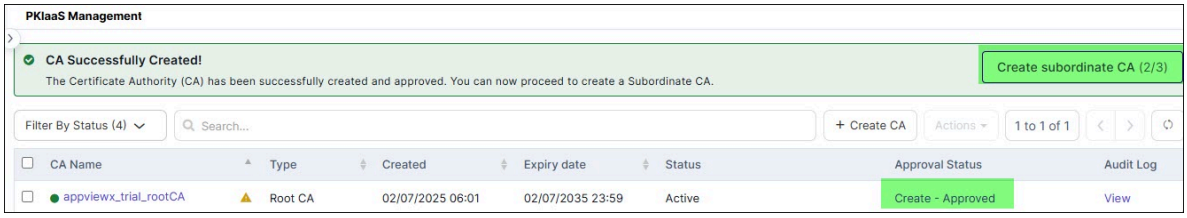
Action Status Description and Required Action

Action Status	Status	Description	Required Action
Email Verification - Pending	Inactive	The custodian's email verification is pending approval and is not active. **Note:** If you want to abort the action, click **Abort.** Any workflow that is triggered and is in progress is killed from the Request page prior to triggering any further actions.	Click the **here** hyperlink to be redirected to the AppViewX login page and the **Requests** page. Click **Approve** by adding your comments. Click **OK** to confirm.
Create - Approval Pending	Inactive	The custodian has been added but is awaiting approval from active custodians.	Active custodians must click the **here** hyperlink in the email to be redirected to the AppViewX login page.

Action Status	Status	Description	Required Action
Create - Approved	Active	The custodian has been approved and added successfully.	-
Email Verification - Rejected	Inactive	The custodian has been rejected.	On rejecting a request, a confirmation popup window appears if the requester wants to submit the request. Click **OK** to resubmit.

d. Click **Manage PKI** to return to the PKIaaS Management page.

On approval, a message, *CA Creation in Progress,* appears and then changes to *CA Successfully Created!* while the **Approval Status** changes to *Create-Approved.*



Note:

You can create a maximum of two root CAs with your trial license.

8. Click **Create subordinate CA.** The **Create Subordinate CA** page appears.
   a. Enter the fields as described in the table.

Field Description for Create Subordinate CA page

Field	Description
Select CA Type	
***CA Name**	By default, the CA name is populated. You can edit this and provide a name with no special characters expect hyphen (-) and undescore (_).
***Issuer Name**	By default, the issuer name is populated. You can edit this.
***Template**	By default, SubCA_Default is selected.
***Valid for**	By default, the validity is set to 5 years.

Field	Description
Configure CA Subject DN Details	
***CA Common Name**	Enter the subordinate 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.
Configure CA Key Size and Algorithm	
CSR Generation	You can only select AppViewX.
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.
Configure CA Artifacts	
Path Length Constraint	This is an optional parameter in an issuing CA certificate; it defines the number of sub CA chains created under that specific issuing CA certificate holding the path constraint value. By default, the value is None. This field can have any of these values: 0, 1, 2, 3, or none. For example, if it is set to **2**, it means that only two intermediate CAs are allowed between the end-entity certificate and this CA certificate. None indicates unlimited.
Custodian Settings	
Custodian	By default, the freemium customer (logged in user) is added as the custodian. He/she will get the approval links via email for all the actions performed in the PKI hierarchy creation.

Note:

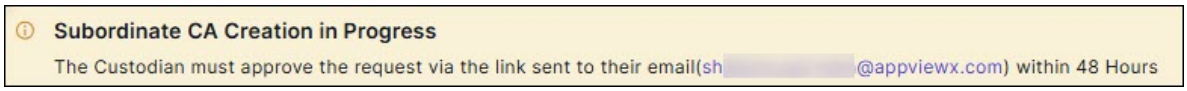
Fields marked with red asterisk (*) symbol are mandatory.

b. Click **Create.**

A window with the summary of values entered appears.

c. Click **Proceed.**

A message, *PKIaaS CA configuration added successfully,* appears on top of the page while another message appears, *Subordinate CA Creation in Progress*.



The custodian must approve the subordinate CA creation request via the link sent to their email address.

Note:

The approval link in the email is valid only for 48 hours.

Action Status Description and Required Action

Action Status	Status	Description	Required Action
Email Verification - Pending	Awaiting Approval	The custodian's email verification is pending approval and is not active. **Note:** If you want to abort the action, click **Abort.** Any workflow that is triggered and is in progress is killed from the Request page prior to triggering any further actions.	Click the **here** hyperlink to be redirected to the AppViewX login page and the **Requests** page. Click **Approve** by adding your comments. Click **OK** to confirm.
Create - Approval Pending	Awaiting Approval	The custodian has been added but is awaiting approval from active custodians.	Active custodians must click the **here** hyperlink in the email to be redirected to the AppViewX login page.

Action Status	Status	Description	Required Action
Create - Approved	Active	The custodian has been approved and added successfully.	-
Email Verification - Rejected	Inactive	The custodian has been rejected.	On rejecting a request, a confirmation popup window appears if the requester wants to submit the request. Click **OK** to resubmit.

d. Click **Manage PKI** to return to the PKIaaS Management page.

On approval, a message, *Subordinate CA Creation in Progress,* appears. Wait until it changes to *Subordinate CA Successfully Created!*

9. Click **Issue Certificate.**

You will be redirected to the **Enroll Server Certificate** page. Follow the steps as described in the Adding/Enrolling Certificate to enroll your certificate.

Chapter 3: Navigating PKI Menu

Navigating PKI Menu

From the PKI menu, you can access:

- **Get Started:** Use this page to initialize PKI, 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. See Dashboard.
- **CA Inventory:** Create root CAs and subordinate CAs and enroll them to the AppViewX PKIaaS certificate authority. See sections under CA Inventory.
- **Custodian Management:** Custodians are responsible for approving any action performed in PKI. You can add or delete custodians from this page. See Onboarding Custodians.

  On completing custodian onboarding, you can add your root CAs and subordinate CAs to PKI.
- **Settings:** Use this page to configure PKI settings. See 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. See Validation Authority.
- **Templates:** This module is available only for AppViewX PKIaaS Native CA users. Use this page to select any of the listed templates or to create your own template to specify certificate parameters. See Templates.
- **Issue Certificate:** This module is available only for AppViewX PKIaaS Native CA users. Use this page to issue certificates. See Issue Certificates.

Chapter 4: PKI Modules

Prerequisites

Prerequisites

On-premise deployments using AppViewX PKIaaS Native CA

1. Ensure these plugins are available:
   - avx-pkiaas-ca-server
   - avx-pkiaas-cert-ocsp-server
   - avx-pkiaas-cert-ocsp-generator
   - avx_platform_gateway_external
   - avx_vendor_cert_scep_agent
2. Ensure these plugins are enabled and are up and running.
3. OCSP HTTP Response Verification
   - Use the following command to verify the presence of the required service port:

     ```
     bash kubectl get svc -A | grep "avx-platform-gateway-scep"
     ```

   - Ensure that the 30022 port is listed. This port is critical for serving OCSP HTTP responses, which are used to check certificate statuses.
4. Configure SMTP server, which is tested successfully, to send test emails to the custodian email ID addresses.
5. Provide a CA name for reference and activate by going to  (**Menu**) icon **> CERT+ > Administration > Certificate Authority**.

6. Onboard at least two custodians before creating CA hierarchy. You can complete the addition of custodians by going to (**Menu**) icon **PKI+ > Custodian Management** with the following privileges under RBAC roles and resources.
   a. Roles automation > service request full
   b. PKI > view all (optional)
   c. Resources > workflow studio, workflow request > PKI+, approval_request

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

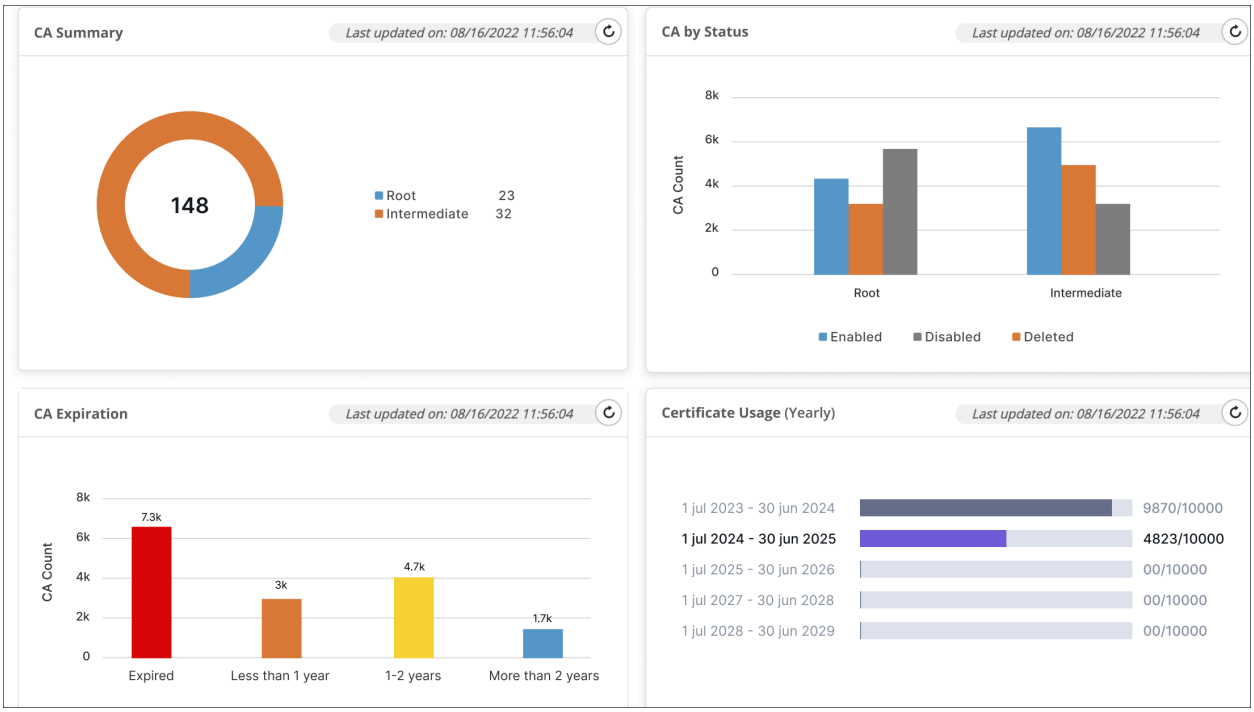
7. **Network Prerequisites**
   - All infrastructure network devices must be able to connect to the AppViewX nodes on 31443 (for Web, API calls, CRL).
   - All infrastructure devices must be able to connect to the AppViewX nodes on 30022 (for OCSP and SCEP).
   - AppViewX must be able to connect to the SMTP server to send test emails to the custodian email ID addresses.

Dashboard

This page gives a quick summary of all the root and the intermediate CAs created via AppViewX PKIaaS. There are two tabs:

- **CA Insight:** This tab displays a quick insight into the CAs based on summary, status, expiration, and certificate usage.
- **Certificates based on CAs:** This tab shows all certificates issued by different CAs, including expired certificates, those expiring in 7 or 14 days, and revoked certificates. It also features widgets that display certificates categorized by templates, CAs, issuance trends, and the CA hierarchy.

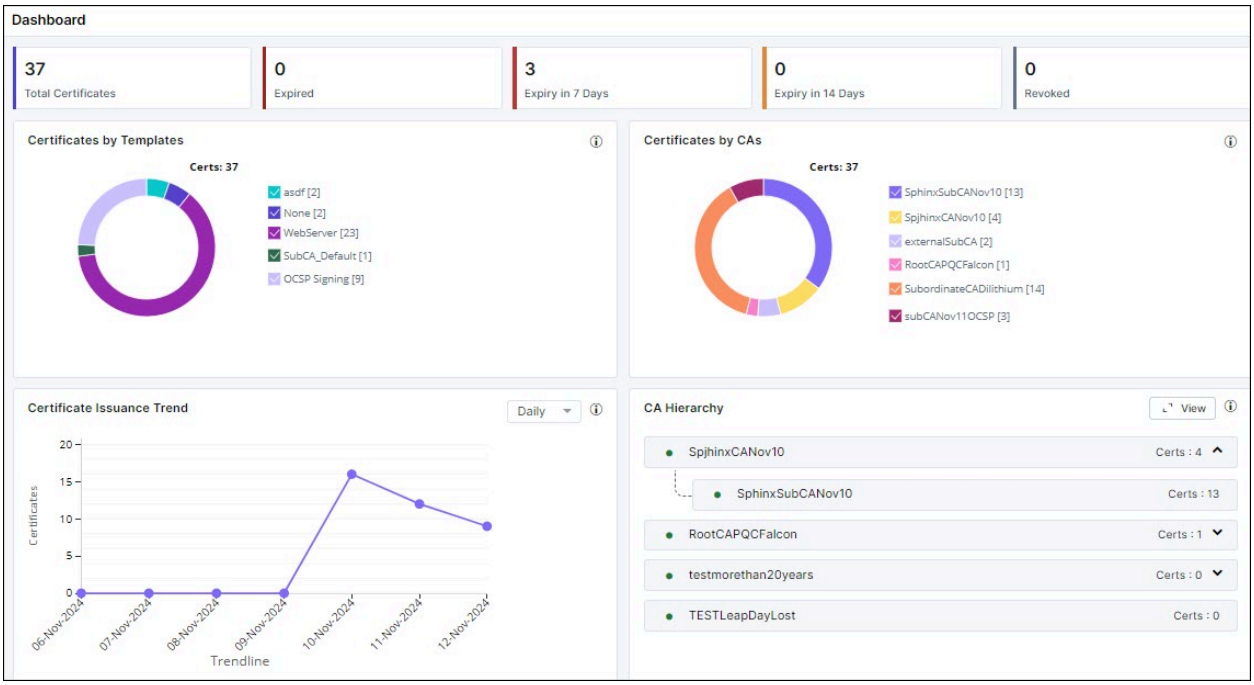
CA Insight



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.
- **Certificate Usage (Yearly):** This widget displays the yearly certificates count starting from the initialization date showing the certificate issuance count by year for the reset date.

End certificates count by CA



The following widgets are displayed on this page:

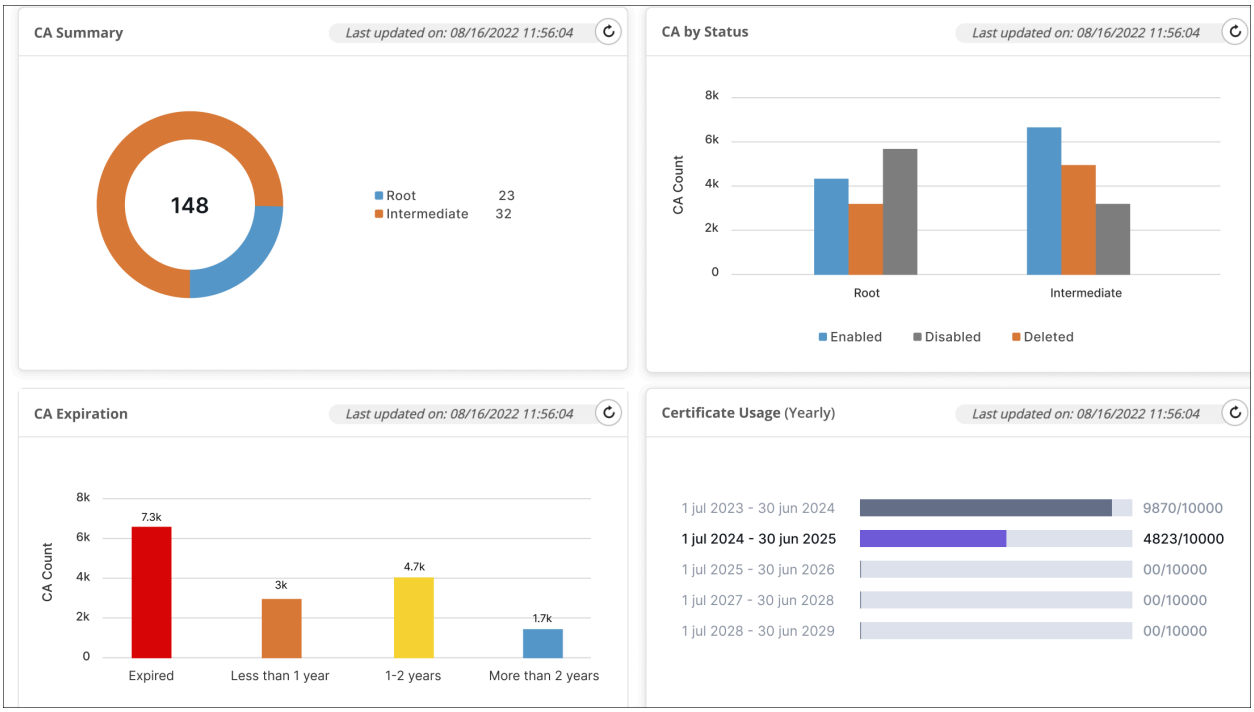
- **Certificates by Templates:** This widget displays all the certificates created via the various templates. By default, all the templates are selected.
- **Certificates by CAs:** This widget displays all the certificates created via the various CAs. By default, all the CAs are selected.
- **Certificate Issuance Trend:** This widget displays all the certificates based on their issuance trend such as daily, weekly, monthly, yearly, and custom. By default, daily is selected.
- **CA Hierarchy:** This widget displays the number of CA hierarchies. Click **View** to display the CA hierarchies created and the certificates under each of the CAs listed along with their count.

By default, the widgets display the certificates for all CAs. You can filter data by selecting a particular CA from the dropdown list on the top right corner of the page.

- For Standard Initialization
- For PKIaaS Native Initialization

For Standard Initialization

CA Insight



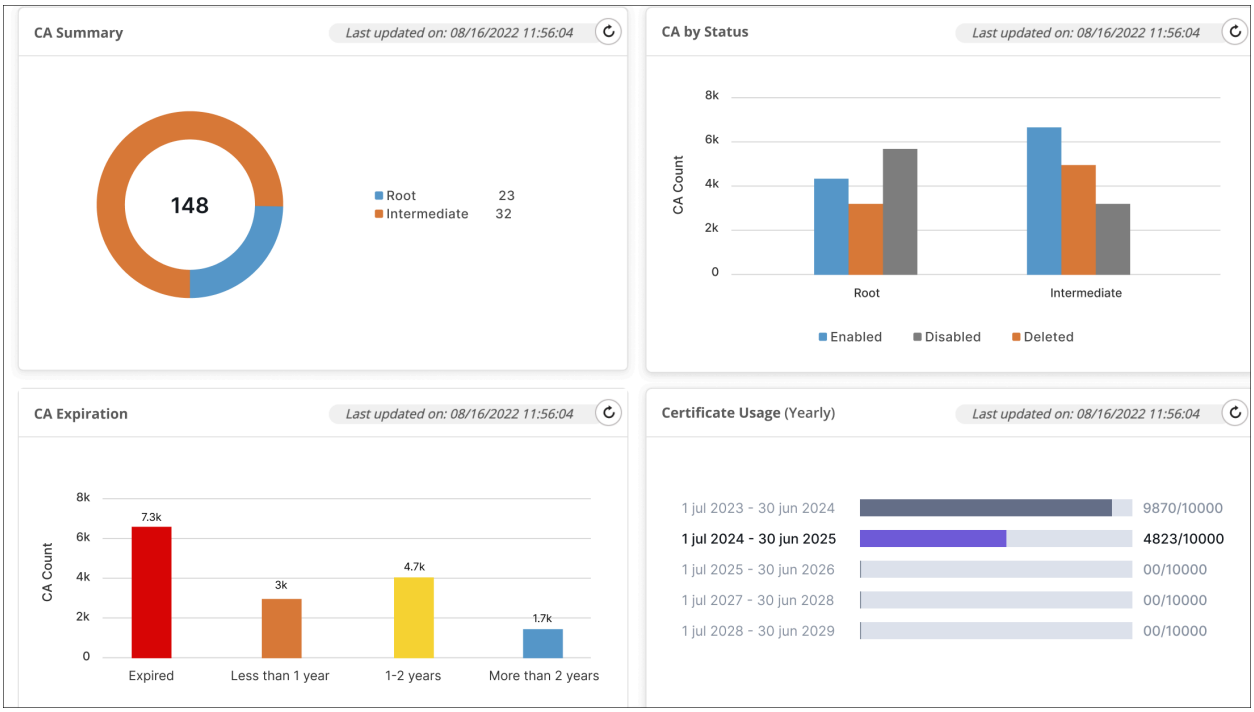
The following widgets are displayed on this page:

- **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.
- **Certificate Usage (Yearly):** This widget displays the yearly certificates count starting from the initialization date showing the certificate issuance/license count by year for the reset date.

For PKIaaS Native Initialization

The following dashboards are available:

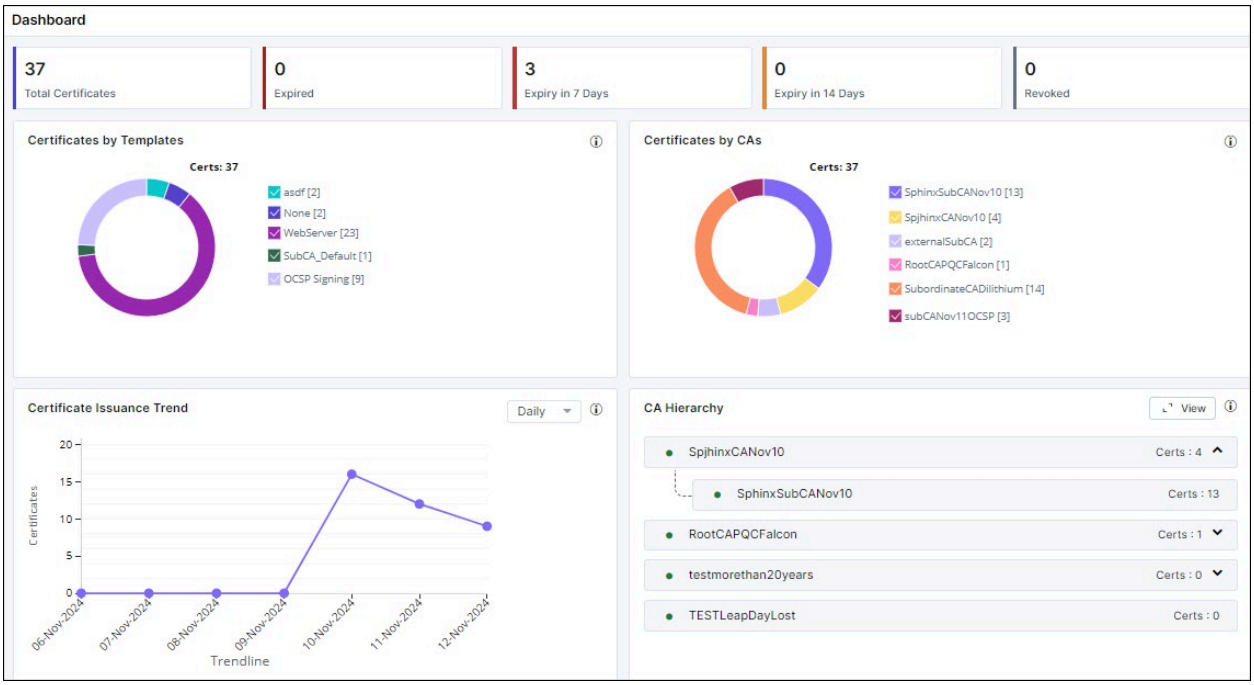
CA Insight



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.
- **Certificate Usage (Yearly):** This widget displays the yearly certificates count starting from the initialization date showing the certificate issuance/license count by year for the reset date.

End certificates count by CA



The following widgets are displayed on this page:

- **Certificates by Templates:** This widget displays all the certificates created via the various templates. By default, all the templates are selected.
- **Certificates by CAs:** This widget displays all the certificates created via the various CAs. By default, all the CAs are selected.
- **Certificate Issuance Trend:** This widget displays all the certificates based on their issuance trend such as daily, weekly, monthly, yearly, and custom. By default, daily is selected.
- **CA Hierarchy:** This widget displays the number of CA hierarchies. Click **View** to display the CA hierarchies created and the certificates under each of the CAs listed along with their count.

By default, the widgets display the certificates for all CAs. You can filter data by selecting a particular CA from the dropdown list on the top right corner of the page.

Custodian Management

Custodians are responsible for approving any action performed in PKI. Custodians are the individuals responsible for issuance of root and intermediate certificates. They approve or reject any action performed on the CA certificates. Custodians typically work in a M-of-N model (or M/N model) to ensure high levels of security and prevent unauthorized issuance of certificates.

Onboard at least two custodians before creating CA hierarchy. You can complete the addition of custodians by going to (**Menu**) icon **> PKI+ > Custodian Management** with the following privileges under RBAC roles and resources.

1. Roles automation > service request full
2. PKI+ > view all (optional)
3. Resources > workflow studio, workflow request > PKIaaS, approval_request

Note:

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

Any administrator can add custodians from the **Custodian Management** page if the key ceremony admins are not configured. Key ceremony admins are an additional layer of control delegation on who can have the authority to add or modify custodians. This is an optional field. Key ceremony admins cannot be added as custodians.

Note:

Only two key ceremony admins can be added.

Key Ceremony Process

Virtual key ceremony in AppViewX PKI is where customers can set a closed group of CA administrators (custodians).

The approvals are based on a M(N) method with a user-defined quorum value, where **M** is the minimum number of custodians required to approve an action, and **N** is the total number of custodians available. A **Quorum** value is the minimum percentage of the number of custodians that must agree or participate to authorize an action or to make a decision regarding the lifecycle of CA Certificates. The default quorum is set to 51%, for example, if the custodian group has three members, then at least two custodians must approve any action to achieve 51% of quorum.

The first custodian is auto-approved and the approval flow gets triggered after adding the second custodian. On adding the second custodian, the individual receives a notification stating *Email Verification - Pending*. Once the email verification is completed, an approval link is sent to the first custodian. Upon approval, the second custodian transitions to the active state.

Onboarding Custodians

Prerequisite

On-prem users need to configure the SMTP 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 configured to 51%. This value signifies the minimum number of approvals needed for tasks such as adding or removing custodians and approving the creation of a certificate authority (CA). For instance, if there are three custodians, the minimum approval required is rounded off to two. In case of six custodians, 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. Click **Save.**
4. Add custodians by entering the following information:

Field Description for Custodian Management page

Field	Description
Email ID	Select an email address of the custodian from the dropdown list to which the approval link and notification messages are sent.
First Name	The first name of the custodian being added. **Important:** Custodian must have login access to AppViewX.
Last Name	The last name of the custodian being added.
Note: Fields marked with red asterisk (*) are mandatory.	

5. Click **Add.**

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.

Important:

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

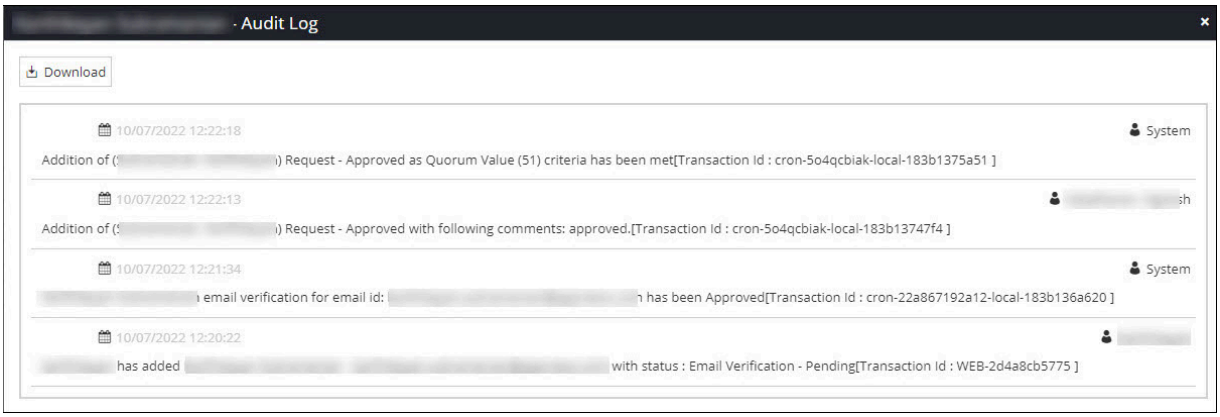
Action Status Description and Required Action

Action Status	Status	Description	Required Action
Email Verification - Pending	Approval Pending	The custodian's email verification is pending approval and is not active.	The newly added custodian receives a notification email. Click the **here** hyperlink to

Action Status	Status	Description	Required Action
		Note: If you want to abort the action, click **Abort.** Any workflow that is triggered and is in progress is killed from the Request page prior to triggering any further actions.	be directed to the AppViewX login page. On successful login, users are directed to the approval page. Users can also approve the request by going to **Menu > Requests > All requests.**
Create - Approval Pending	Approval Pending	The custodian has been added but is awaiting approval from active custodians.	Active custodians must click the **here** hyperlink in the email to be redirected to the AppViewX login page. On successful login, users are directed to the approval page. User can also approve the request by going to **Menu > Requests > All requests.**
Create - Approved	Active	The custodian has been approved and added successfully.	-
Email Verification - Rejected	Inactive	The custodian has been rejected.	On rejecting a request, a confirmation popup window appears if the requester wants to submit the request. Click **OK** to resubmit.

6. To add consecutive custodians, follow the aforesaid steps. Successful addition of custodians depends on the approval of active custodians per the quorum value set.
7. [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 and exporting it 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.



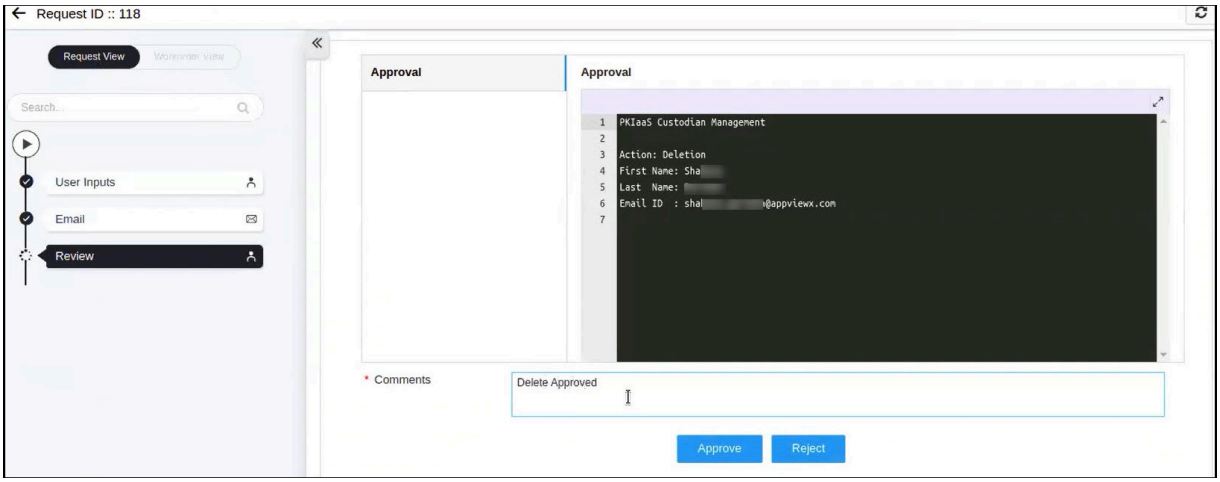
Deleting Custodians

Attention:

Any administrator or key ceremony administrator, if configured, can delete custodians. The quorum value must be met 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 meet the minimum approval required 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 remains as *Active.*

Filtering Custodians

You can apply filters on 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 see 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 AppViewX PKIaaS root CA, see Creating Subordinate CA from PKIaaS Root CA.
- To create a subordinate CA from an external root CA, see Creating Subordinate CA from External Root CA.

Important:

Avoid using the the default policy for PKIaaS; instead, create a dedicated policy specifically for creating certificates with PKIaaS CA.

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 AppViewX PKIaaS Certificate Authority:

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

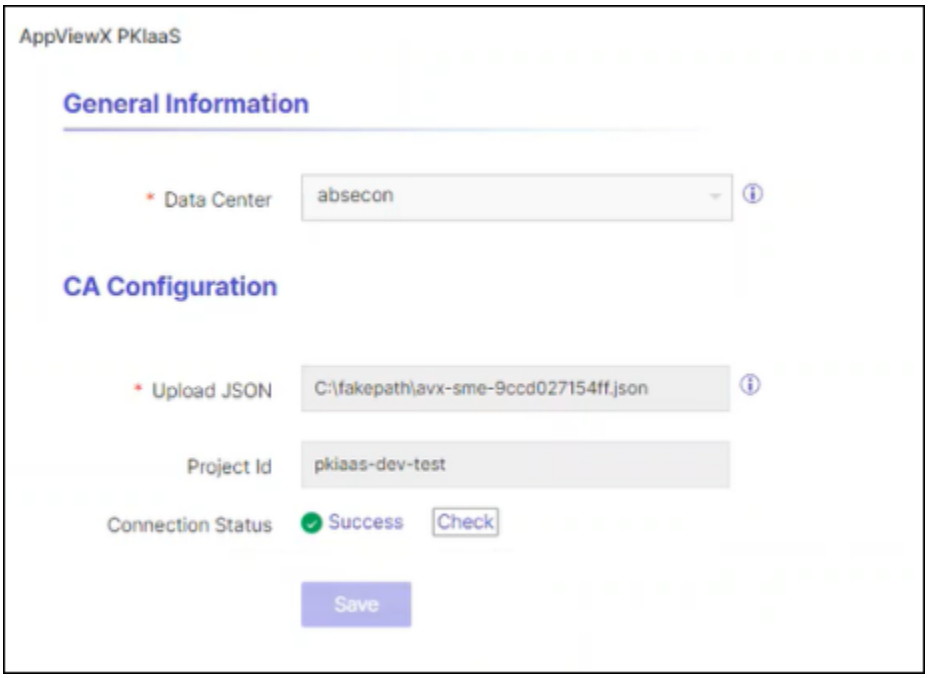
Field	Description
***Data Center**	Select the data center through which the communication must happen.
CA Configuration	
***Upload JSON**	JSON credentials will be provided by AppViewX.
Project Id	This is automatically populated.

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 (**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.
Tier	This is a ready-only field. In case of standard initialization, **Standard** is selected; else **AppViewX PKIaaS Native** if it was used for PKI initialization.
Certificate Authority Type	Select **Root CA.**
***Template**	This field appears only if **Tier = AppViewX PKIaaS Native.** Select a template from the dropdown list.
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***CA Common Name**	Enter the root CA subject name.
***Organization**	Enter the organization name owning the CA.

Field	Description
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.
Configure CA Key Size and Algorithm	
CSR Generation	Select AppViewX if you are generating keys using HashiCorp Vault, else select HSM.
***Device**	This field is displayed only when CSR Generation = HSM. Select a configured device from the dropdown list.
***Key Handler Name**	This field is displayed only when CSR Generation = HSM. The field is auto-populated on selecting the device.
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.

Note:

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

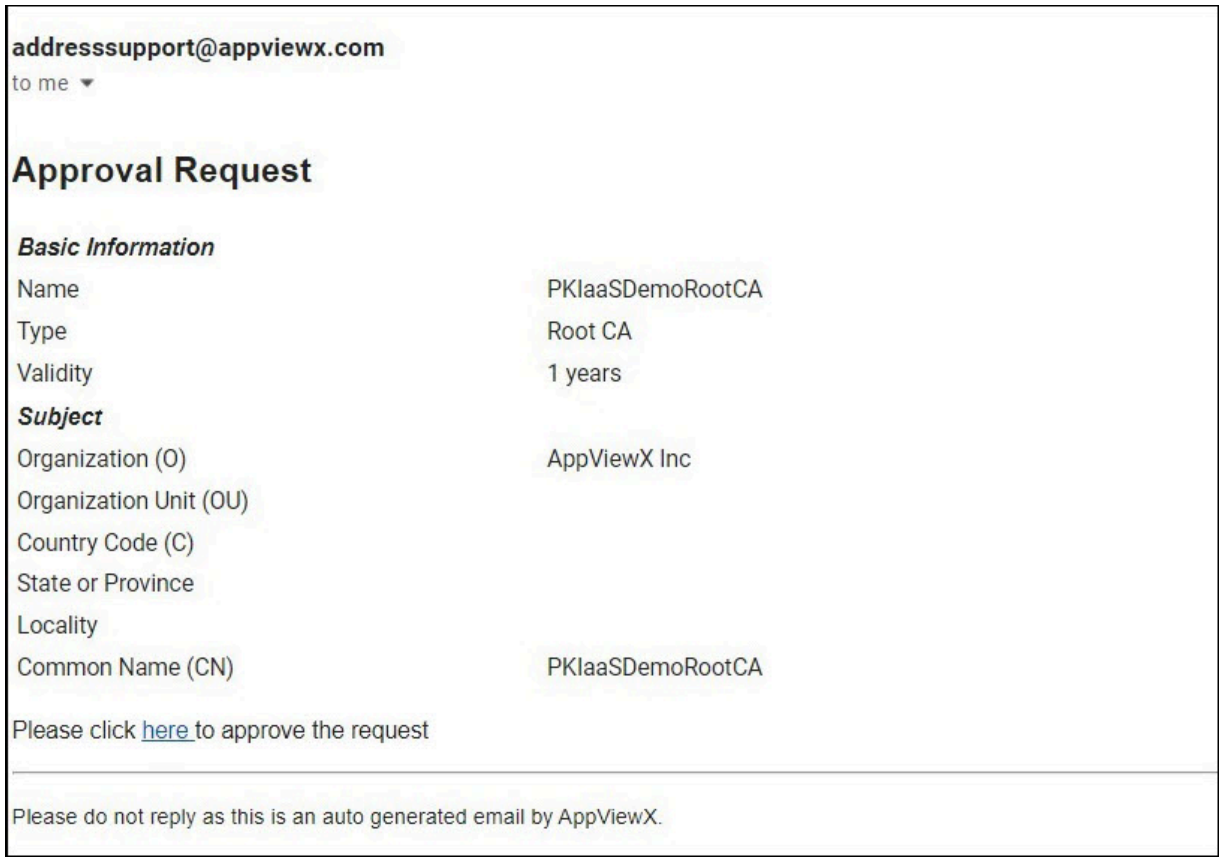
4. Click **Create.**

   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

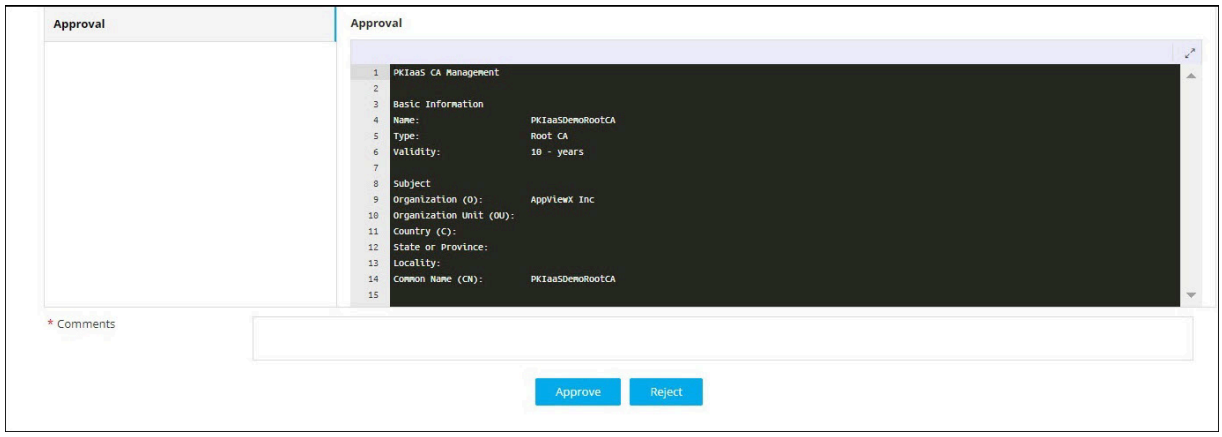
Organization (O)	AppViewX Inc
Organization Unit (OU)	
Country Code (C)	
State or Province	
Locality	
Common Name (CN)	PKIaaSDemoRootCA

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.
Tier	This is a ready-only field. In case of standard initialization, **Standard** is selected; else **AppViewX PKIaaS Native** if it was used for PKI initialization.
Certificate Authority 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 be 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.
***Template**	This field appears only if **Tier = AppViewX PKIaaS Native.** Select a template from the dropdown list.
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***CA Common Name**	Enter the root 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.

Field	Description
Configure CA Key Size and Algorithm	
CSR Generation	Select AppViewX if you are generating keys using HashiCorp Vault, else select HSM.
***Device**	This field is displayed only when CSR Generation = HSM. Select a configured device from the dropdown list.
***Key Handler Name**	This field is displayed only when CSR Generation = HSM. The field is auto-populated on selecting the device.
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.
Configure CA Artifacts	
Path Length Constraint	This is an optional parameter in an issuing CA certificate; it defines the number of sub CA chain created under that specific issuing CA certificate holding the path constraint value. This field can have any of these values: 0, 1, 2, 3, or none. For example, if it is set to **2**, it means that only two intermediate CAs are allowed between the end-entity certificate and the root certificate. None indicates unlimited.

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.

Field	Description
Tier	This is a ready-only field. In case of standard initialization, **Standard** is selected; else **AppViewX PKIaaS Native** if it was used for PKI initialization.
Certificate Authority 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 **External** if root CA is outside of the AppViewX system.
***Template**	This field appears only if **Tier = AppViewX PKIaaS Native.** Select a template from the dropdown list.
***Valid for**	Select the number of years to CA expiry.
Configure CA Subject Name	
***CA Common Name**	Enter the root 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.
Configure CA Key Size and Algorithm	
CSR Generation	Select AppViewX if you are generating keys using HashiCorp Vault, else select HSM.
***Device**	This field is displayed only when CSR Generation = HSM. Select a configured device from the dropdown list.
***Key HandlerName**	This field is displayed only when CSR Generation = HSM. The field is auto-populated on selecting the device.
***Key Size and Algorithm**	Select the CA key size and algorithm from the dropdown list.
Configure CA Artifacts	

Field	Description
Path Length Constraint	This is an optional parameter in an issuing CA certificate; it defines the number of sub CA chain created under that specific issuing CA certificate holding the path constraint value. This field can have any of these values: 0, 1, 2, 3, or none. For example, if it is set to **2**, it means that only two intermediate CAs are allowed between the end-entity certificate and the root certificate. None indicates unlimited.

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

Prerequisites

Prior to performing any action on the CA, ensure that you have necessary role-based access controls and workflow access pertaining to the CA request.

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

- Disable
- Enable
- Delete

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 is 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

Before you begin:

- Remove the CA you want to delete from any auto-enrollment settings, policies, or workflows that are used to issue or revoke certificates from that CA.
- 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.

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.

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:
   - If you are deleting a PKIaaS subordinate CA and if there are valid certificates issued by the CA, then you get a message that you must first revoke the certificates and the CA certificate before deleting the CA. The revocation of certificates is permanent and not reversible. Click **Continue** to view the certificates that will be revoked. Click **Revoke and Delete CA.**
   - If the CA has no active certificates, then 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.**
4. 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 performed successfully appears.

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

Validation Authority

Certificate authorities use Online Certificate Status Protocol (OCSP) to get 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 for verification against a trusted certificate authority. The OCSP server then returns a response indicating whether the certificate is good, revoked, or unknown.

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.
- For on-premise deployment, configure OCSP as explained here.

You can select one or more certificates from the inventory and click **Actions > Revocation Check** to perform revocation validation. After successful validation, the certificate status is reflected through color-coding in the Common Name column.

- CRL Profiles
- OCSP Profiles

CRL Profiles

Note:

- This module is available starting from the Thames HF2 (2024.0.2.0) release for those using AppViewX PKIaaS Native CA for PKI initialization.
- CRL routed via CC will work only with the latest version of CC.

CRL Scheduler

The CRL scheduler ensures that CRLs for root and subordinate CAs are automatically generated and updated at regular intervals as defined by the CA's policies. The frequency of updates may depend on the CA's configuration (e.g., daily, weekly, etc.). To do it manually, click **Publish Now** in **Actions**.

Note:

The **CRL Scheduler** and **Actions** are available only for AppViewX Private CA. Ensure that you have necessary role-based access controls and workflow access to publish CRL.

Enter the following details:

Fields for CRL Scheduler

Field	Description
***Timezone**	Select a timezone from the dropdown list.
Starts on	Select a start date and time by clicking the calendar.
***Frequency**	Select the frequency as daily, weekly, or monthly.
***Days of Week**	This field appears only for root CA. Select the days of the week you want the scheduler to run.
***Overlap Period**	Select the overlap period in days or weeks.

Note:

Field marked with red asterisk (*) symbol are mandatory.

• CRL Scheduler

CRL Scheduler

The CRL scheduler ensures that CRLs for root and subordinate CAs are automatically generated and updated at regular intervals as defined by the CA's policies. The users can select different time zones based on their location. For root CA, the available frequency options are daily, weekly and monthly. For sub CA, the available frequency options are hourly, daily, weekly and monthly. Users can also manually publish the CRL for an individual CA and configure its next update time. To do it manually, click **Publish Now** in **Actions**.

Note:

The **CRL Scheduler** and **Actions** are available only for AppViewX Private CA. Ensure that you have necessary role-based access controls and workflow access to publish CRL.

Enter the following details:

Field Description for CRL Scheduler

Field	Description
***Timezone**	Select a timezone from the dropdown list.
Starts on	Select a start date and time by clicking the calendar.
***Frequency**	Select the frequency as daily, weekly, or monthly.
***Overlap Period**	Select the overlap period in days or weeks. Overlapping period refers to the number of days added to the CRL validity period when the next CRL is published.

Note:

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

OCSP Profiles

Note:

OCSP routed via CC will work only with the latest version of CC.

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.

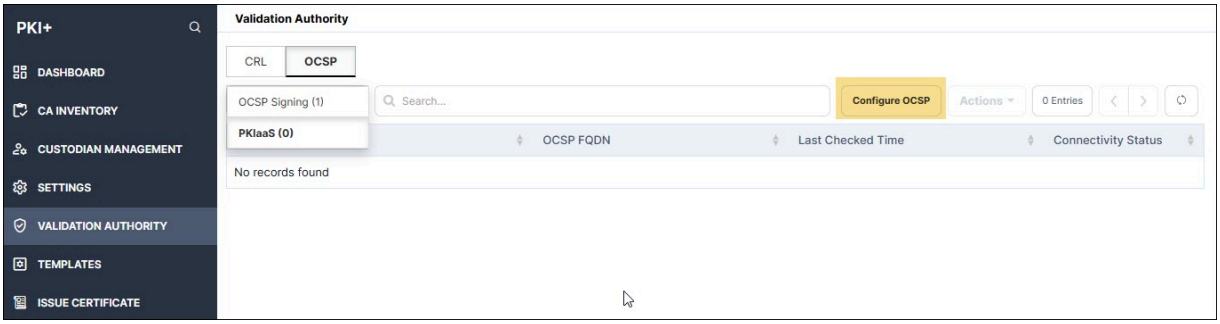
> **Note:**
>
> An OCSP signing certificate can be revoked only on deleting the CA. If an OCSP signing certificate is revoked or deleted from the **CERT+ > Certificate Inventory > Server** page, then the OCSP responder will not work. To remediate this action, you can create a new OCSP signing certificate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

- Configuring OCSP for On-Premise Deployment
- Creating OCSP Signing Certificate

Configuring OCSP for On-Premise Deployment

To configure OCSP:

1. Go to (**Menu**) icon **> PKI+ > Validation Authority.** By default, CRL is selected.
2. Click the **OCSP** tab and click **PKIaaS** from the dropdown list as shown.



3. Click **Configure OCSP.**

   The **Configure OCSP - PKIaaS** window is displayed.

4. Enter the following fields:

Field Description for Configure OCSP - PKIaaS page

Field	Description
***OCSP Name**	Provide a friendly name.
***OCSP FQDN**	Enter the node domain name where OCSP plugin is hosted.

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

5. Click **Add.** The entered information is displayed in the table.

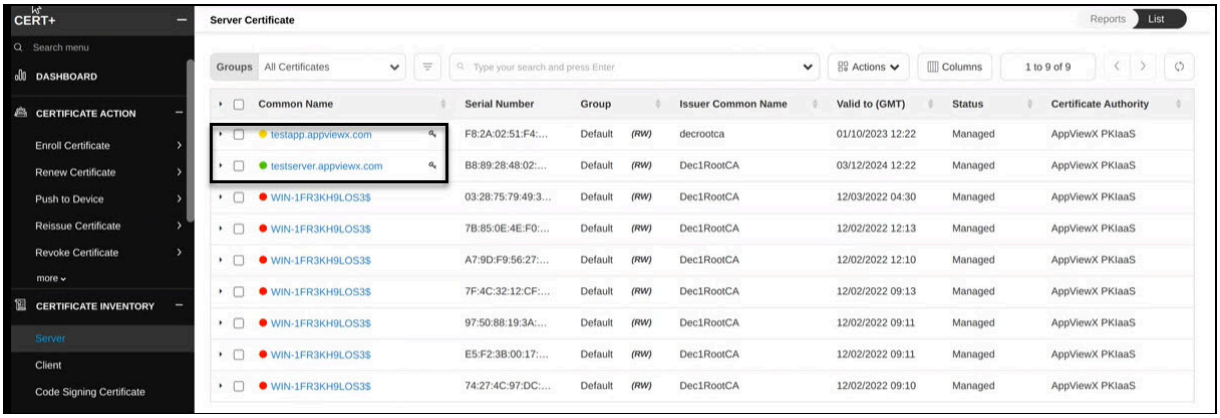
   To troubleshoot OCSP responder with openSSL, see Section, Troubleshooting OCSP Request with OpenSSL.

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.



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
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:** • Only the default admins can add key ceremony admins. • If key ceremony administrators are configured, only they have the authority to add or remove custodians. However, key ceremony administrators cannot be designated as custodians themselves. • SSO users cannot be key ceremony admins.
Issued certificate status in CERT inventory	Select any of the options: • **Monitored:** This is the default selection. Certificates that are auto-enrolled are added in the inventory as *Monitored*. • **Managed:** Certificates issued via AppViewX PKIaaS are added in the inventory as *Managed*.

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

3. Click **Save.**
4. Upload the CPS document.

Fields for CPS Upload section

Field	Description
***Upload CPS**	A CPS (Certification Practice Statement) is a comprehensive document that defines the practices, procedures, and responsibilities of a Certificate Authority (CA) in issuing and managing digital certificates. It offers transparency into the CA's operations, detailing how certificates are requested, validated, issued, renewed, revoked, and how the CA ensures the security and integrity of these processes. The CPS is a critical element in PKI that establishes the trust framework governing the CA's activities. It is especially important for auditors, relying parties (those who verify certificates), and relying organizations to understand the CA’s operational procedures, security safeguards, and risk management strategies. Download the sample CPS document, make edits according to their organization policies, and then upload it.
Note: Field marked with red asterisk (*) symbol are mandatory.	

What to do next:

Onboarding Custodians

For Standard Initialization

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 to establish connection with PKIaaS.
***Default Region**	Select a default region to create a CA.
Email ID 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 administrators. **Note:** • Only the default administrators can add key ceremony administrators. • If key ceremony administrators are configured, only they have the authority to add or remove custodians. However, key ceremony administrators cannot be designated as custodians themselves. • SSO users cannot be key ceremony administrators.
Issued certificate status in CERT inventory	Select any of the options: • **Managed:** Certificates issued via AppViewX PKIaaS are added in the inventory as *Managed*. • **Monitored:** This is the default selection. Certificates that are auto-enrolled are added in the inventory as *Monitored*.

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

3. Click **Save.**

For PKIaaS Native Initialization

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

Field Description for General Settings section

Field	Description
Key Ceremony Admins	Select two key ceremony administrators. **Note:** • Only the default administrators can add key ceremony administrators. • If key ceremony administrators are configured, only they have the authority to add or remove custodians. However, key ceremony administrators cannot be designated as custodians themselves. • SSO users cannot be key ceremony administrators.
Issued certificate status in CERT inventory	Select any of the options: • **Managed:** Certificates issued via AppViewX PKIaaS are added in the inventory as *Managed*. • **Monitored:** This is the default selection. Certificates that are auto-enrolled are added in the inventory as *Monitored*.

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

3. Click **Save.**
4. Upload the CPS document.

Fields for CPS Upload section

Field	Description
***Upload CPS**	A CPS (Certification Practice Statement) is a comprehensive document that defines the practices, procedures, and responsibilities of a Certificate Authority (CA) in issuing and managing digital certificates. It offers transparency into the CA's operations, detailing how certificates are requested, validated, issued, renewed, revoked, and how the CA ensures the security and integrity of these processes. The CPS is a critical element in PKI that establishes the trust framework governing the CA's activities. It is especially important for auditors, relying parties (those who verify certificates), and relying organizations to understand the CA’s operational procedures, security safeguards, and risk management strategies. CP and CPS are configurable under templates as per the customer policies. Customers can also upload their CPS document (.pdf) to PKIaaS for hosting. In this case, the CPS URL will be auto generated while template configuration. The certificate policy link present in the template will be part of the issued certificate's policy extension.

Field	Description
	Note: If you are using AppViewX to host, then by default the URI is generated for the template that is reflected in the certificate, so the default URI has to be retained as is. If any changes are made, then those changes will be reflected in the certificate and the CPS will not be hosted.

Note:

Field marked with red asterisk (*) symbol are mandatory.

Templates

Note:

- This module is available starting from the Thames HF2 (2024.0.2.0) release for those using AppViewX PKIaaS Native CA for PKI initialization.
- For versions prior to Thames FP1 HF3, enable **Templates** function by going to (**Menu**) icon **> Platform > Role.** Search for the created administrator role and click the link. Switch to the **Authorized functions** tab, and select the **Templates** check box in the PKI module.

You can either use any of the existing templates or create a customized template to specify certificate parameters.

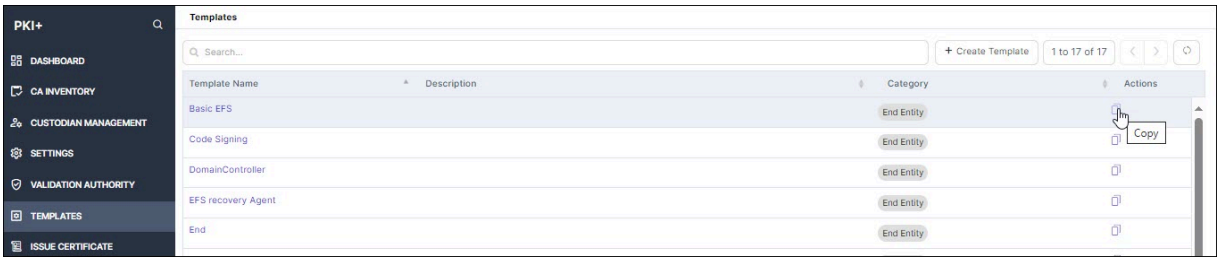
Using Existing Templates

To use existing templates:

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

   The **Templates** page is displayed with pre-existing templates to choose from.

2. Select a template that best suits your needs and click the **(Copy)** icon in the **Action** column to create a copy of the selected template.



A copy of the selected template is displayed.

3. Edit the fields and click **Save**.

The newly created template appears on the home page of **Templates**.

4. To delete the template, click the **Delete** icon against the selected template.

> **Note:**
>
> You can only delete the templates that you created.

Creating Custom Templates

You can create **custom templates** using **AppViewX PKIaaS Native CA** offers a wide range of benefits, including enhanced security, consistency, scalability, and ease of use. By aligning the certificate issuance process with your organization's specific requirements, you can optimize the management of digital certificates and strengthen your overall PKI environment. Custom templates help ensure compliance, reduce errors, and streamline the certificate lifecycle, making the process more efficient and secure for your organization. You can either use any of the existing templates or create a customized template to specify certificate parameters.

To create custom templates:

1. Click **+ Create Template** on the top right corner of the screen.

The **Templates** page is displayed.

2. Enter the following information:

Field Description of Templates Section

Field	Description
General	
***Template Name**	Provide a name for easy reference.
Description	Provide particulars on template creation as to who created it, when it was created, and why it was created.
Category	Select any of the options: • Root CA • Sub CA • End Entity (default value) **Note:** This field is not editable once the template is created.
Validity Offset	This is the value provided to adjust the start date of certificate validity. By default, it is -10 minutes from the current time.
Basic Constraint Details	
Critical	Select this option to indicate the information in an extension is important.
Key Usages	
Critical	Select this option to indicate the information in an extension is important.
Basekey Usage	Select a value from the dropdown list that defines the functional purpose of the certificate.
Extended Key Usages	
Critical	Select this option to indicate the information in an extension is important.
Extended Key Usage	Select a value from the dropdown list that defines the application usage of the certificate.
Enable Custom	Select this option to provide custom EKU values in the text box below. Multiple entries must be separated by a comma.
Custom Extensions	

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enable Custom Extensions</td><td>Based on your organization needs, you can add more custom extensions that will be included in every certificate issued using this template.

<table><tr><th>Field</th><th>Description</th></tr><tr><td>OID</td><td>OIDs are used to define specific certificate policies in a Certification Practice Statement (CPS). Each policy has a unique OID.

An OID (Object Identifier) is a globally unique identifier used to represent specific objects, attributes, or policies in systems like PKI, LDAP, SNMP, and more. It follows a dot-separated numeric format that uniquely identifies each object in a hierarchical structure.</td></tr><tr><td>Encoding Type</td><td>Specifies the format in which the custom extension date is encoded. Select a value from the dropdown list based on your data requirements and usage context.</td></tr><tr><td>Value</td><td>Provide the field value. You can give any value for the provided custom OID.</td></tr><tr><td>Critical</td><td>Select this option to indicate the information in an extension is important.</td></tr></table>
On clicking Add, the data is populated in a table.</td></tr>
<tr><td colspan="2">Certificate Policy</td></tr>
<tr><td>Enable Certificate Policy</td><td>Certificate Policy specifies the policy under which a certificate was issued. On enabling it, the following fields are displayed.

<table><tr><th>Field</th><th>Description</th></tr><tr><td>Inherited from CA</td><td>Select this option to indicate it was inherited from CA.</td></tr><tr><td>Critical</td><td>Select this option to indicate the information in an extension is important.</td></tr></table></td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Additional Policies</td><td>Enable this option if you want to create custom policies as CPS URI or User Notice Text. Provide OID, type, and value. Click Add for the data to be populated in a table.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Subject Alternative Names</td></tr>
<tr><td>Critical</td><td>Select this option to indicate the information in an extension is important.</td></tr>
<tr><td>Field Name</td><td>Select value as DNSName, IPAddress, Email, or URI.</td></tr>
<tr><td>Encoding Type</td><td>Select a value from the dropdown list.</td></tr>
<tr><td colspan="2">Other Extensions</td></tr>
<tr><td>Authority Key ID</td><td>Sha1 hash of the issuer public key. By default, this is enabled.</td></tr>
<tr><td>Subject Key ID</td><td>Sha1 hash of the subject public key. Select hash value as 60 or 160 bit. By default, this is enabled.</td></tr>
<tr><td>Enable CRLDP</td><td>Enable to add CRLDP to the certificate for status verification. By default, this is enabled only for sub CA and end entity categories.</td></tr>
<tr><td>CA defined CRL Distribution Point</td><td>This field appears only for sub CA and end entity categories. This is selected when Enable CRLDP is enabled.</td></tr>
<tr><td>Custom CRL Distribution Point URI</td><td>This field appears only when Enable CRLDP is enabled. Provide custom CRL URLs in the text box below. Multiple entries must be separated by a comma.</td></tr>
<tr><td>Enable AIA</td><td>By default, this is enabled for sub CA and end entity categories.</td></tr>
<tr><td>Issuer Certificate download link</td><td>This field appears only for sub CA and end entity categories. You can disable this option to remove the issuer certificate link from the certificates issued using this link.</td></tr>
<tr><td>CA defined OCSP link</td><td>By default, this is enabled for sub CA and end entity categories. Enable this for issuer defined OCSP.</td></tr>
<tr><td>Custom OCSP URI</td><td>Enable this for user defined OCSP. Select this option to provide custom OCSP URLs in the text box below. Multiple entries must be separated by a comma.</td></tr>
</table>

3. Click **Save**.

   The newly created template appears on the home page of **Templates**.

Issue Certificates

Note:

- This module is available starting from the Thames HF2 (2024.0.2.0) release for those using AppViewX PKIaaS Native CA for PKI initialization.
- For versions prior to Thames FP1 HF3, enable **Issue Certificate** function by going to (**Menu**) icon **> Platform > Role.** Search for the created administrator role and click the link. Switch to the **Authorized functions** tab and select the **Issue Certificate** check box in the PKI module.

Once you have created a template, you can issue certificates by generating a **Certificate Authority (CA)** and signing a **digital certificate** for an entity (such as a user, device, server, or application). This certificate serves as proof of identity and facilitates secure communication, authentication, and encryption in a PKI-enabled system.

1. Go to (**Menu**) icon **> PKI+ > Issue Certificate.**

   The **Issue Certificate** page is displayed.

2. Enter the following information:

Field Description for Issue Certificate section

Field	Description
***CA Name**	Select the CA name from the dropdown list.
Certificate Type	Select the certificate type as end certificate or CA certificate. By default, end certificate is selected.
***Template**	Select a template from the dropdown list.
***Validity**	Select the certificate validity in years, months, or days.
***Upload CSR**	Browse and upload the CSR.

Field	Description
***Certificate Download Format**	Select the format for the certificate to be downloaded.

Note:

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

3. Click **Issue Certificate.**

   The certificate will be issued with the selected parameters.

Chapter 5: 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 6: Managing Certificates

Short-Lived Certificates

Short-lived certificate refers to an SSL/TLS certificate that is issued with a very short validity period, typically ranging from a few days to a few months. These typically reduce the risk associated with certificates that might be compromised or misused over time. By limiting their validity, the attack surface is minimized because certificates are rotated more frequently.

Benefits of Short-Lived Certificates

- **Improved Security**: Short-lived certificates lower the impact of a potential compromise since certificates are valid only for a short period.
- **Encourages Automation**: With shorter validity periods, the use of automated tools (like **ACME protocol** for certificate management and many more MDM tools) becomes more common. This encourages the automation of certificate renewal, which reduces human errors and increases operational efficiency.
- **Faster Revocation**: If a certificate is compromised, revocation becomes more effective because the certificate will expire quickly anyway.

Long-Lived Certificates

Certificate Group

Prerequisites

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 (inherited 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.
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.

Field	Description
	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.

- For Standard Initialization
- For PKIaaS Native Initialization

For Standard Initialization

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 the 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 CA details

Field	Description
***CA Accounts**	Select the CA account name configured during initialization.

Field	Description
Certificate Issuance From	Select Issuer Name.
***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.
***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 wildcard 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.
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 CA 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.

   Based on your selection, there will be a compliance report created under the dashboard for the list of certificates along with its non-compliant parameters relevant to this policy.
9. 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.

For PKIaaS Native Initialization

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.

Field	Description
Description	Enter the policy information.
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 CA details

Field	Description
***CA Accounts**	Select a CA account from the dropdown list.
Certificate Issuance From	By default, Issuer Name is selected.
***Issuer Location**	Select a location from the dropdown list.
Template Name(s)	Select the templates from the dropdown list.
***Validity**	Enter a value and press Enter.
***Bit Length-Key Type**	Select a value from the dropdown list.
***Hash Function**	Select a value from the dropdown list.
***Key Versions**	Applicable only for Sphincs+.

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.

Field	Description
Email	The email contact details of the person responsible for maintaining the certificate.
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 CA 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.

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. • **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.

Field	Description
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.

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 cases, 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 valid.
Red	Certificate has expired.
Gray	Certificate is new.
Blue	Certificate will expire in 90 days.
Yellow	Certificate will expire in 30 days.
Orange	Certificate will expire in 10 days.
Black	Certificate is revoked.

Auto-Enrollment Protocols

AppViewX CERT+ enables certificate auto-enrollment by automating all the steps involved, including CSR generation, domain ownership verification, certificate download, and provisioning, making the process efficient, scalable, and secure. AppViewX CERT+ supports all major auto-enrollment protocols including – ACME, EST, SCEP, CMP, WAEP, and Microsoft Intune. Automating certificate enrollment reduces human error, outages, and security compromises, while improving productivity.

Auto-enrollment protocols are standardized enrollment mechanisms accepted across a wide range of enterprise systems for device and application certificate enrollment. Systems leveraging Auto-enrollment protocols typically expect minimum to no admin intervention. Network devices such as routers-switches, DevOps tools, and Enterprise Mobility Management platforms are typical examples of such systems.If the deployment mode is

- SaaS, deploying a cloud connector enables auto-enrollment.
- On-prem installations without cloud connectors, users should provide the AppViewX host information, which includes the IP address and port of the URL or endpoint. If their devices support auto-enrollment to a public URL, auto-enrollment is available as part of the tenant, and configuration details are provided in the documentation.

The cloud connector is advised for DMZ-based deployments or for enrollment through your cloud connector. This is especially useful in scenarios where endpoints cannot communicate with a public URL for auto-enrollment through a private channel, necessitating the use of the cloud connector.

- EST
- ACME
- SCEP
- MS Intune
- CMP
- WAEP

For more information, refer to the CERT Guide.

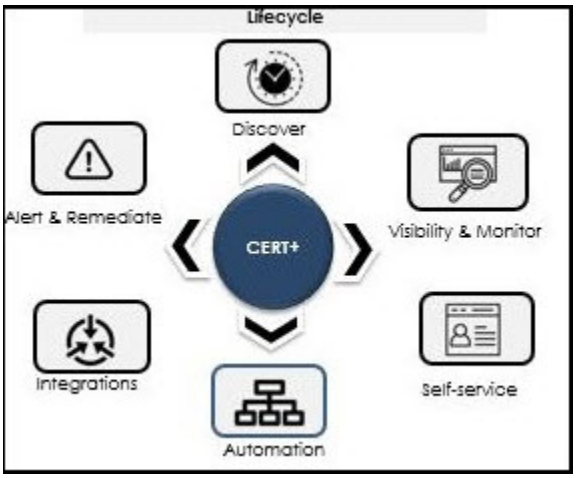
Service Catalogs

AppViewX's Page builder tool gives you step-by-step instructions on creating custom pages, incorporating various page elements like HTML pages, reports, workflow catalogs, forms, tables etc to suit user-specific requirements. or more infomaton, refer to the CERT Guide.

Chapter 7: 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:

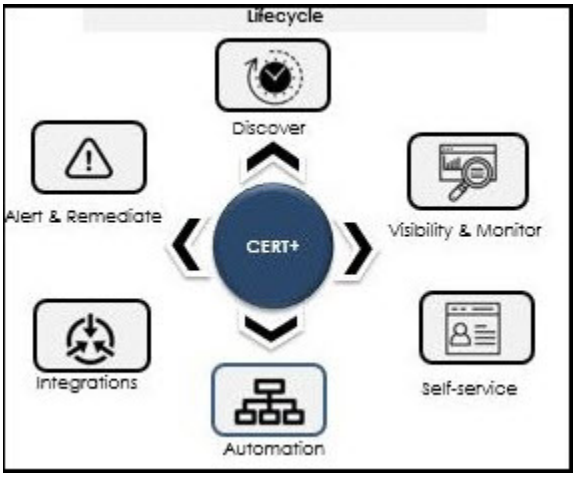


- **Certificate Discovery & Inventory Management**: Allows users to discover certificates across the network and manage inventory of all certificates in one place.
- **Visibility and Monitoring**: Enables the user to monitor certificate expiry and usage. The monitored data is represented as a detailed 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 longer necessary for business.
- **Certificate Audit**: Track and audit the usage, creation, expiration, and revocation of certificates. Track user interaction with the platform.

What is Certificate Lifecycle Management (CLM)?

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 longer 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.
10. 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.*

11. Click **Implement.**
12. 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**.
13. 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.*
14. On the **Renew Certificate** popup window, select the type of certificate renewal as **Now** or **Set auto-renew**.
15. 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.

Field	Description
	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.
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.

Field	Description
***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 8: Business Continuity and Key Security Mechanism

Backup and Recovery and Business Continuity

AppViewX Backup and Recovery and Business Continuity are key features designed to ensure that AppViewX PKI (Public Key Infrastructure) and other AppViewX services remain operational and secure, even in the event of system failures or disasters. These features help maintain the availability, integrity, and reliability of critical cryptographic and certificate management processes in on-premises environments.

Here’s an overview of Backup and Recovery and Business Continuity:

Key Aspects of AppViewX Backup and Recovery:

1. Configuration Backup:
   - AppViewX backs up all configuration settings, including user roles, policies, certificate templates, CA (Certificate Authority) configurations, and other operational settings.
   - This ensures that even if the system crashes or the configuration is lost, you can restore it quickly without manual reconfiguration.
2. Certificate & Key Store Backup:
   - AppViewX can securely back up the certificate inventory and cryptographic keys (both public and private keys) used in the PKI infrastructure.
   - Backups ensure that certificates can be reissued, renewed, and redeployed without the risk of losing access to critical certificates or keys.
3. Database Backup:
   - AppViewX relies on a centralized database to store critical data such as logs, audit trails, certificate information, and configuration details.
   - Regular database backups ensure that if there’s a database corruption or failure, the data can be restored to its most recent state without loss.
4. Automated and Manual Backups:
   - The system can be configured for automated backups at defined intervals (e.g., daily, weekly, monthly) to reduce the risk of data loss.
   - Administrators can also trigger manual backups based on specific needs, such as before a major system update or change.
5. Offsite Backup and Disaster Recovery:
   - Backup files can be stored offsite or replicated to secondary locations to ensure data availability in case of site-specific failures (e.g., a data center outage).
   - Offsite backups provide an additional layer of protection for disaster recovery.

6. Key Backup:
   - Private keys used in the AppViewX-managed PKI (including internal CAs, certificates, etc.) can be backed up securely to ensure that even in the case of a failure, private keys remain recoverable. It ensures continuity in operations like signing certificates and key management.
7. Restoration Process:
   - The system provides easy-to-follow procedures for restoring from backups, ensuring minimal downtime.
   - AppViewX's restoration tools enable quick recovery of the platform, including full system recovery or targeted recovery of specific data, configurations, or keys.
8. Granular Recovery Options:
   - Users can choose to restore entire systems, specific configurations, or individual certificates and keys.
   - This granular control enables efficient recovery and reduces the time needed to get the system back to full functionality.

For more information, refer to these sections.

Key Security Mechanism

In **AppViewX** , **Key Security Mechanism** refers to the set of processes and technologies used to protect the cryptographic keys (especially private keys) that are central to the operation of a **Public Key Infrastructure (PKI)**. These mechanisms ensure that keys, including **private keys** used by **Certificate Authorities (CAs)**, **servers**, and **end-user devices**, are stored securely and managed in compliance with industry standards and best practices.

AppViewX PKI offers several key security mechanisms that help to safeguard sensitive cryptographic data, ensure the integrity of digital certificates, and maintain the confidentiality of key material.

AppViewX PKI is a powerful, flexible, and automated platform designed to streamline the management of **PKI** infrastructure, ensuring **security**, **compliance**, and **operational efficiency** across an organization's certificate and key management ecosystem. It is ideal for large enterprises, cloud environments, and organizations that require seamless certificate management across diverse infrastructure components.

Chapter 9: Reporting and Monitoring

Reporting and Monitoring

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

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

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

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.

Alerting and Logging

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 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.

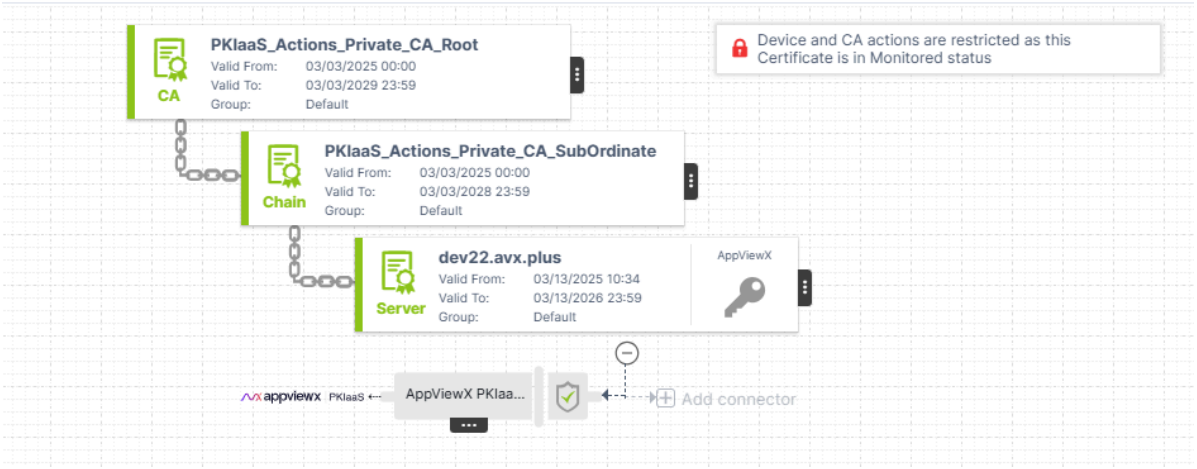
Chapter 11: Troubleshooting

For more information to troubleshoot some common problems that can occur while executing CLM actions, refer to the CERT Troubleshooting Guide.

Troubleshooting OCSP Request with OpenSSL

Follow these steps to test the OCSP service via CC URL: http://{CCURL}:{Scep port}/ocsp:

1. Download the immediate issuer and end certificates from the AppViewX UI with the following names:
   - PKIaaS_Actions_Private_CA_SubOrdinate - issuer.crt
   - dev22.avx.plus - cert.crt



2. Configure openSSL in the end device.
3. Trigger the following OpenSSL command with issuer.crt and cert.crt:

```
openssl ocsp -issuer issuer.crt -cert cert.crt -text -url http://pe-pltf-node66.lab.appviewx.net:30022/ocsp -noverify
```

If the certificate is revoked, the revoke status will be received in the OCSP response as shown:

```
        73:c3:2e:b4:ba:86:8f:51
-----BEGIN CERTIFICATE-----
MIIE8DCCAtqgAwIBAgIQGfAd1HQ3U6lEDbdrBXSiNzALBgkqhkiG9w0BAQswJDER
MA8GA1UECgwIQXBwVmlld1gxDzANBgNVBAMMBnN1Yl9jYTAeFw0yNTAyMjQwNTQx
MTdaFw0yNjAyMjQyMzU5NTlaMCkxETAPBgNVBAoMCEFwcFZpZXdYMRQwEgYDVQQD
DAtzdWJfY2Eub2NzcDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ+v
tt6sUEonDaqMN1ylsEXbsRS8uCiKdexoDWKTKqkkvtXdDrnjrUht694p1yX/quSY
rKXe5WD7zMqsrOsR9PLDui9LISYLiIKL424NBcm7HHUcRuKM5uEqcaBvCXhpChJS
XSxXHqsVBf23GofB0hwIerZ1wB6ITTqaUjHWw1qiOK5/rcrQexiUOeAeVHjstE7q
vMPwY7TX7EWR/WCFNiD5JpnnNL0gZB8GcVDPgUfyImhuvqGNBp9HgoqpwPsOKfTs
15Pi4uH4mxryyICy/Me7vtJutomHhyafKVM4NApEKQk2VjNZYlDSvI59hShnHV01
Q5fBdB+NGAcxNp5/9lsCAwEAAaOCARswggEXMB0GA1UdDgQWBBSrFsz60PxDIfqw
TakroVXL1gEtrDAfBgNVHSMEGDAWgBTq2vj0fYYIEsyaoBOt7LUV8LxkkDAOBgNV
HQ8BAf8EBAMCB4AwDAYDVR0TAQH/BAIwADATBgNVHSUEDDAKBggrBgEFBQcDCTBN
BgNVHR8ERjBEMEKgQKA+hjxodHRwczovLzQuMjI0LjExMS4yMzM6NDQzL2F2eGFw
aS9kb3dubG9hZC1jcmwvc3ViX2NhL2NybC5jcmwwUwYIKwYBBQUHAQEERzBFMEMG
CCsGAQUFBzAChjdodHRwczovLzQuMjI0LjExMS4yMzM6NDQzL2F2eGFwaS9kb3du
bG9hZC1pc3N1ZXIvc3ViX2NhMAsGCSqGSIb3DQEBCwOCAgEAcAm7kOqekT6/wN0R
kiHbpa4dinbemrg+3LnpSaAh/67hmNfDn1otjWurLrvkQNKS4e6yyn96Op0soU6y
2dPruL7Z5bEItLuOhfiY4+/DtvylvMrAuKv63j1fW452oOyHkM0ZD8HwPZ51yM3y
B7WdPNJGYFsM5x/Ta2glu6HFC7KcEKK7FSrZ7opx+WJ87fudt0/fEU3ei/oiKIPs
MV8HD7FXKNOQd2i5qFuLctpkkM/I813C+v/wPdoKzgwOzRZaH5hGYVpJFyJowyvM
PuE438DcGoGImEhWQH6CS8G8vPAFQ5AeD6i1Xl5EsjQ/TfQuCWlEyEdwvoFwAdqm
pSoT4qjzRfpBPdXUIuEW5qOz14Jj1tMMNIPwrkUEZX7z/8oqbc8ltJprNp9gRUxM
D8TqJoOf9rFPDIIz5Rkt5nRgW5k7bpF8N+9xTl7n18sJ8f6wQef0/KoO2DWPIHB1
ybf8FfA7yXCkjZY5M1X+MCXrg7j77gc4UmQ1p2of60AotkVozj8LDVX4XkG352bu
wMOeXff56SuUjPeyVoT9744iHQRRxPG6y5d/8OVPPFeOjcxXVesDrgUiO8aUuiuD
0bhlXzZWlZQNpO5m7rLB5quLy0++fYn3iZpE5xS5tI7t8bdmd5Jf57oARB623a3m
pkIwU3pBSt6E7Dx1c8MutLqGj1E=
-----END CERTIFICATE-----
ocsp/PKIOCSPServerSHA256RSA4096.appviewx.info.crt: revoked
        This Update: Feb 25 10:19:10 2025 GMT
        Next Update: Feb 25 10:19:10 2025 GMT
        Reason: keyCompromise
        Revocation Time: Feb 25 10:19:10 2025 GMT
```

4. Once the CC URL is accessible from OCSP, test the same with CC’s load balancer.