appviewx

PKIaaS User Guide

Version: 2021.1.0

Copyright AppViewX, Inc.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of AppViewX_v2021.1.0 PKIaaS	Nov 2021

About this Guide

This guide explains the capabilities of AppViewX PKI as a Service (PKIaaS). This guide provides step-by-step instructions to configure and manage AppViewX PKIaaS.

Audience

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

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: System Requirements

- System Requirements

System Requirements

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

- Hardware Requirements
- Operating System Requirements
- Browser Requirements

Hardware Requirements

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

- **Single Node Requirements**

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

- **Multi Node Requirements**

For deploying the OVA, ensure that you have all the prerequisites as mentioned below.

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Multi-node (master node) **Note:** One node for a single master installation and	4	4GB	100GB

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

- **Platform Bare Minimum Requirements**

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

Operating System Requirements

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

- CentOS 7.X
- RHEL 7.X

Browser Requirements

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

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

Chapter 2: What is Certificate Authority

What is Certificate Authority?

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

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

There are two types of certificate authorities:

- **Public CA:** A public CA is a third-party entity that issues certificates for a fee after doing the necessary checks on the organization requesting a certificate. The checks by default include domain validation, and Third-party CAs have their own public-private key pairs with which they sign the certificates. Most of the well-known CAs are recognized by servers and clients; therefore, certificates signed by them are immediately validated by the entity initiating a secure connection. Publicly-signed certificates offer a higher level of assurance since they are issued by a recognized CA, and are generally used for securing websites and other endpoints involving direct user interaction.
- **Private CA:** A private CA is when an organization creates its own local CA without going for an external one. In this case, the certificates are signed with the private key of the organization's root certificate (the foremost certificate created to sign other certificates). Private CAs can be created to issue certificates for an organization's internal network where discretion is required, and only a select group of users are involved. They may include VPNs, sensitive databases, secure mail servers among others.

AppViewX PKIaaS Certificate Authority

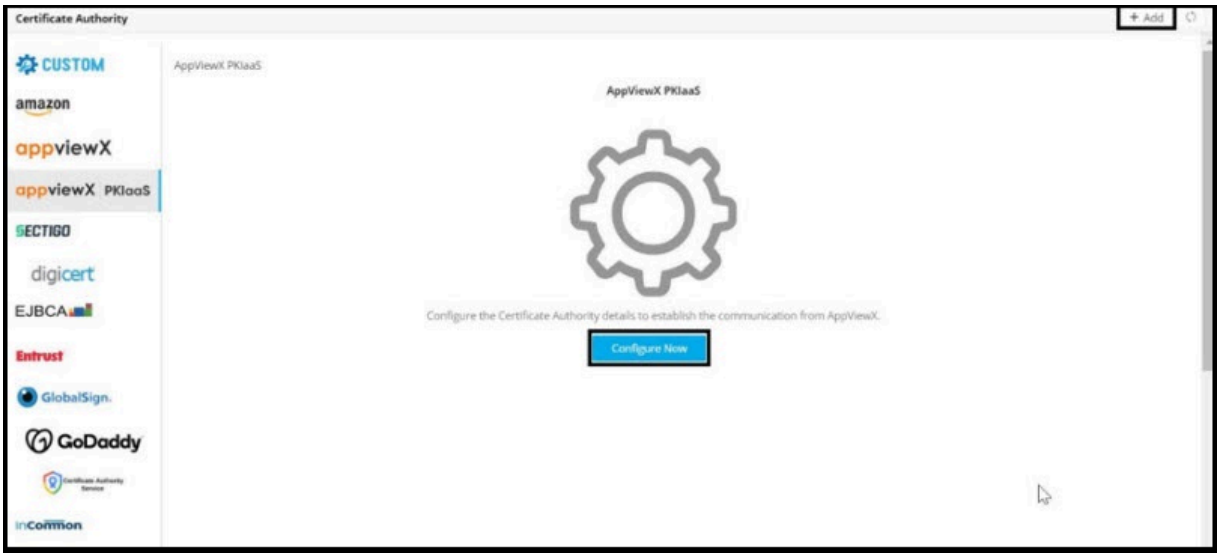
AppViewX's PKIaaS combines the convenience of a customized PKI with our powerful certificate lifecycle automation capabilities, and allows you to consume the entire solution as a service. Setting up a secure, scalable, and compliant PKI has never been easier.

Configure Certificate Authority

To configure a certificate authority:

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

   The **CERT+** left navigation pane appears.
3. Click **Certificate Authority** from **Administration** on the LHS pane.
4. Click **AppViewX PKIaaS** from the list of CA vendors.



5. Click **Configure Now.**

   The **PKIaaS** page appears.
6. Complete SMTP configuration and onboard at least two custodians before initializing PKI as a Service. You can complete the addition of custodians by going to **Menu > CERT+ > Administration > Custodian Management.** For instructions, see Section, Onboard Custodians.
7. Initialize project creation for PKIaaS by following the instructions in the Section, Prerequisites.
8. To create a root or subordinate CA, follow the instructions in the Section, Create Certificate Authority.

Validate Certificate Authority

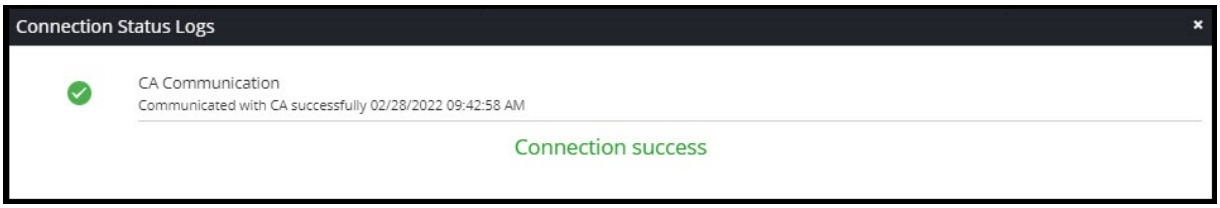
Once the **AppViewX PKIaaS** settings are added, you need to validate to check if the connection between AppViewX and **AppViewX PKIaaS** is properly configured.

To validate the **AppViewX PKIaaS**:

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

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

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



Certificate Group

- Before you Begin
- Add Certificate Group
- Edit Certificate Group

Before you Begin

Before starting **Certificate Groups** configuration:

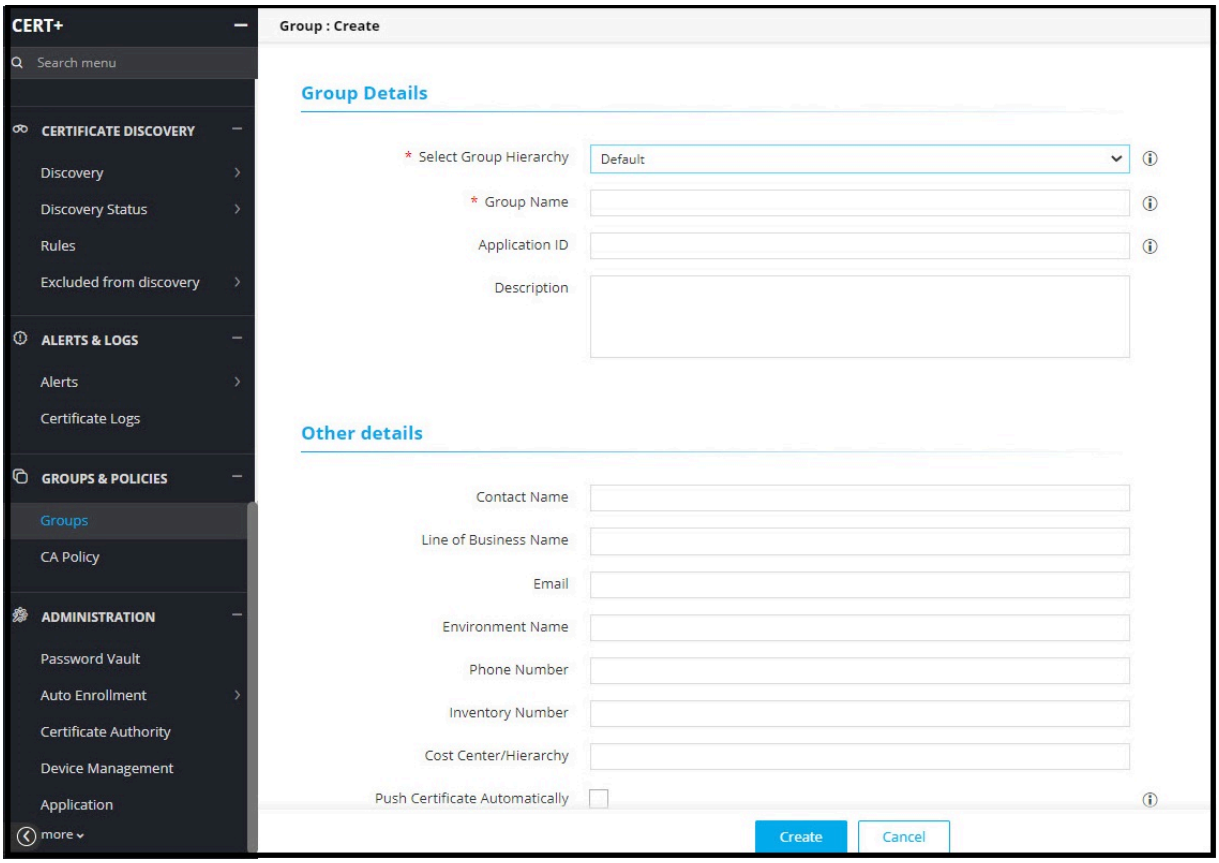
- **Certificate Groups** are used to categorize the certificates according to various **business units.**
- In some organizations, **Certificate Groups** are also used to assign access permissions. Only privileged users (inherits from Resource > User Group) can view the respective **Certificate Groups**.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

Add Certificate Group

To create a certificate group:

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

   The **Create Group** page is displayed.



5. In the **Group Details** section, enter the following details:

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.

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

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

Field	Description
Line of Business Name	Enter the name of the business unit.
Email	Enter the email address of the contact person.
Environment Name	Enter the name of the environment.
Phone Number	Enter the phone number of the contact person.
Inventory Number	Enter the number related to the inventory.
Cost Center/ Hierarchy	Enter the cost center code/ label.
Push Certificate Automatically	To associate the certificate automatically with its device, select the **Push Certificate Automatically** checkbox.
Renew Automatically	To enable automatic renewal of the certificates under this group, turn on the Renew Automatically toggle. **Note:** If you enable the automatic renewal, two more details have to be entered. The details to be entered are as follows: • **Start Renewing:** Enter a number between 1 - 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.**

7. 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.**

Edit Certificate Group

To modify a certificate group:

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

   The **CERT+** left navigation pane appears.
3. Click **Groups** from **Groups & Policies** on the LHS pane.

   The group inventory page appears.

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

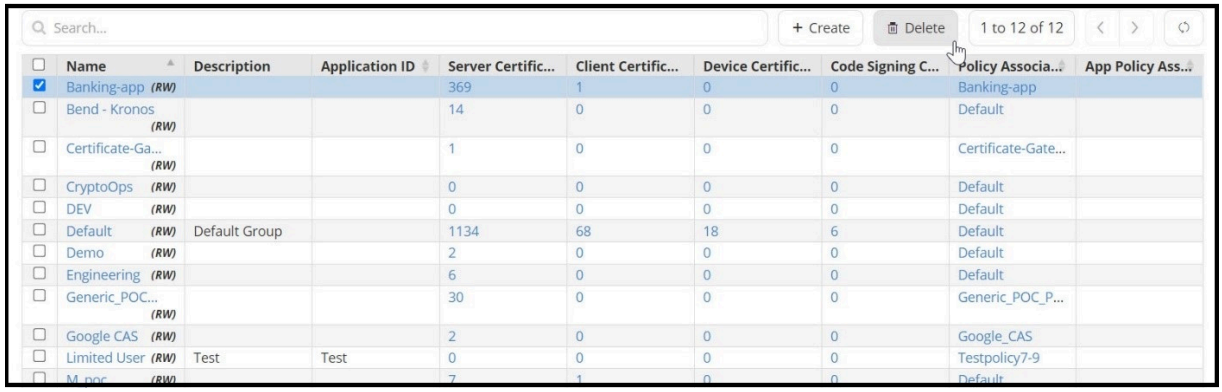
Delete Certificate Group

To delete a certificate group:

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

   The **CERT+** left navigation pane appears.
3. Click **Groups** from **Groups & Policies** on the LHS pane.

   The group inventory page appears.



4. Select the group you want to delete and click **Delete.**

   A **Confirmation** popup window appears.
5. Click **Yes**.

   The group is deleted from the inventory.

Assign or Unassign Group to Certificate

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

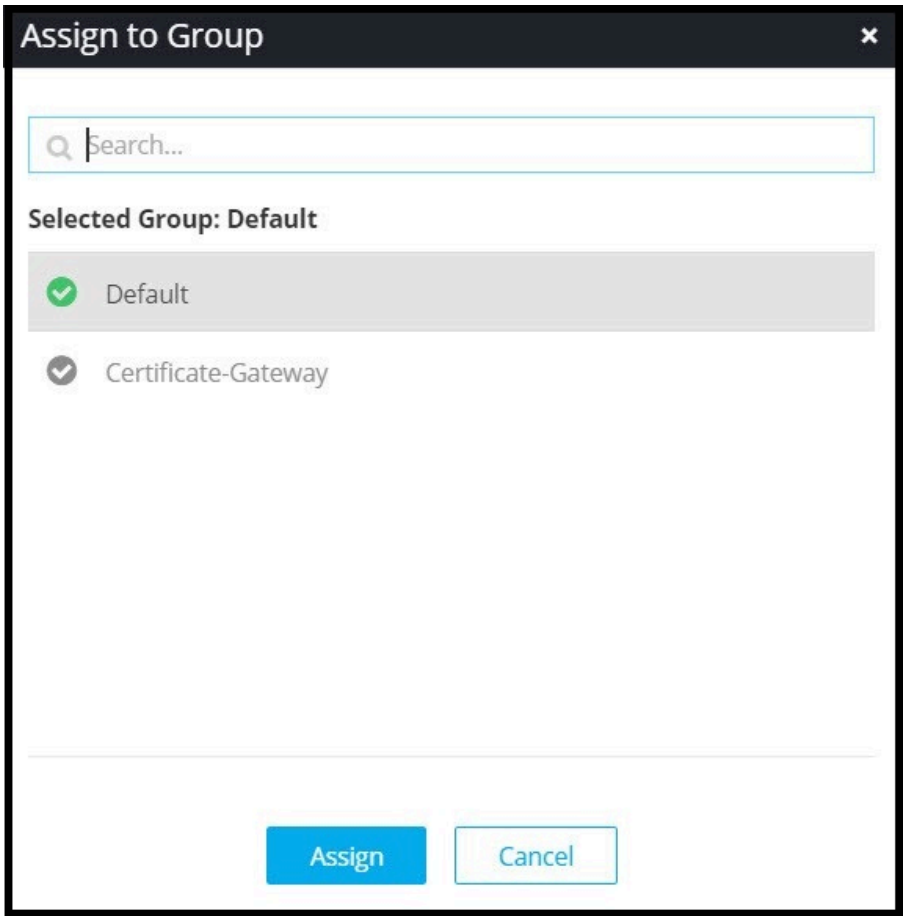
1. Click the **Menu** ( ) icon.
2. Click **CERT+**.

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



4. Select the group you want to assign to the certificate.
5. 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.

• Add Certificate Authority Policy

Add Certificate Authority Policy

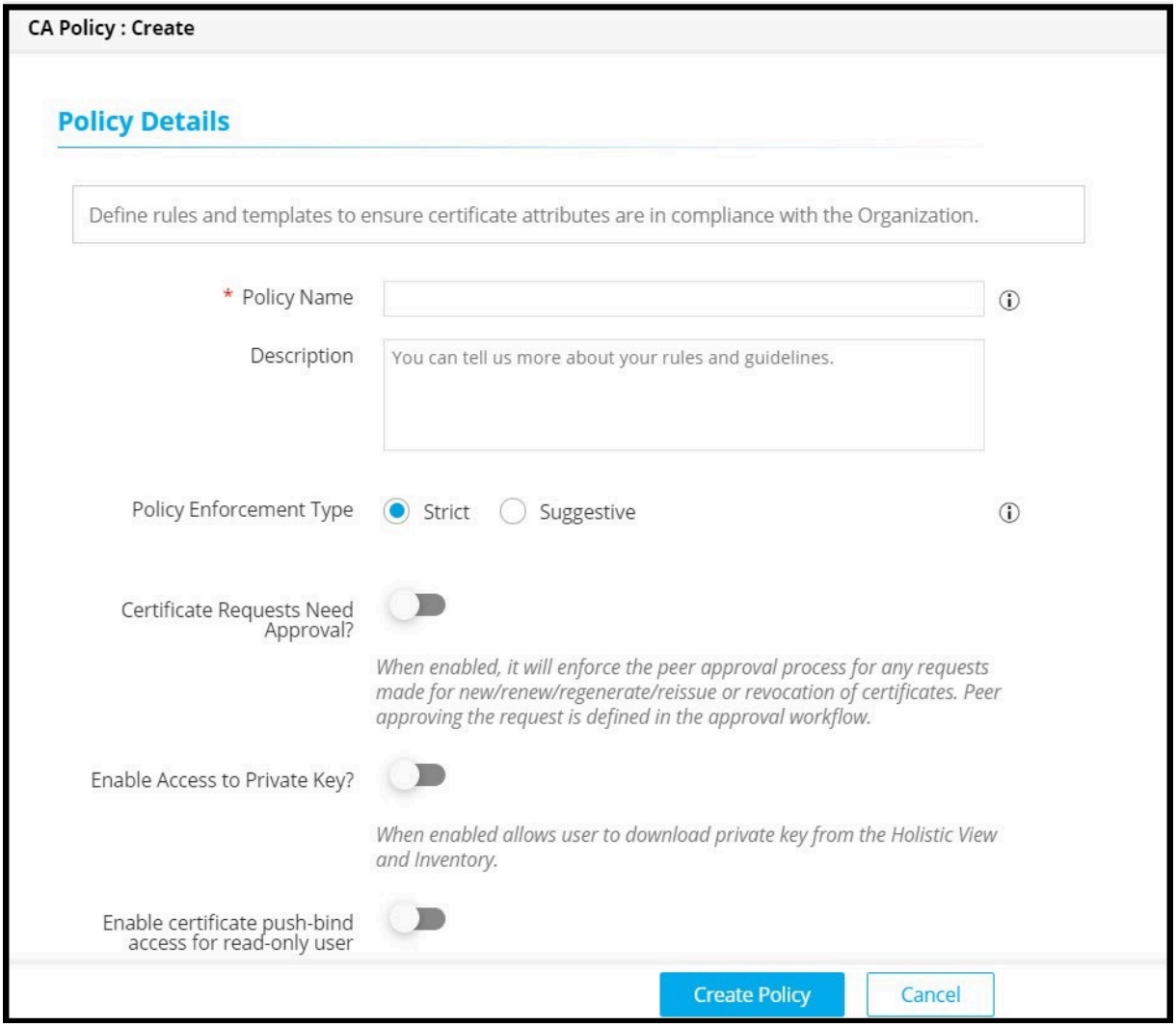
The CA policy defines rules and templates to ensure certificate attributes comply with the organization.

To create a CA policy:

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

   The **CERT+** left navigation pane appears.
3. Click **CA Policy** from **Groups & Policies** on the LHS pane.
4. Click **+ Create** in the command bar to configure certificate practice standards for business unit.

   The **Policy Details** page is displayed.

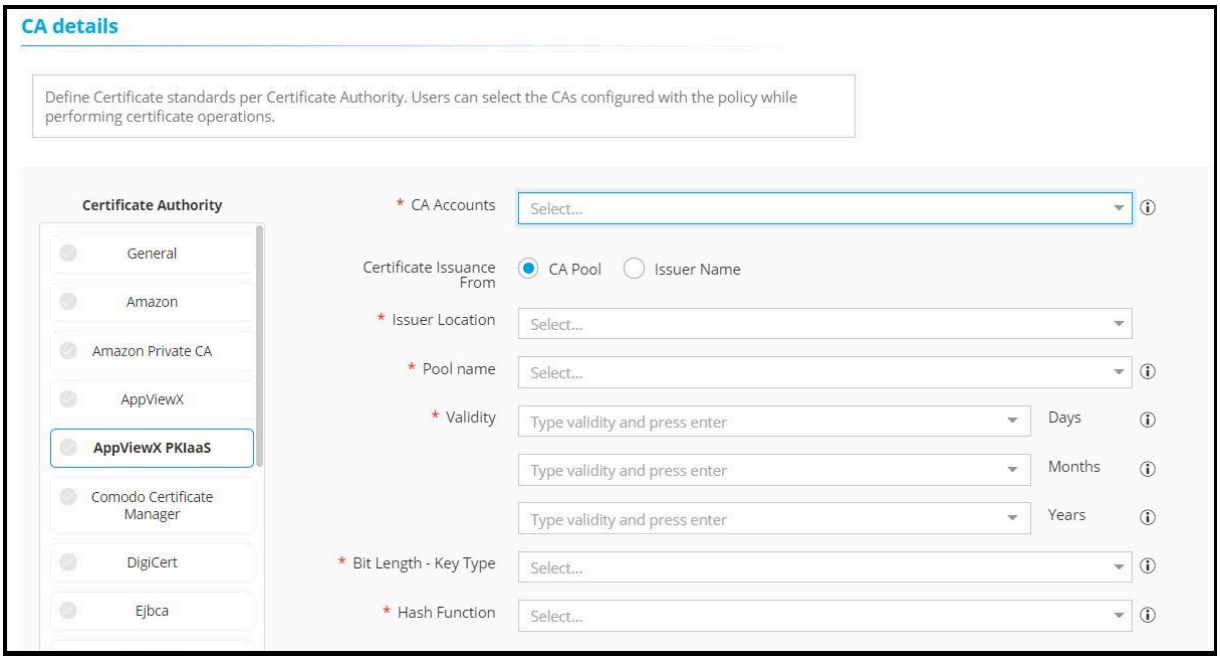


5. Enter the details as described:

Field	Description
***Policy Name**	Enter a unique name for the certificate policy.
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?	Turning on this toggle button allows private keys of the certificates to be exported.
Enable certificate push-bind access for read-only user	Turning on this toggle button allows 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?	Turning on this toggle button checks if issuer and root of the certificate are compliant to the standard defined in the policy.

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

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



Field	Description
***CA Accounts**	Select the CA to associate with the policy. Based on the CA selected, fields are populated.
Certificate Issuance From	Select either CA Pool or Issuer Name. By default, CA Pool is selected.
***Issuer Location**	Select location from the dropdown list.
***Pool Name**	Select pool name from the dropdown list. This field appears only on selecting **CA Pool** in the **Certificate Issuance From** field.
***Issuer Name**	Select issuer name from the dropdown list. This field appears only on selecting **Issuer Name** in the **Certificate Issuance From** field.
***Validity**	Select a value from the dropdown list.
***Bit Length-Key Type**	Select a value from the dropdown list.
***ECDSA curve**	Select a value from the dropdown list.
***Hash Function**	Select a value from the dropdown list.

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

Field	Description
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.
Organizational 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.

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.

Chapter 3: How Certificate Authority Works

- How Certificate Authority Works?

How Certificate Authority Works?

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

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

- Certificate Signing Request (CSR)
- Verification
- Certificate Enrollment

Certificate Signing Request (CSR)

Certificate Signing Request (CSR) is the message that is sent to the CA to get a digital certificate created. A CSR is often generated on the same server on which the certificate is to be installed. Before creating a CSR, the applicant must first generate a public-private key pair. The public key is included in the CSR and is used by the CA to create the certificate while the private key (to be kept private again) is used to sign the information contained in the CSR.

See Section, Generate CSR for Certificate.

Verification

After the CSR is generated and sent to the CA, the CA conducts a verification process before issuing the certificate. The steps involved in verification depend on the type of certificate requested.

- **For Domain Validation (DV) certificates –** if the domain name is the same as what is listed as the Common Name on the CSR, the CA verify the domain ownership themselves (although this depends on the CA. Some may require additional form-fills or other checks). If not, the CA might mail a link to a list of email addresses on the domain (administrator@, webmaster@) with a verification link, clicking

on which will prove domain ownership. Further steps depend on the CA handling the request. These certificates typically take a few minutes to be issued.

- **For Organization Validation (OV) and Extended Validation (EV) certificates –** these certificates entail more verification steps. Here, the CA verifies the physical existence and eligibility of the organization. This may involve visiting the organization in person, verifying the phone number and email address provided, etc., apart from domain control verification. These certificates typically take up to 3 days to be issued.

Certificate Enrollment

Enrollment is the process by which users request CAs (Certificate Authorities) to provide them with x.509 certificates. There are multiple ways by which this is usually accomplished – both manual and automation (using certain protocols) – each with their own advantages. The enrollment process usually involves the CA signing the user's key, and affixing it with an TLS certificate which can then be used to secure the user's external-facing (or internal) systems.

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

The CSR has to be sent to the CA in a certain format, which contains all the information a CA will need to verify the legitimacy of the requesting body. CAs are known for being very stringent with regards to issuing certificates to requesters *only* after they have been proven to be legitimate. CSRs usually follow PKCS #10 (Certificate Request Syntax Standard – developed by RSA), and include the following information:

- **Public Key:** The requester generates a key pair using a Cryptographic Service Provider (CSP) that is usually installed on their computer. They then send the public key to the CA.
- **Digital Signature:** The CSR is hashed using a hashing algorithm, and then encrypted with the requester's public key, resulting in the formation of a digital signature.
- **Hashing Algorithm:** The algorithm used in the previous step is also sent to the CA in order for it to decipher the request. This adds an additional layer of security and authenticity.
- **DN:** The Distinguished Name of the requester, in order to verify identity.

The requester is also obliged to send other information pertaining to domain ownership and contact information.

The CA, once it receives a CSR from a requesting body, then has to verify the legitimacy of the requester using the information provided. Once it does so, it proceeds to carry out the key signing process, which is detailed below:

- The Digital Signature is first decrypted using the requester's private key to ensure that the request has not been tampered with, in the time between the requester sending it and the CA initiating the signing process.
- The CA then uses the provided Hashing Algorithm and creates a hash of the request it just received (in other words, it creates a digital signature).
- If this new signature matches the Digital Signature provided by the requester, the CA takes it as proof that the request is valid, and moves onto the next step.
- The CA signs the requester's public key and affixes it with an x.509 certificate.
- The signed public key and the certificate are sent back to the requester, completing the issuance process.

- Post-Enrollment Usage of Certificates
- Add/Enroll Certificate
- Upload Key
- Add Certificate Authority Connector to Certificate

Post-Enrollment Usage of Certificates

Once a requester obtains a digital certificate and a signed public key, they can install this certificate onto an endpoint, which, from then on, becomes a trusted network entity.

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, once again, decrypting the digital signature provided by the CA (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).

The third party contrasts the decrypted has function against the has obtained by hashing the digital certificate. A match indicates that the certificate's owner is truly the legitimate owner of the certificate. The communicating third party can then retrieve the public key from the digital certificate, validate it, and proceed to establish a secure encrypted connection.

Chapter 4: Certificate Chain of Trust

Certificate Chain of Trust

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

Trusted root CAs are CAs that are recognized by the clients by default. Server and intermediate certificates could be signed by a CA that is not recognized by the browser. In such an event, the root CA could sign the intermediate CA, which in turn could sign the server certificate. Now if the client attempts a connection with a server that has a certificate signed by a trusted intermediate CA, the server's certificates can be traced back to the root certificate through an intermediate certificate and is thus trusted by the client.

The certificate chain simplifies key management and certificate monitoring by grouping CAs into a tree-like structure, where verifying the top or root CA automatically verifies the whole chain.

Links in Certificate Chain

Root CA

Root CAs (called trust anchors in X.509 terminology) hold the highest position in the trust tree and are recognized by all clients (browser/OS) at all levels. Root CAs are responsible for identifying intermediate CAs and verifying their trustworthiness. The root CA uses its certificate's private key to sign the certificates of the intermediate CAs (or, in the case of unchained certificates, the server certificate) under it. The trustworthiness of the root CA is thus passed down to the intermediate CAs; any CA that is validated by the root CA is automatically trusted by its clients.

Intermediate CA

The intermediate CA is the middle-man between the root and server certificates. The intermediate CA certificates are either signed by the root CA, or by another intermediate CA certificate signed by a root CA. The intermediate certificate, in turn, signs the server certificate. There is often one, or more, intermediate CA certificate in a chain. For the server certificate to be compatible with all its clients, the intermediate certificate has to be installed on the server. If not, it might prevent some browsers, mobile devices, applications, etc. from trusting the server certificate.

Server Certificate

This is the certificate that's publicly issued server to specific domains that the user needs authorization for. The server certificates are signed by the intermediate CA, and can be traced back to the root CA. When the Chain of Trust is verified, the client makes a secure connection with the server.

View Certificate Topology

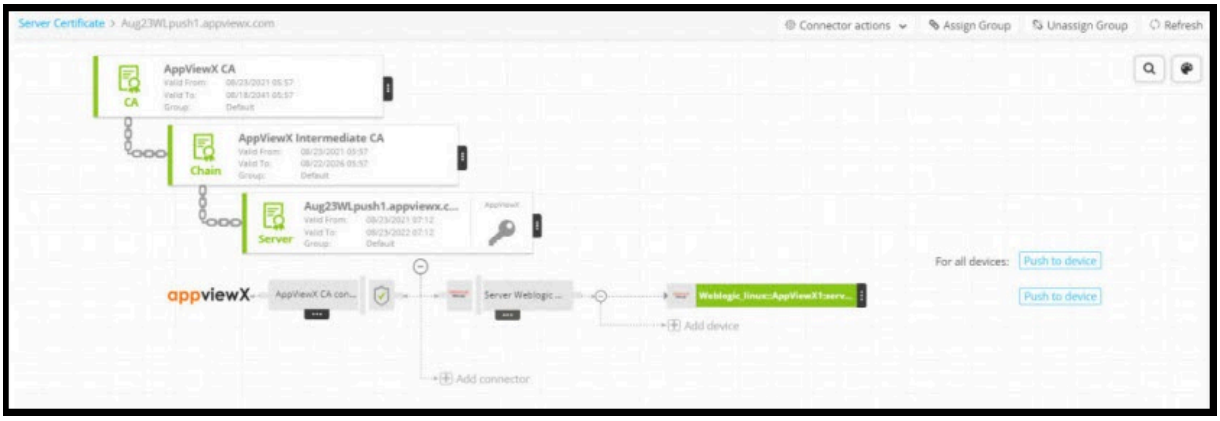
To view the topology that a server or client certificate belongs to:

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

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

3. Click **Certificate Inventory** and select the type of certificate you want to view**.**
4. On the list that appears on the screen, click the **Common Name** of the certificate.

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



Note:

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

5. Click **Refresh** ().

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

Chapter 5: Certificates

- Certificates

Certificates

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

There are three types of certificates:

- Server Certificate
- Client Certificate
- Code Signing Certificate

A digital certificate contains:

- Name of the certificate holder or the service or the individual.
- Serial Number that is used to uniquely identify certificate.
- Expiry date.
- Copy of the certificate holder's public key (used for decrypting messages and digital signatures).
- Digital Signature of the certificate-issuing authority.

- Certificate Enrollment
- Application Connector
- Push Certificate to Device

Certificate Enrollment

Enrollment is the process by which users request CAs (Certificate Authorities) to provide them with x.509 certificates. There are multiple ways by which this is usually accomplished – both manual and automation (using certain protocols) – each with their own advantages. The enrollment process usually involves the CA signing the user’s key, and affixing it with an TLS certificate which can then be used to secure the user’s external-facing (or internal) systems.

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

The CSR has to be sent to the CA in a certain format, which contains all the information a CA will need to verify the legitimacy of the requesting body. CAs are known for being very stringent with regards to issuing certificates to requesters *only* after they have been proven to be legitimate. CSRs usually follow PKCS #10 (Certificate Request Syntax Standard – developed by RSA), and include the following information:

- **Public Key:** The requester generates a key pair using a Cryptographic Service Provider (CSP) that is usually installed on their computer. They then send the public key to the CA.
- **Digital Signature:** The CSR is hashed using a hashing algorithm, and then encrypted with the requester's public key, resulting in the formation of a digital signature.
- **Hashing Algorithm:** The algorithm used in the previous step is also sent to the CA in order for it to decipher the request. This adds an additional layer of security and authenticity.
- **DN:** The Distinguished Name of the requester, in order to verify identity.

The requester is also obliged to send other information pertaining to domain ownership and contact information.

The CA, once it receives a CSR from a requesting body, then has to verify the legitimacy of the requester using the information provided. Once it does so, it proceeds to carry out the key signing process, which is detailed below:

- The Digital Signature is first decrypted using the requester's private key to ensure that the request has not been tampered with, in the time between the requester sending it and the CA initiating the signing process.
- The CA then uses the provided Hashing Algorithm and creates a hash of the request it just received (in other words, it creates a digital signature).
- If this new signature matches the Digital Signature provided by the requester, the CA takes it as proof that the request is valid, and moves onto the next step.
- The CA signs the requester's public key and affixes it with an x.509 certificate.
- The signed public key and the certificate are sent back to the requester, completing the issuance process.

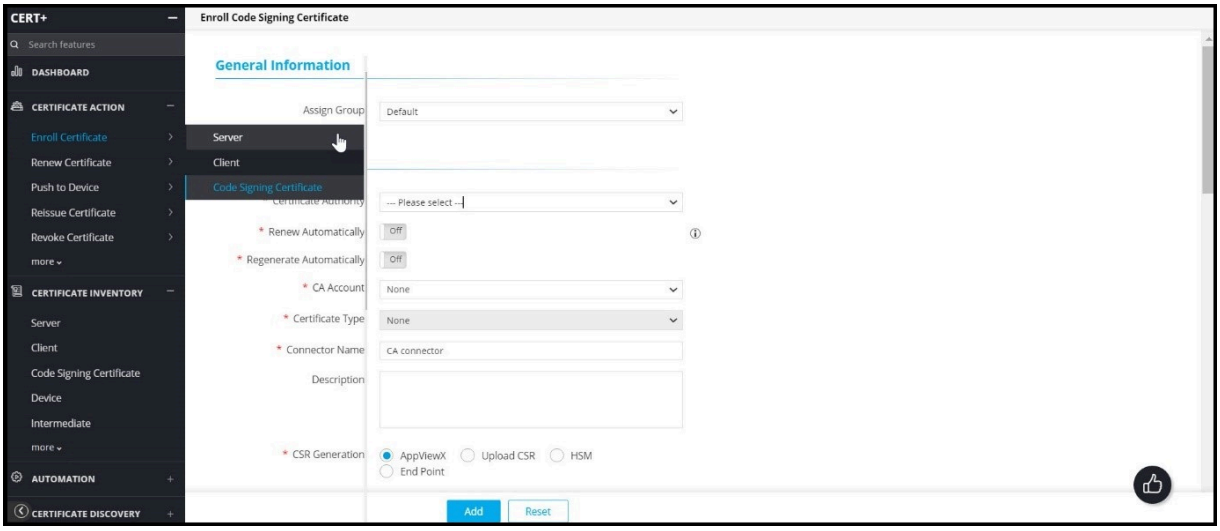
- Post-Enrollment Usage of Certificates
- Add/Enroll Certificate
- Upload Key
- Add Certificate Authority Connector to Certificate

Add/Enroll Certificate

To enroll a certificate:

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

   The **Enroll Certificate** page appears.



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

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	To which account the enrollment request is submitted.

Field	Description
Certificate Profile	Select the profile from the dropdown list.
*Issuer Location	Select issuer location from the dropdown list.
*Pool Name	This field appears when Assign Group is Default. Select the pool name 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.
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.

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

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.

Field	Description
	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.
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.
***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.

Field	Description
***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.

8. 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.

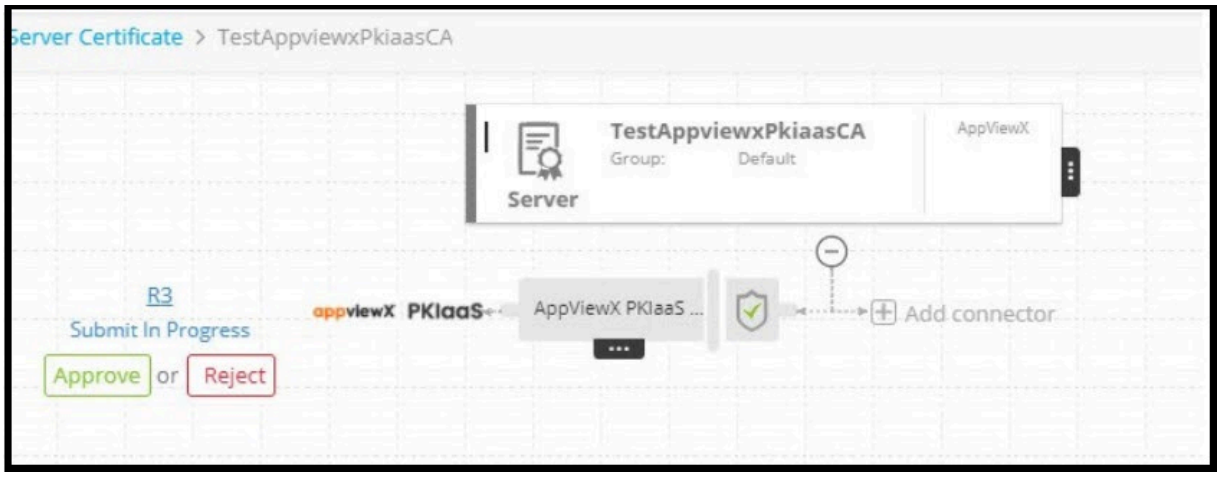
The following table describes the options available in the attachments section.

Field	Description
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.

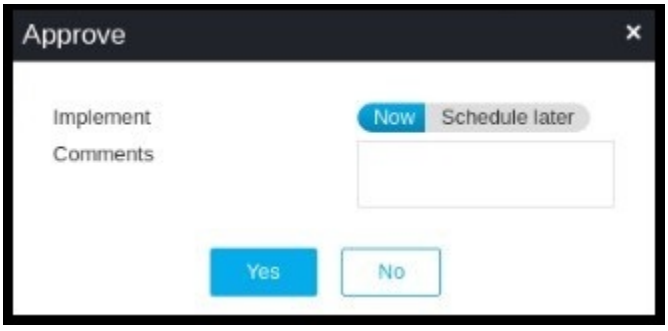
9. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example: cost center. Inventory can be filtered based on these attributes as well. If the Certificate Attributes are added under **Administration > Certificate Attributes,** it is reflected in the enrolment page.
10. In the **Generic Fields** section enter the **Device Name** and the **Application IP Address**.
11. In the **Vendor-Specific Details** section, CA-specific details can be provided here (Template name for Microsoft CA). Some of the CAs will expect additional details other than CSR parameters for their operational purposes.
    - By default, the **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section).
    - The **Certificate ID** can be modified by the user.
    - If the user edits the **Certificate ID**, any change to the **Common Name** will not be reflected in the **Certificate ID**.
    - If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

12. 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.

13. 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.
14. Click **Approve**.



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

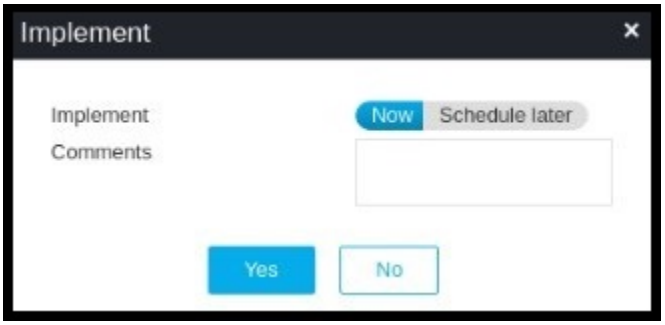


16. Enter the comments in the field.
17. Click **Yes**.

Once approved, you can see the Implement option in a holistic view.

18. Click **Implement.**

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



20. Enter the comments in the field.
21. Click **Yes**.

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.

Upload Key

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

1. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Select the type of certificate you want to upload key for from the **Certificate Inventory.**
4. 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.
5. Hover the mouse over icon on the server certificate and click **Upload Key.**

6. If the key you want to upload is password-protected, a popup screen appears asking you to enter the associated password.
7. Click **Submit.**
8. On the screen that pops up, navigate to the key you want to upload and click **Open.**

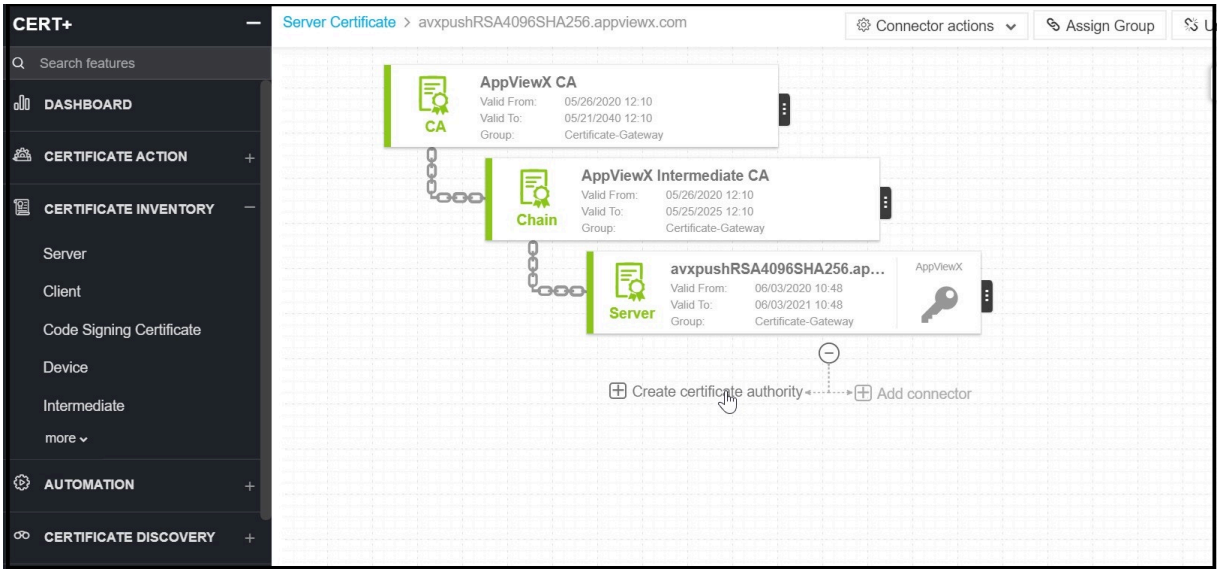
> **Note:** If the key you are trying to upload does not match the certificate, an error message that the *Certificate and key do not match* appears.

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

Add Certificate Authority Connector to Certificate

To add a Certificate Authority (CA) connector to the discovered or uploaded server or client certificate:

1. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Select the type of certificate you want from the **Certificate Inventory.**
4. Switch to the **List** toggle button on the top-right side of the page.
5. On the Certificates list view, click the **Common Name** of a certificate you want to add a certificate authority connector to.
6. On the Certificate topology page, click **Create certificate authority**.



7. On the details page, in the **Assign Group** field, select a group to assign the certificate.
8. In the **Certificate Authority** field, select a CA from the dropdown list. Other fields on the page change depending on the selected certificate authority. For each type of certificate authority, fields marked with a red asterisk (*) are mandatory.
9. Click **Add.**

Application Connector

An application connector is a software application running on a server. To add the application connector, the application should be managed under the AppViewX device inventory. All the supported devices in the AppViewX inventory can be provisioned with the certificate by adding the connector. The connector enables cloud-managed devices as it will provision certificates from on-premises infrastructure.

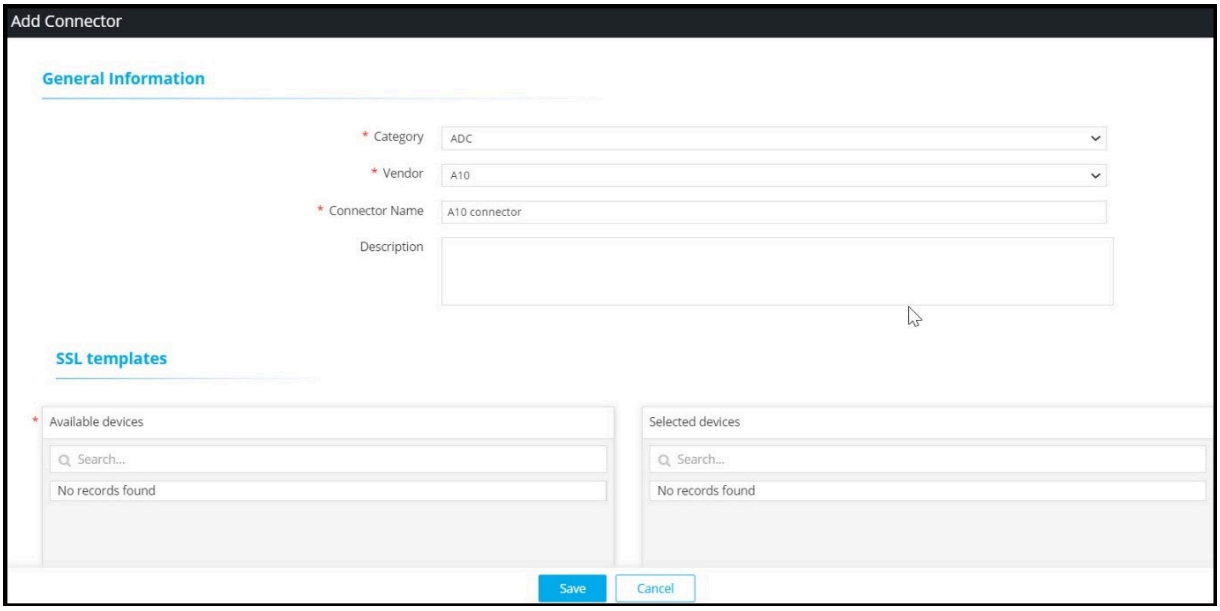
- Add Application Connector to Certificate

Add Application Connector to Certificate

To add an application connector to a certificate:

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

   The **Add Connector** is displayed.



6. 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.

7. From the list of available devices, click **Add to List** () button beside each device you want to select.
8. 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.
9. 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.

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

Push Certificate to Device

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

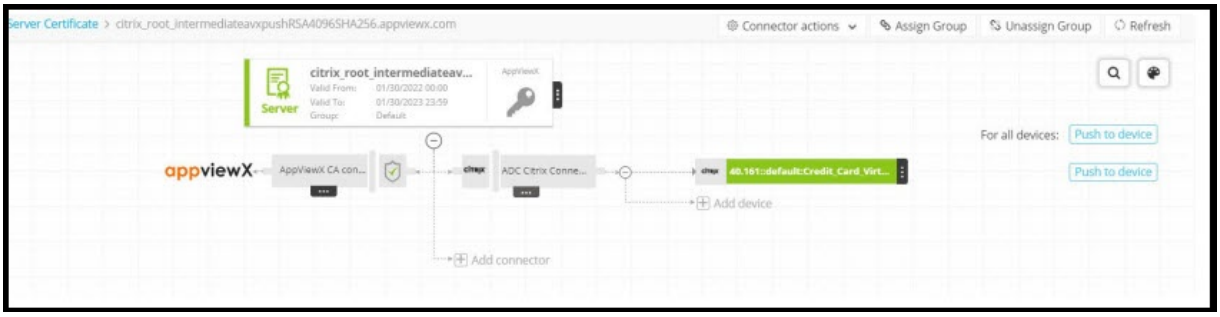
If the **Push automatically** field is selected while adding application connectors to a new certificate, then the certificate is automatically pushed to the device when it is retrieved. In such case, you need not complete the process manually.

Prerequisites

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

To push a certificate to a device:

1. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Select **Push to Device** from **Certificate Action.**
   The **Server Certificate** page appears.
4. Search for the certificate in the inventory and click the **Common Name** of the certificate to view the holistic view.



5. Click **Push to device.**
6. 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.
7. 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**.
8. Click **Implement.**
9. 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**.

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

Chapter 6: Certificate Discovery

Certificate Discovery

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

Certificate Authority Scan

AppViewX can communicate with CA and scan certificates.

Prerequisite

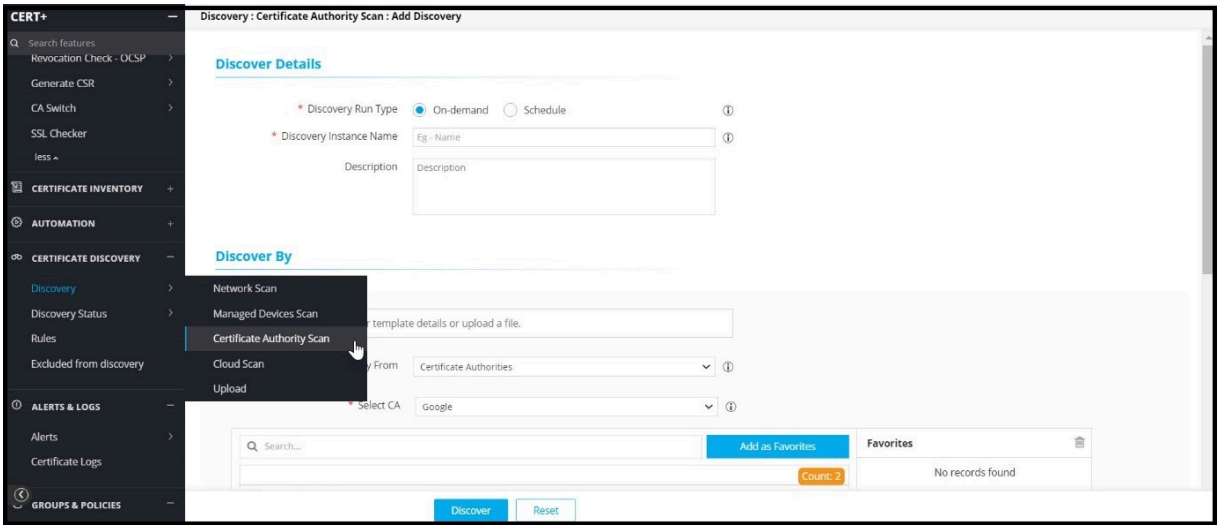
To discover certificates from a CA, the CA account must be determined under the AppViewX Inventory settings.

To discover a certificate from CA:

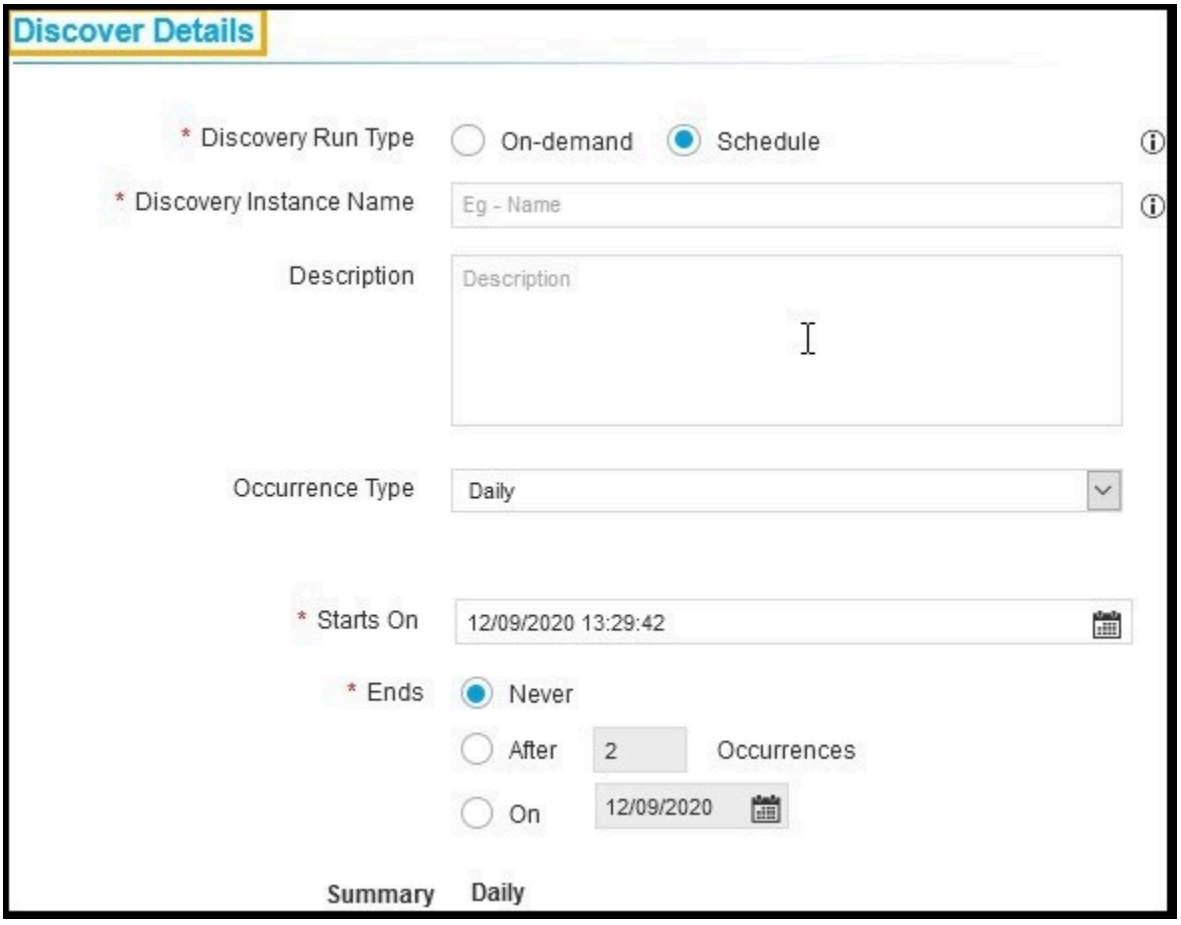
1. Click the **Menu** () icon.
2. Click **CERT+**.

   The **CERT+** left navigation pane appears.
3. Click **Discovery** from **Certificate Discovery** on the LHS pane.
4. Click **Certificate Authority Scan.**

   The **Add Discovery** page appears.



5. In the **Discover Details** section, enter the details as follows.



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

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. Options are: • **On-demand:** You can trigger a discovery manually whenever you want. • **Schedule:** By scheduling the discovery, you can automate the process for a defined time/ frequency. If you select **Scheduled** discovery, fill out the following details. • **Occurrence Type:** Select the type of occurrence from the dropdown list. Options are: • Daily • Weekly • Monthly • Yearly • **Repeat On:** Select day in the week to schedule the weekly discovery. • **Starts On:** Select the date to start the scheduled discovery. • **Ends:** Select the desired last discovery: • **Never:** Continues to discover the certificate. • **After:** Stops the discovery process after number of occurrence entered in the field. • **On:** Stops the discovery process for the selected period from calendar. • **Note:** AppViewX will trigger the discovery certificate process for that instance.
***Discovery Instance Name**	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** You can enter maximum of 2000 words in the field.

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

6. In the **Discover By** section, enter the following details:

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

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

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

8. In the **After Discover** section, enter the details as follows.

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

Field	Description
	Note: If this check box is enabled, the certificate group will be associated automatically with rules of access control.
***Certificate Group**	Select the certificate group from the dropdown list. Discovered certificates will be associated with this provided group.

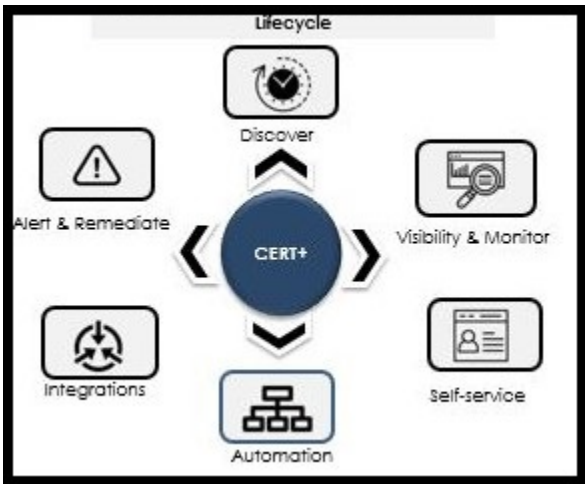
9. Click **Discover** to perform an on-demand discovery or click **Schedule** to perform a scheduled certificate discovery.

Chapter 7: Certificate Lifecycle Management

- What is Certificate Lifecycle Management (CLM)?

What is Certificate Lifecycle Management (CLM)?

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



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

- **Certificate Revocation**: Allows users to revoke a certificate in the event of certificate loss, compromise, or any other reason when the certificate is no more necessary for business.
- **Certificate Audit**: Track and audit the usage, creation, expiration, and revocation of certificates. Track user interaction with the platform.

What is Certificate Lifecycle Management (CLM)?

There is a growing need for organizations to allow and control only specific individuals, devices, machines to gain access to the network. The need for digital certificates to authenticate, identify and control who can access and operate on an organization's network. Managing digital certificates across complex networks to ensure protection and prevent failures is a must for all businesses. CLM ensures continuous monitoring of digital certificates, with the ability to audit and keep track of expirations and renewals to avoid any service disruption. The digital certificate is a mechanism by which machines and individuals are identified and authenticated.

Inventoried Certificate Actions

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

The following actions can be performed on certificates:

- Download Certificate
- Upload Certificate
- Export Certificate
- Renew Certificate
- Regenerate Certificate
- Revoke Certificate
- Generate CSR for Certificate
- Submit CSR to Certificate Authority
- Download CSR
- Suspend Certificate

Download 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.

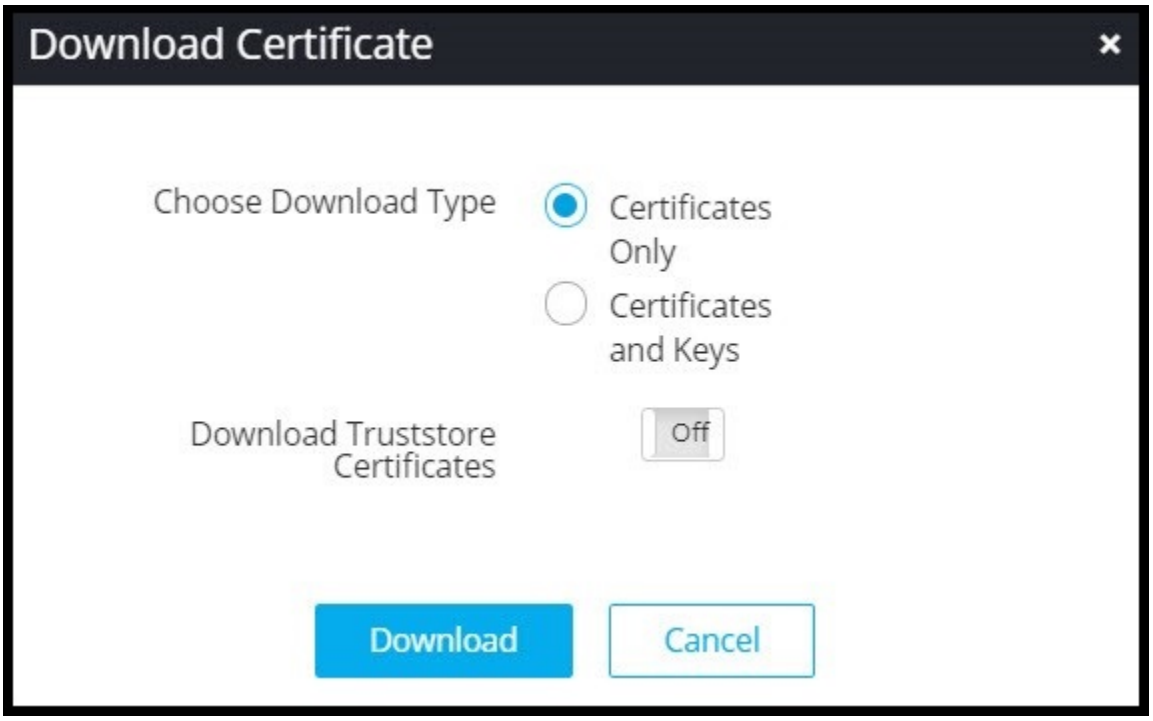
Download from Certificate Inventory

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. Click the **Menu** (☰) icon.
2. Click **CERT+**. The **CERT+** left navigation pane appears.
3. Click **Download** from the **Certificate Inventory** after selecting the type of certificate you want to download.
4. Switch to the **List** toggle button on the top right corner of the certificate page.
5. 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*.

6. Click **Actions,** and select **Download Certificates.**



7. In the **Download Certificate** popup window, select **Certificates Only.**
8. 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.

9. Click **Download.**
10. To view details of the certificate, unzip the file, and open the security certificate file. Click **Details.**

Download from the Certificate Topology

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

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

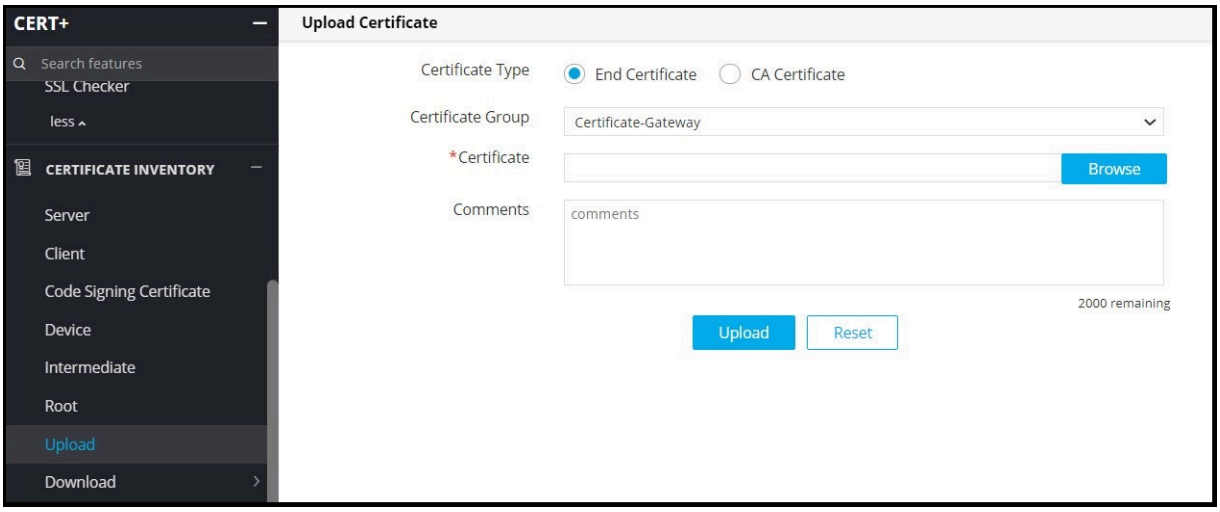
7. In the **Download certificate** pop-up window, select the file format.
   - For PEM and DER certificate types, you can enable/disable the **Download Trust Store Certificates** option along with the end certificates.
   - For PEM and DER certificate types, you can enable/disable the **Download Trust Store Certificates** option along with the end certificates.
8. Click **Yes.**

Upload Certificate

To upload a certificate:

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

   The **Upload Certificate** screen is displayed.



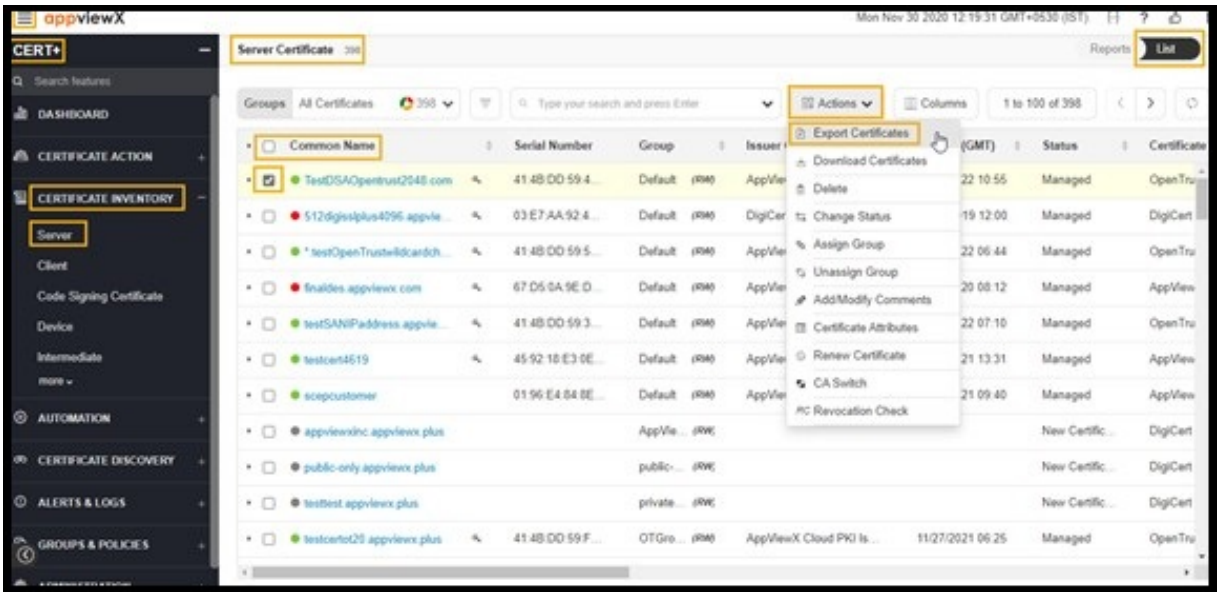
4. Select the **Certificate Group** into which the uploaded file must be mapped in CLM.
5. Choose the certificate file and click **Open.**
6. Click **Upload.**
   Once uploaded, go to the selected certificate group in inventory to see the uploaded certificate-keys.

Export 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 of this action can be selected in <.xls> or <.csv> format. This can be used for reporting or making another inventory.

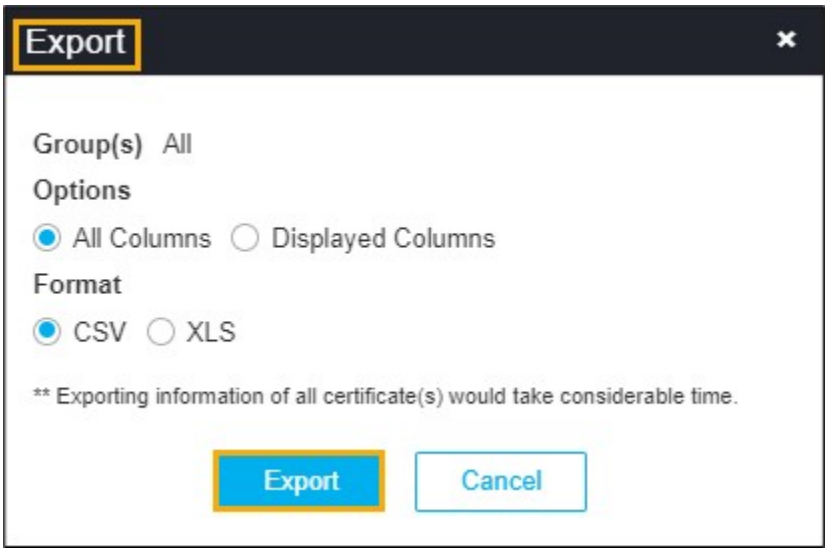
To export the server certificate:

1. Click the **Menu** (☰) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Click the **Certificate Inventory** and select the type of certificate you want to export.
   The **Certificate** screen is displayed.
4. Switch to the **List** toggle button on the top right corner of the certificate page.



5. In the **Common Name** column certificate list, select the check box against the certificate that you want to export certificate to.
6. Click **Actions**, and then select **Export Certificates** from the list.

   The **Export** popup window appears:



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

Renew 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. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Click **Renew Certificate** from **Certificate Action.**
4. Click **Server, Client,** or **Process Explorer** depending on the type of certificate you want to renew.
5. Switch to the **List** toggle button on the top right corner of the page.
6. In the **Common Name** column certificate list, select the certificate that you want to renew.

7. Hover the mouse over icon and click **Renew.**
   You are redirected to the **Certificate** page.

8. 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.*
9. Click **Approve.**
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.

Regenerate Certificate

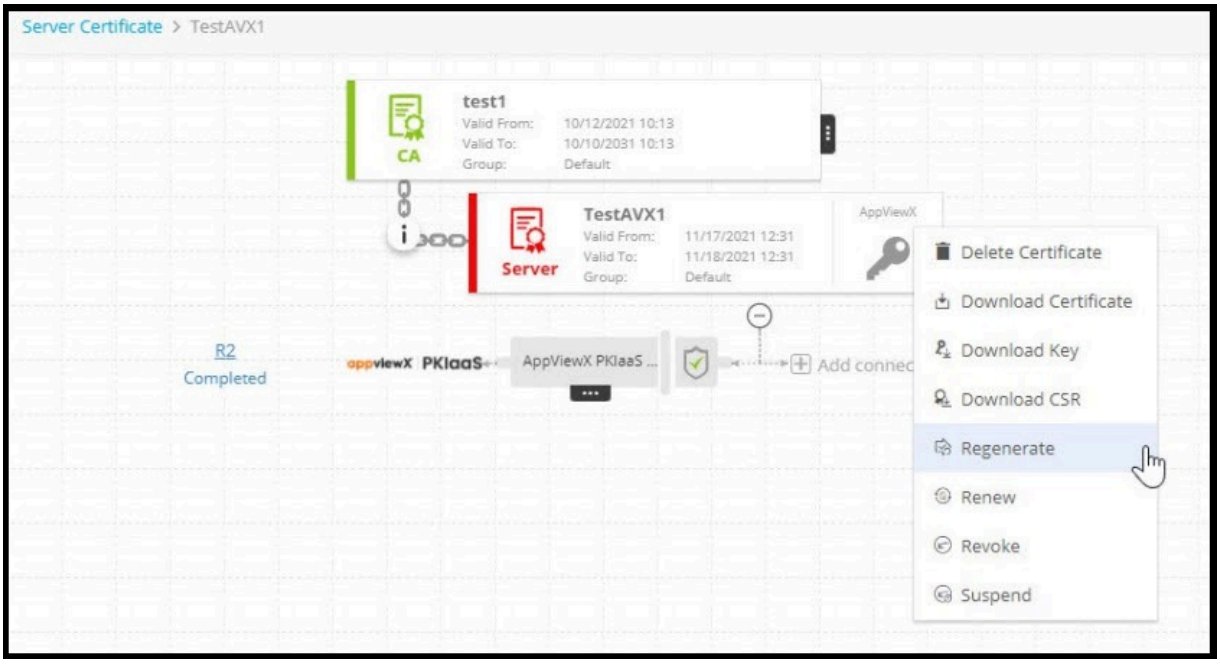
> **Note:** The regenerate option allows you to create a new certificate with a new key and with similar parameters to an existing certificate so that you can host it on a different type of web or application.

To regenerate a certificate:

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

   The **CERT+** left navigation pane appears.
3. Switch to the **List** toggle button on the top right corner of the page.
4. In the **Common Name** column certificate list, select the certificate that you want to regenerate.

   The Certificate page is displayed.
5. Hover the mouse over **More** ( ) icon on the certificate, and click **Regenerate.**



   You are redirected to the **Server Certificate** page.
6. In the **Vendor Specific Details** section, enter a new **Certificate ID** and click **Regenerate.**
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 **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 and the work order status is displayed beside the certificate on the topological view.

11. Click **Refresh** ( ). The work order status is displayed beside the certificate.
    After the regenerating action is completed, the status is updated to *Completed.*

Revoke 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. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Switch to the **List** toggle button on the top right corner of the page.
4. In the **Common Name** column certificate list, select the certificate that you want to revoke.
5. Hover the mouse over **More** ( ) icon on the certificate, and click the **Revoke** option.

6. Select a reason for revoking the certificate.
7. 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.
8. Click **Approve**.
9. On the **Approve** screen that pops up:
   - Click **Now** or **Schedule Later** button in the **Implement** field.
   - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
   - Enter comments and click **OK**.
10. Click **Implement.**
11. On the **Implement** screen that pops up:
    - Click **Now** or **Schedule Later** button in the **Implement** field.
    - If you select **Schedule Later**, set the date and time that you want the certificate push to occur.
    - Enter comments and click **OK**.
12. Click **Refresh** ( ). 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.*

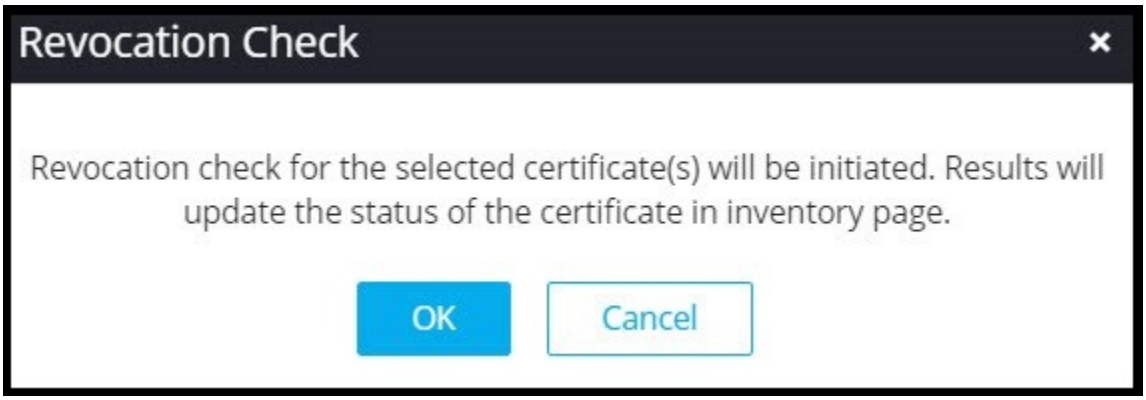
Perform Revocation Check

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

   The **Revocation Check** dialog box appears.



6. Click **OK.**
   Once validated, the status certificate is updated in the color code of the **Common Name** column.

Generate CSR for Certificate

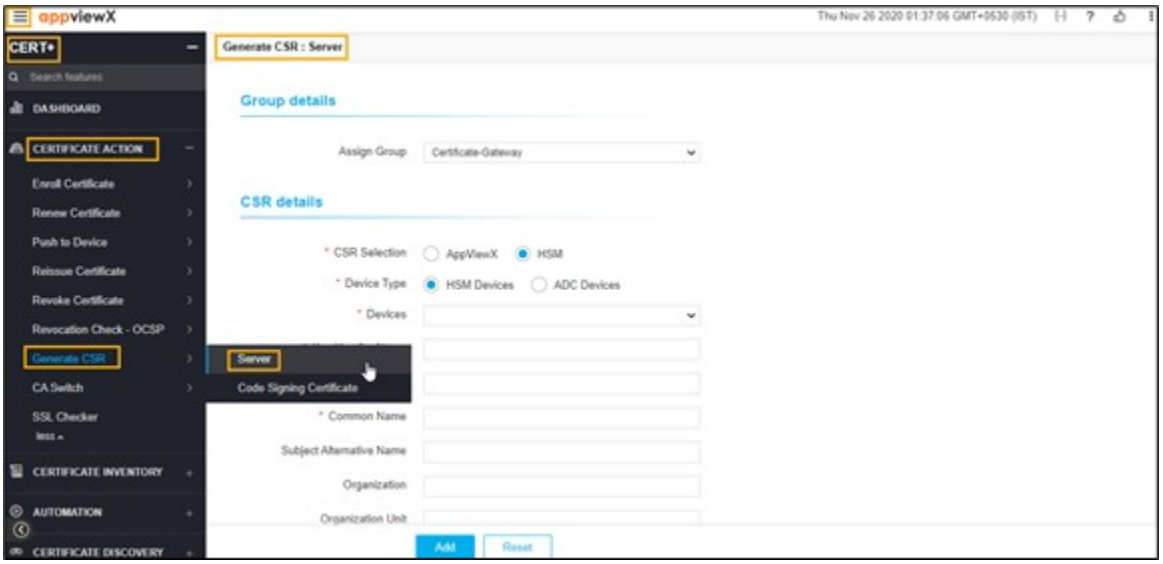
To generate a manual CSR for the certificate:

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

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

3. Click **Generate CSR** from **Certificate Action.**
4. Click **Server** or **Code Signing Certificate.**

   The **Generate CSR** page appears.



5. 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
***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 allowed except period (.), hyphen (-), and underscore (_).
Subject Alternative Name	Select the alternative subject name from the dropdown list. You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. **Note:** Multiple values must be separated by a comma.

Field	Description
	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.
Validity	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown lists.
***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.

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

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.

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

Submit CSR to Certificate Authority

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

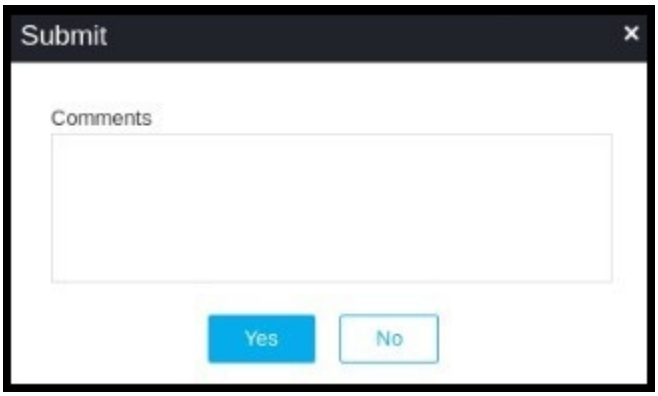
To submit CSR to CA:

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

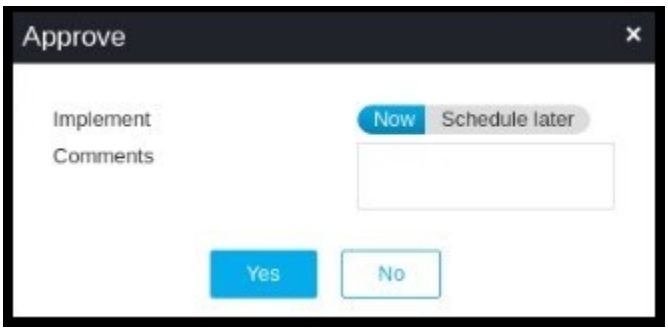
   The certificate topology screen opens.

4. Add a CA connector to the certificate topology as explained in the Section, Add Certificate Authority Connector to Certificate.
5. 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.



6. Click **Approve**.
7. Click the **Schedule later** button if the workflow request has to be approved automatically in the future.

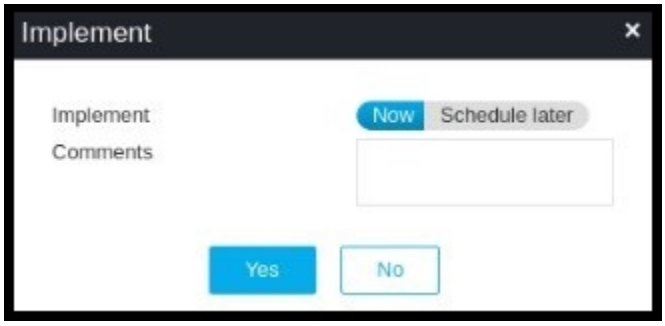


8. Enter the comments in the field.

9. Click **Yes**.
   Once approved, you can see the Implement option in the holistic view.
10. 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.



11. Enter the comments in the field.
12. Click **Yes**.
    CSR Submission to CA is in progress.
13. 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.

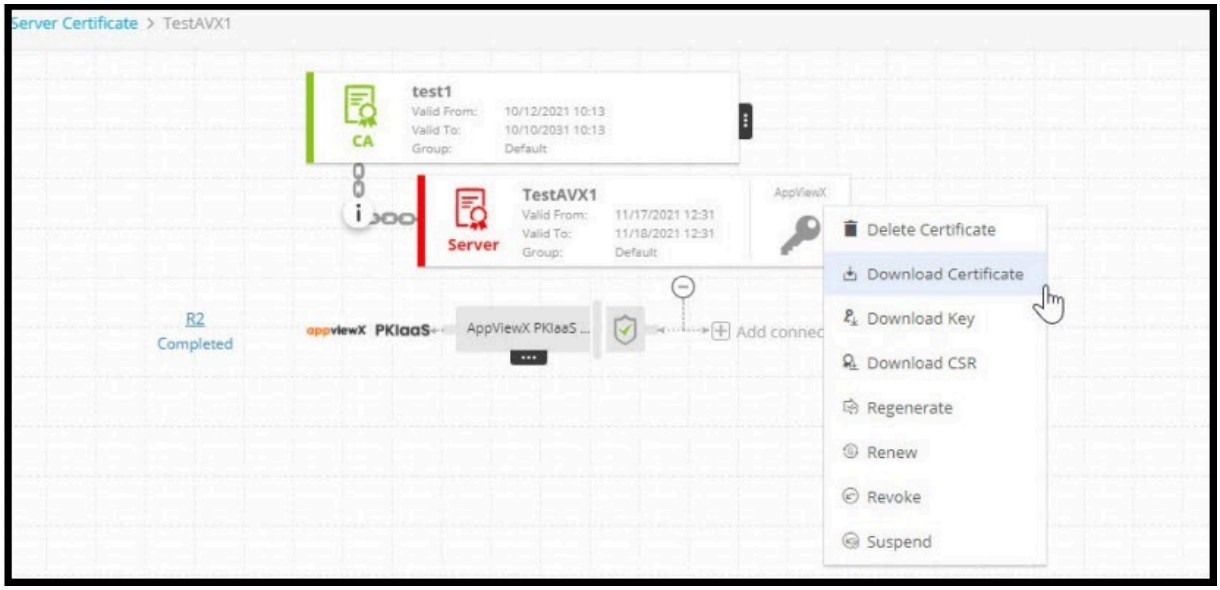
Download CSR

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

From holistic view:

1. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. From **Certificate Inventory,** click **Server** or **Code Signing Certificate.**

4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over  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.

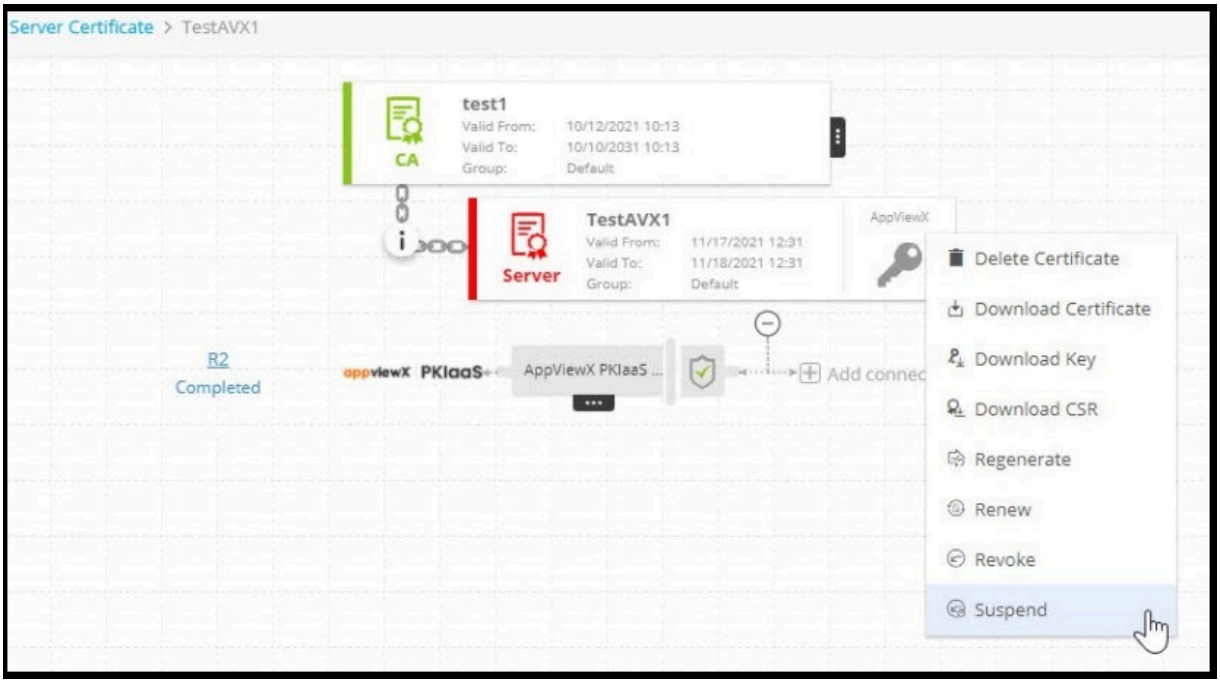
Suspend Certificate

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

6. Hover the mouse over **More** ( ) icon on the certificate, and click the **Suspend** option.



7. In the **Comments** field, enter the reason for suspending the certificate.
8. Click **Yes.**

Change 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:

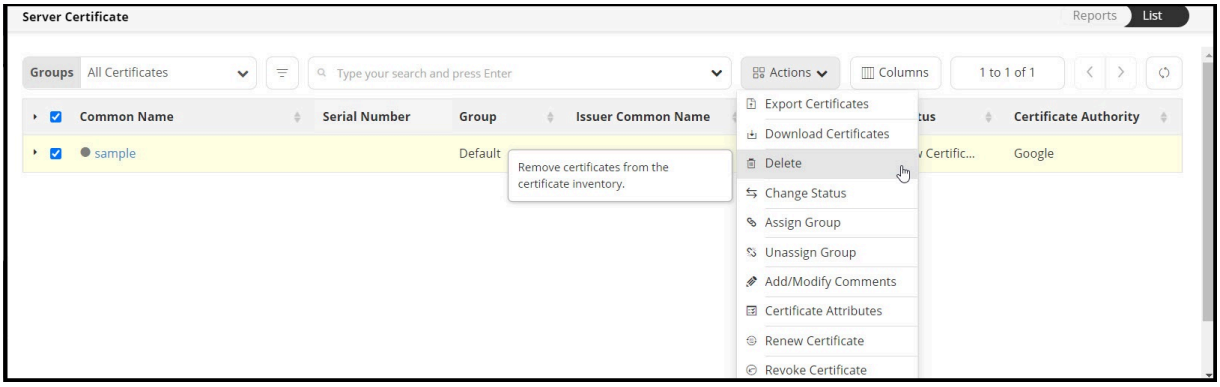
1. Click the **Menu** ( ) icon.
2. Click **CERT+**.
   The **CERT+** left navigation pane appears.
3. Click **CA Switch** from **Certificate Action** and select the type of certificate for which you want to change status.
4. On the Change status pop-up screen that appears, select **Managed** (to create,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

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.

Delete Certificate

To delete a certificate or policy:

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



5. Click **Actions,** and select **Delete** from the dropdown list.

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

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

Chapter 8: Reporting and Monitoring

Overview

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

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

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

Dashboard Actions

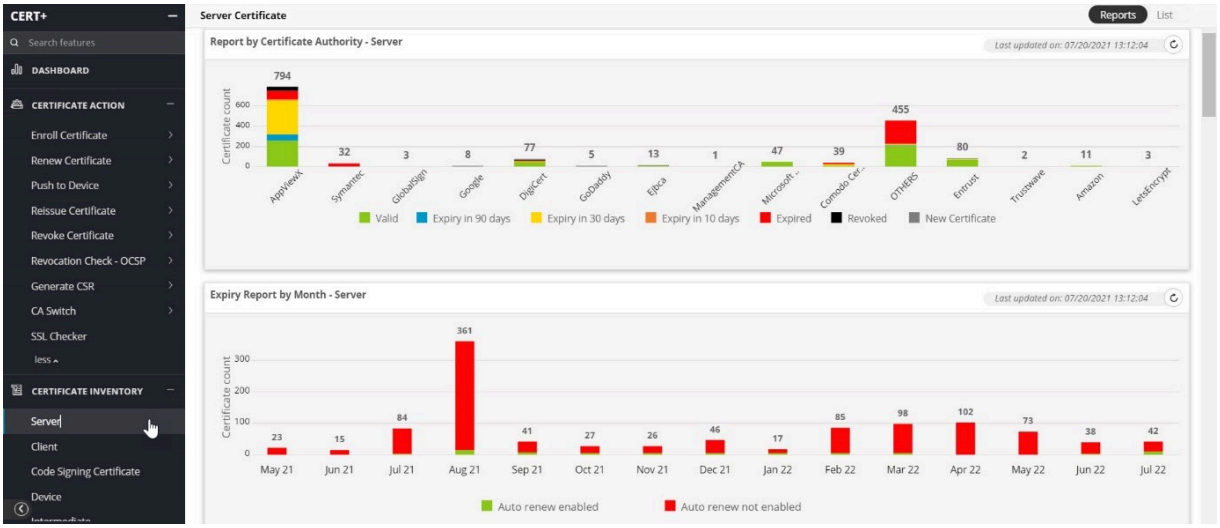
This section explains how to create, export, import, and delete dashboards.

View Certificate Reports

To view certificate reports:

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

   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.

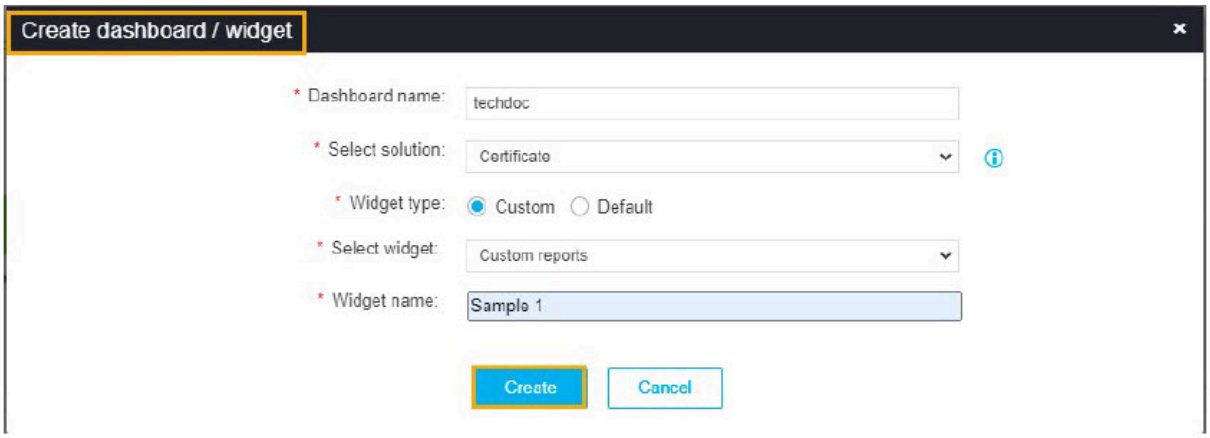
Create Dashboard

To create a dashboard:

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

   The **CERT+** left navigation pane appears.
3. Click **Dashboard** in the left navigation pane.
4. Click the **Create (+)** icon in the command bar.

   The **Create dashboard/widget** window appears.
5. Enter the field information in the **Create dashboard/widget** window.



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

Field	Description
***Dashboard name**	Name of the dashboard.

Field	Description
***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.

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

Export Dashboard

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

Import Dashboard

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

Delete Dashboard

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

Certificate Reporting

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

Chapter 9: Alerts and Logs

Alerts and Logs

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: PKI Standard Practices

PKI Standard Practices

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

- Ensured to be prepared to respond in a timely manner in case of a CA or end-entity certificate compromise and have a plan or workflow to replace all affected certificates or the trust chain.
- In the event of a key or certificate compromise, a fresh key pair should be generated on a secured system. The compromised item should be revoked and taken out of the service as soon as the systems are secured.
- If you are not sure of your private key possession, report it to your CA and suspend the key immediately. Once you find the key is secure, reinstate the certificate.

CA Compromise and Remediation Matrix

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