**AppViewX - Google CA Solution Guide**

**Google CA Solution Guide**

(Document Revision 1.0)

**Copyright © 2020 AppViewX, Inc. All Rights Reserved.**

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

**Trademarks**

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

This product includes software developed by the CentOS Project ([www.centos.org](https://www.centos.org/)).

This product includes software developed by Red Hat, Inc. ([www.redhat.com](https://www.redhat.com/en)).

This product includes software developed by VMware, Inc. ([www.vmware.com](https://www.vmware.com/in.html)).

All other trademarks mentioned in this document are the property of their respective owners.

**Contact Information**

AppViewX, Inc.

500 Yale Avenue North, Suite 100

Seattle, WA 98109

Tel: +1 (206) 207 7541

Email: info@appviewx.com

Web: [www.appviewx.com](http://www.appviewx.com/)

**Table of Contents**

Contents

[Document History 635](#_Toc56110256)

[Purpose 636](#_Toc56110257)

[Overview 636](#_Toc56110258)

[Pre-requisites 636](#_Toc56110259)

[Infra Requirements 636](#_Toc56110260)

[Launching AppViewX 637](#_Toc56110261)

[Configure Google CA 637](#_Toc56110262)

[Create a Certificate Group 640](#_Toc56110263)

[Create a Certificate Policy 643](#_Toc56110264)

[Configure Single Sign-on 645](#_Toc56110265)

[Enable Auto Enrollment – SCEP 647](#_Toc56110266)

[Certificate and Role Synchronization 650](#_Toc56110267)

[Certificate Action 651](#_Toc56110268)

[Enroll 651](#_Toc56110269)

[Regenerate 651](#_Toc56110270)

[Revoke 651](#_Toc56110271)

[Renew 652](#_Toc56110272)

[Reissue 652](#_Toc56110273)

[Enroll (or) Create a Certificate 652](#_Toc56110274)

[Regenerate a Certificate 658](#_Toc56110275)

[Revoke a Certificate 664](#_Toc56110276)

[Push to Device 667](#_Toc56110277)

[Add an Application Connector to the Certificate Topology 667](#_Toc56110278)

[Push a certificate to a device 668](#_Toc56110279)

[Roll Back a Certificate from a Device 670](#_Toc56110280)

[Prerequisites 670](#_Toc56110281)

[Roll back a certificate from a device 670](#_Toc56110282)

[Finding More Information 671](#_Toc56110283)

[Documentation Feedback 671](#_Toc56110284)

[Requesting Technical Support 672](#_Toc56110285)

[Self-Help Online Tools and Resources 672](#_Toc56110286)

# Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Product** | **Version** | **Date** | **Comments** | **Final Approval?** |
| AppViewX – Google CA | v2020.3.0 | Nov 12, 2020 | Features of Google CA in AppViewX | Yes |

# Purpose

This guide describes AppViewX's Certificate lifecycle platform and provides a step by step configuration of Google CA in AppViewX to perform certificate lifecycle management. The document covers the Google CA account configuration, creating certificate groups, and certificate policies to enable the automation of certificate lifecycle management. The certificate lifecycle involves enrollment, renewal, revocation, and regeneration.

# Overview

AppViewX CERT+ Certificate Lifecycle Management platform can discover, manage and automate the lifecycle of digital certificates.

It helps you to replace your manual certificate management processes. It also introduces management features like monitoring certificate expiry, usage, and notifying administrators about any events. This platform provides the capability to discover existing certificates and push certificates to endpoints. It also acts as a repository for all certificates-related information such as endpoint information, validity, status, the chain of trust, and so on.

Users can manage and automate the certificate lifecycle that can be broken into the below-listed stages.

* Create new certificates
* Regenerate Certificate
* Renew Certificate
* Reissue Certificate
* Revoke Certificate

Note: The document explains only the actions which are currently supported by Google CA,

* Create new certificates
* Regenerate Certificate
* Revoke Certificate

# Pre-requisites

The product comes with a user account who has super users permission, and all the ACF permissions.

# Infra Requirements

Users must have the below configurations available

1. Valid Google Cloud account configured with Organization, Project and CA configured
2. AppViewX must be Installed from Google Marketplace into Customer’s Google Cloud platform
3. Installed AppViewX must be up and running in the Google Cloud

# Launching AppViewX

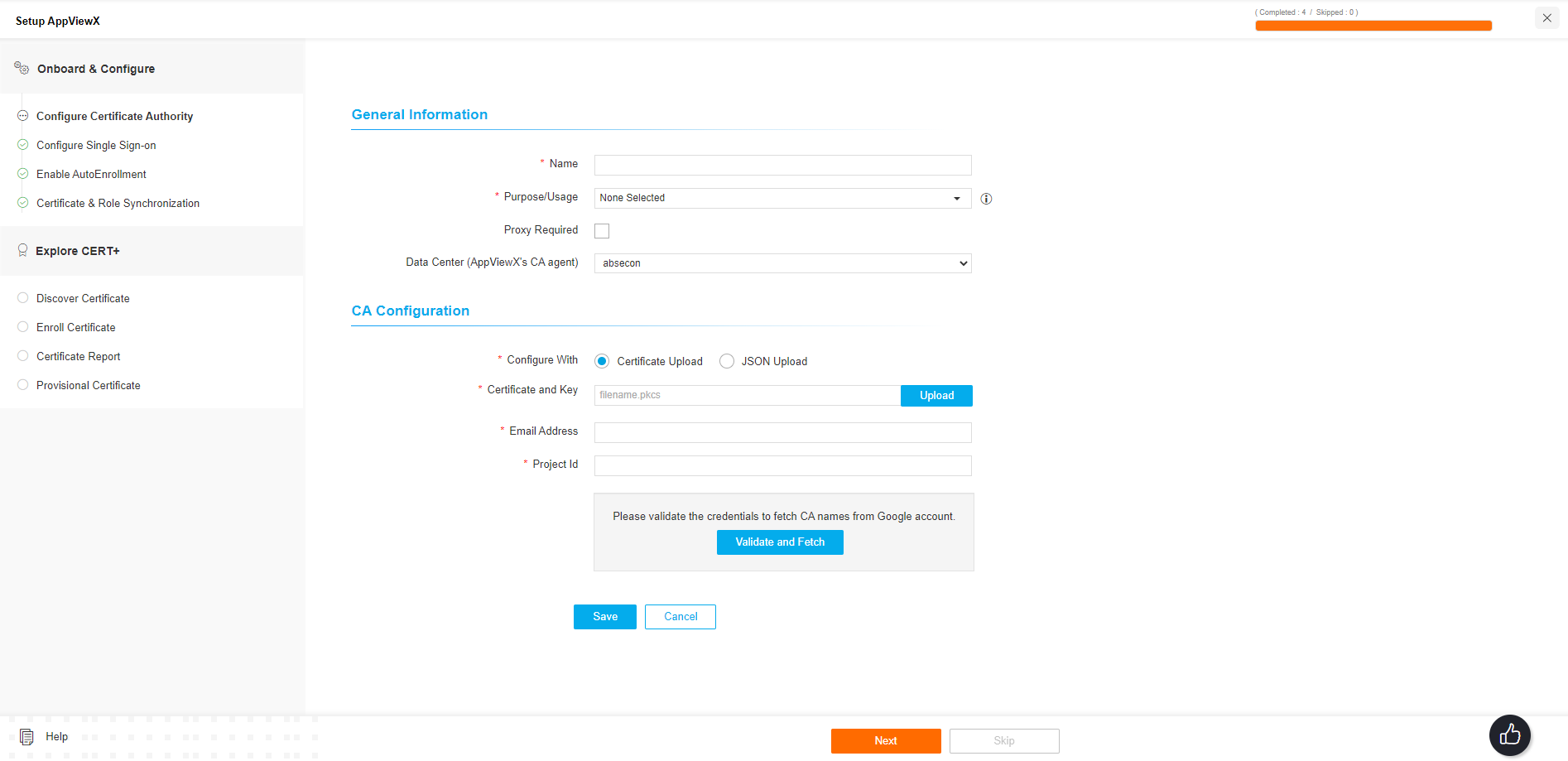
User will be landed in to Get started page, followed by the onboarding steps to collect the basic details which are required to operate AppViewX seamlessly.



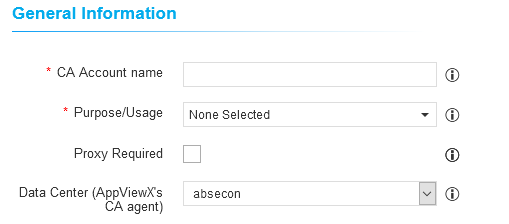
# Configure Google CA

**Onboarding Step 1:**

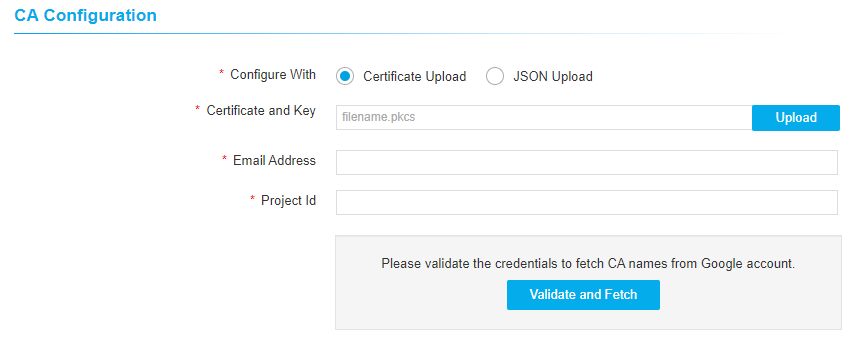
Before an administrator or user can enroll a certificate through CERT+, the system needs to be able to communicate with the Certificate Authority signing the certificate. AppViewX would need to be able to Establish network connectivity with the CA, Authenticate itself with the CA for requesting CSR signing on behalf of the administrator or user. This can be achieved by configuring the CA settings on AppViewX by providing the information specific to each Certificate Authority.

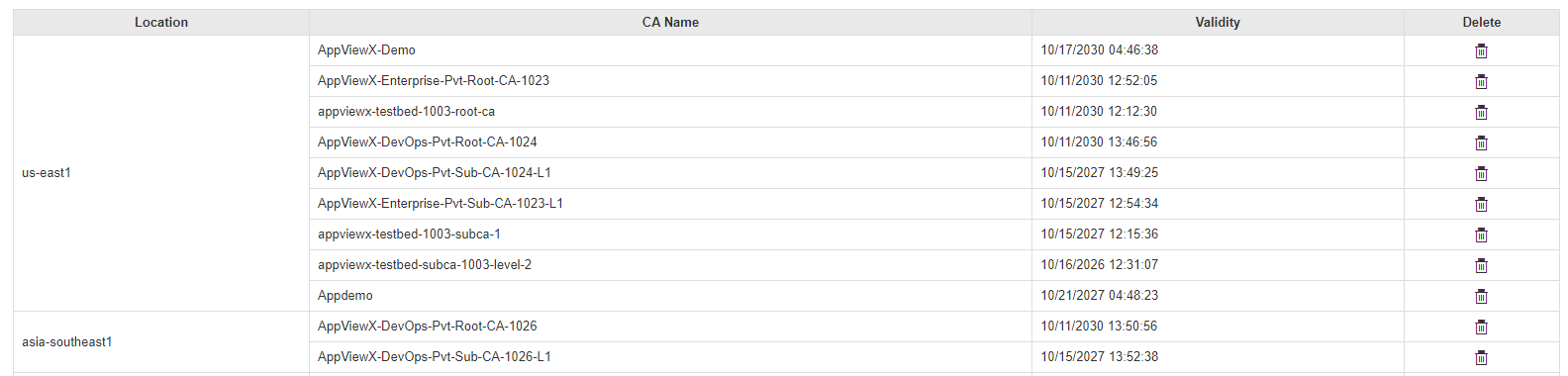


1. On the **Google CA configuration** page, enter the details in the **General information** and **CA Configuration** sections.
2. Under the **General Information** section, enter the required details in the respective fields:

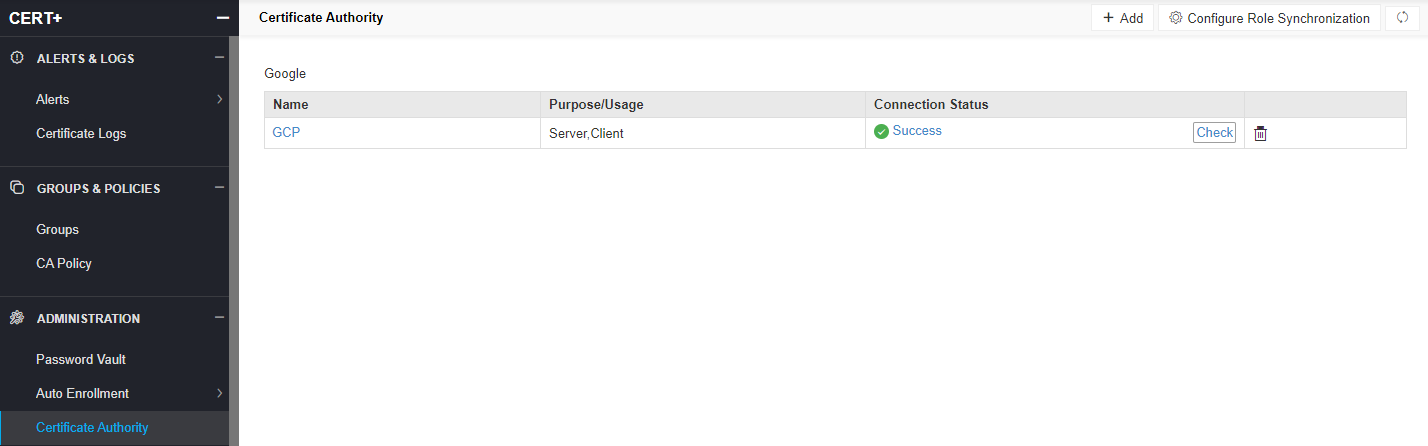


* The CA Account name is a unique name for the Certificate Authority (CA) account represented during certificate enrollment and policy creation.
* To enroll for a server certificate, choose Server from the Purpose drop down. To enroll for a client certificate, choose Client from the Purpose drop down.
* Select the Data center from which communication should establish to Certificate Authority

1. Under the **CA Configuration** section, enter the required details in the respective fields: 

* Select the Type of configuration – Certificate Upload or JSON upload which has the details of project and access credentials to configure the Google CA.
* Upload .pkcs file in the Cetificate and Key field if the configuration method is certificate upload.
* Click on Validate and Fetch to validate the uploaded Certificate/JSON to get the Email addresses, Project ID, Issuing location, Issuing CA associated with the uploaded project configuration.
* 
* Save the details as a CA settings and repeat the same steps to add more CA settings

To configure Google CA in the product, do the steps as follow:

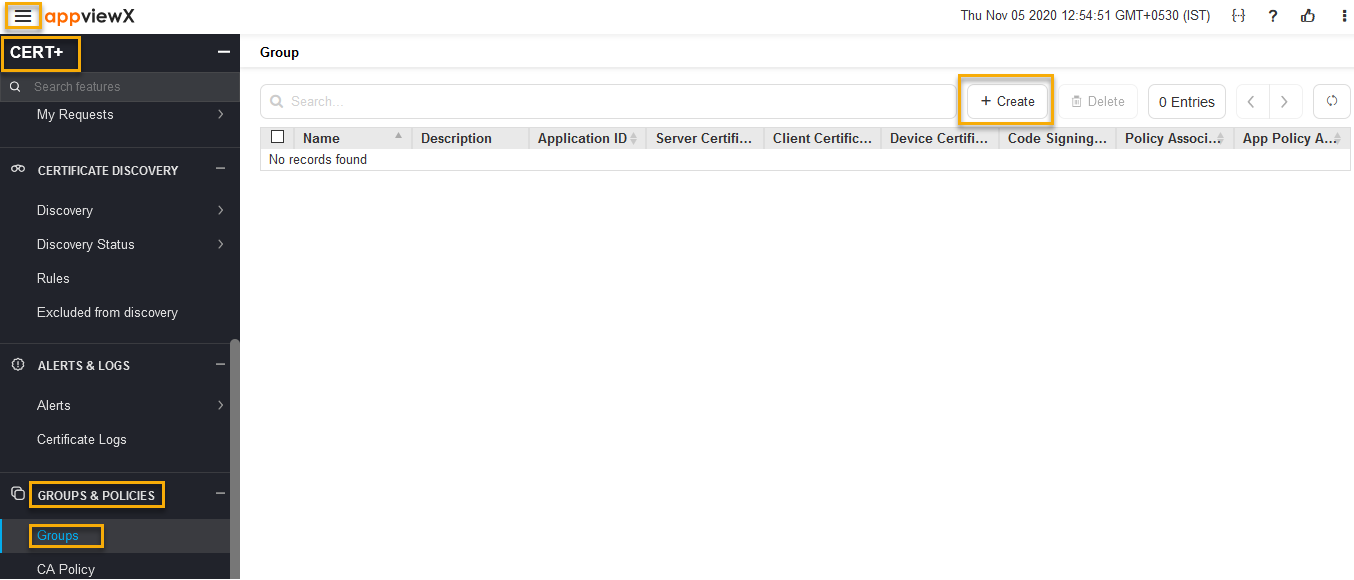
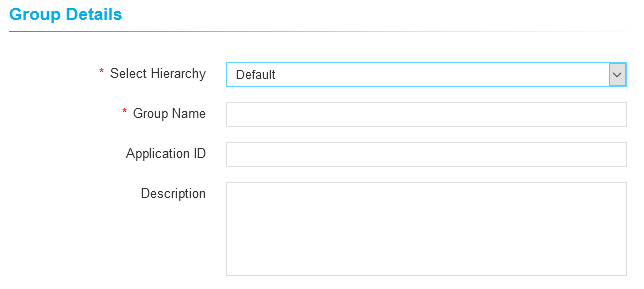
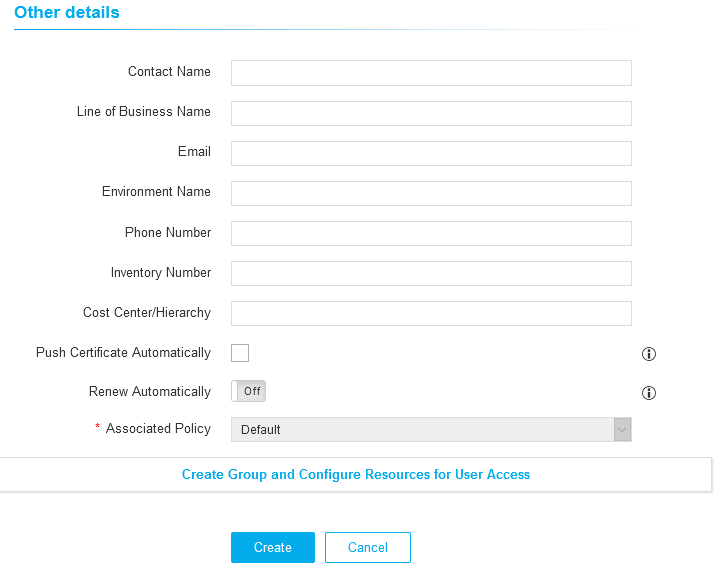
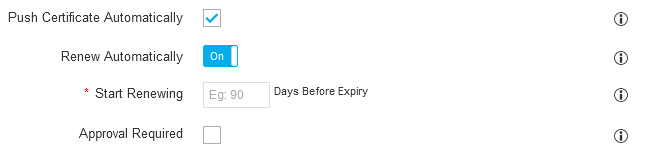
1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Navigate to **CERT+** > **Administration** > **Certificate Authority** 
4. Click **+Add** icon on the top right of the page.
5. Complete the form with mandatory details and save the settings.

# Create a Certificate Group

The certificates generated/discovered in the AppViewX can be logically grouped together for ease of management. All the certificate actions on a specific group can be restricted via RBAC. By default, all the certificates will be added under the “Default” group.

As and when the Certificate Authority in Configured in the step 1 of onboarding, AppViewX automatically creates a Certificate group as CA\_Account\_Name\_ProjectID. This group is used to organize the certificates which are being discovered from the respective Projects.

To create new groups for better organization of Certificates, follow the below steps,

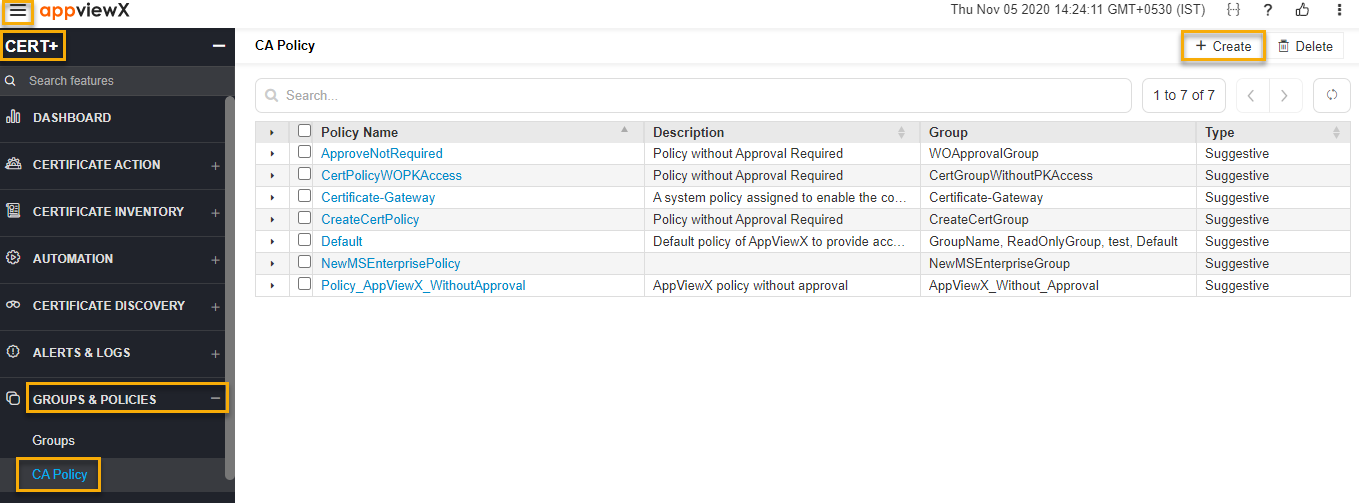
1. Click the menu button.
2. Navigate to **CERT+** > **Administration** > **Groups & Policies** > **Groups**.
3. On the **Groups** inventory page, click **+ Create** to configure certificate groups
4. On the **Certificate Group creation** page, enter the details in the **Group Details** and **Other Details** sections.
5. Under the **Group Details** section**,** enter the required details in the respective fields:
   1. Select **Hierarchy** as **Default.**
   2. Enter the **Group Name** for the new group
   3. **Application ID:** This is an optional field. Enter Application IDthat is associated with the business units.
6. **Description:** This is an optional field, Enter a descriptionof the certificate group. Any fields in the **Other details** section can be used to save information required for the business unit.
7. Certificate(s) associated to this group can be pushed automatically to the end machines only when the **Push Certificate Automatically** option is enabled.
8. Certificate(s) associated to this group can be renewed automatically to the end machines only when the **Renew Automatically** optionis enabled.
9. When the **Renew Automatically** optionis enabled, AppviewX can auto-renew the certificate based on the specified days before expiry.
10. 
11. Disable **Approval Required,** to proceed auto-renewal without approvals or enable **Approval Required,** if approval required for auto-renewal as well.
12. Click **Create** to add the certificate group to the system.

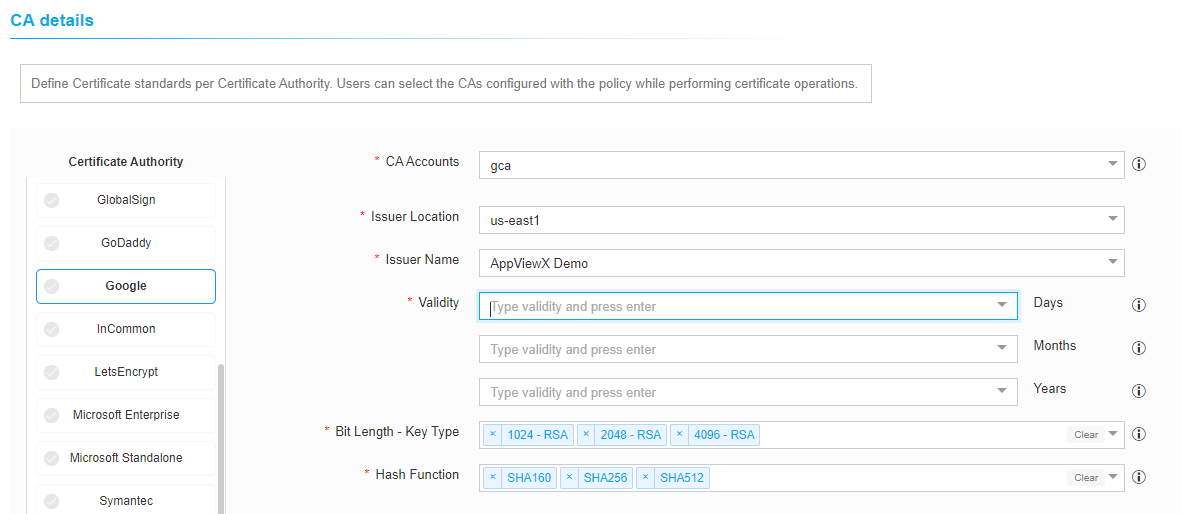
# Create a Certificate Policy

Defined set of certificate parameters can be created as policies. This helps in enforcing the security compliance over certificate creation across the organization. Also these policies will be used to generate compliance reports against existing certificates.

As and when the Certificate Authority in Configured in the step 1 of onboarding, AppViewX automatically creates a Certificate policy as CA\_Acc Name\_Project ID. This policy will be mapped to the Certificate group which is created to hold the certifricates from the respective project. Each CA settings with a project ID configured in the AppViewX will create a respective group and policy to it.

To create new policies for better organization of Certificates, follow the below steps,

1. Click the menu button.
2. Navigate to **CERT+** > **Administration** > **Groups & Policies** > **CA Policy**.
3. On the CA Policy inventory, click on **+** **Create** to configure certificate policy.
4. On the **policy creation** page, enter the details in the **Policy Details**, **CA Details,** and **Group Selection** sections.
5. Under the **Policy Details** section**,** enter the required details in the respective fields:
   1. Enter the **Policy Name**.
   2. In the **Description** field, enter the policy information.
   3. Choose the **Policy Type** as **Strict** or **Suggestive**:
      1. **Strict** - Enforce the standards defined in the policy where a user can not modify any parameters while certificate enrollment in AppviewX
      2. **Suggestive** - Suggests users with policy parameters. A user can modify suggested values if required while certificate enrollment in AppviewX
6. When Approval Required is enabled, it will enforce the peer approval process for any requests made for new/renew/regenerate/reissue or revocation of certificates. By default, Approval Required is disabled.
7. To export/ download the private key of a server certificate, enable Private Key Access in the policy page. By default, Private Key Access is disabled to secure private key export/download by the users.
8. When **Private Key Access** is enabled, it automatically enables **private key access for read-only user.**
9. Private Key of the certificate in read only group can be exported only when private key access for read-only user enabled. By default, both Private Key Access and private key access for read-only user are disabled.
10. By enabling Enable certificate push-bind access for read-only user option, users in the read only user group can perform certificate push, bind and rollback operations from the holistic view of the certificate associated with this policy. By default, Enable certificate push-bind access for read-only user is disabled.
11. Enable Include Root and Intermediate Certificates for Compliance Check to perform a compliance check. Enabling this option would validate if Issuer and Root of the certificate are also complaint to the standard defined in Policy
12. In the **CA Details** section, enter the required details in the respective fields:
    1. On the left pane, a window with a list of AppViewX supported Certificate Authorities are listed,
    2. Select the Google CA in the left pane.
    3. CA Accounts - Select the CA account name configured in the Certificate Authority page.
    4. Issuer Location – Selec the location to filter the Issuing CAs
    5. Issuer Name – Select the issuing CA from the list
    6. Validity – enter the validity in days/month/year
    7. Bit Length - Key Type - Select the certificate bit length and key type as per organization standards and policies.
    8. Hash Function - Select the certificate hash algorithm as per organization standards and policies. Recommending to use SHA256 and above.



**Certificate Parameters** section is optional. Certificate parameters filled in the policy page will automatically pre-populate in the certificate enrollment page.

* **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** - The country 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 address can be added.
* Click **Save CA Details** to save the added information before group selection.
* Under the **Group Selection** section, select the group(s) that you want to enforce this policy (or) create a new group to which the policy should be associated.

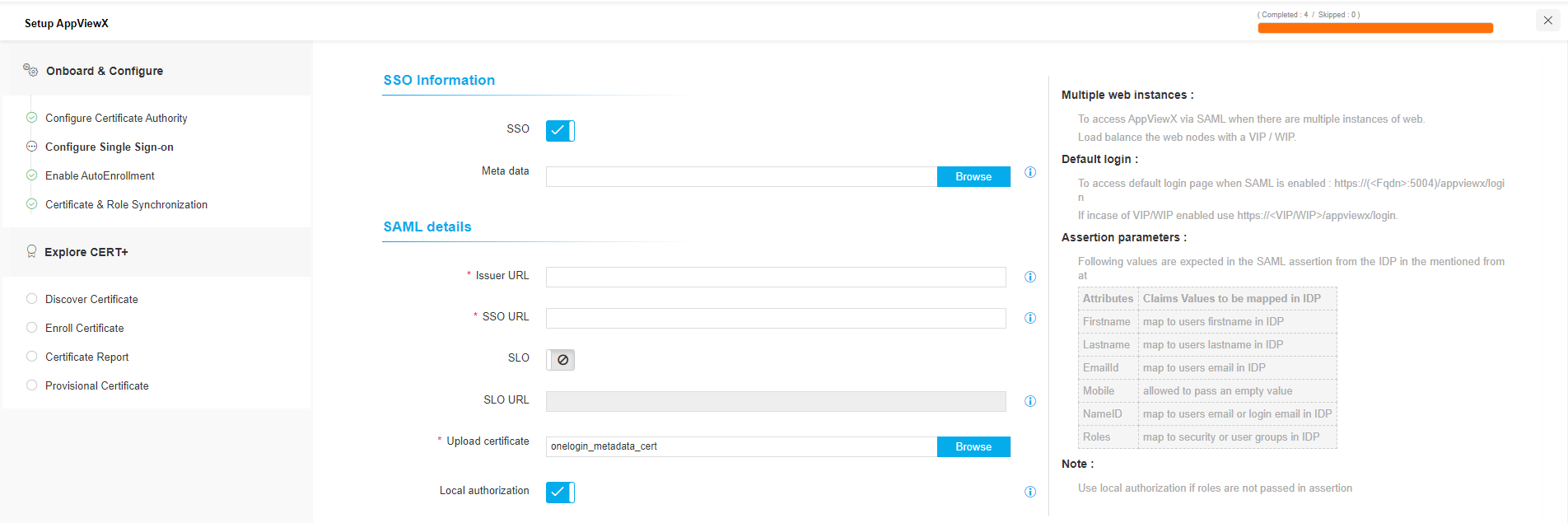
1. Under the Compliance Check section, you can enable the Perform Compliance Check, to trigger compliance check for the certificates in the inventory against the policy details.
2. Click the **Create Policy** button.

# Configure Single Sign-on

**Onboarding Step 2:**

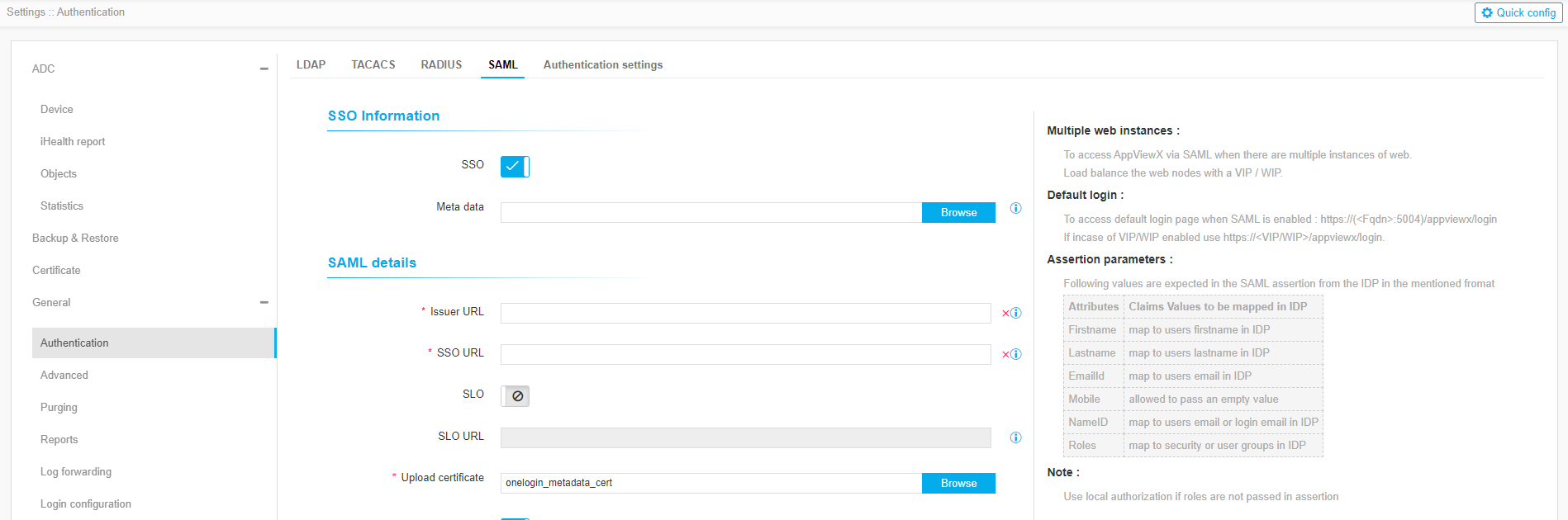
Configure external authentication or single-sign-on for users to log in to AppViewX

1. Click Disabled icon to enable the Single Sign-on (SSO).
2. (Optional) Click Browse to locate and select the metadata file containing the SSO
3. configuration.
4. In the Issuer URL field, enter the entity ID of your Identity Provider (IdP).
5. In the SSO URL field, enter the protected endpoint provided by your IdP, to which, AppViewX
6. sends the authentication request.
7. (Optional) Click the (Disabled) button to enable the Single Logout (SLO).
8. In the SLO URL field, enter your IdP protocol endpoint.
9. Click Browse to locate and select the required certificate.
10. Click Save.
11. Click Copy (in the Entity ID, Service URL, and SLO URL fields) and paste it in the respective field to configure the AppViewX details in your IdP server.



To Configure the Security Assertion Markup Language (SAML) server for authentication in the product, follow the below steps

1. The AppViewX system allows you to add more than one Security Assertion Markup Language (SAML) server for authentication.
2. To configure the settings for SAML authentication,
3. Click Settings>> General>> Authentication>> Quick Config.
4. Click SAML sub-tab.



1. Fill all the required fields
2. Click Save.

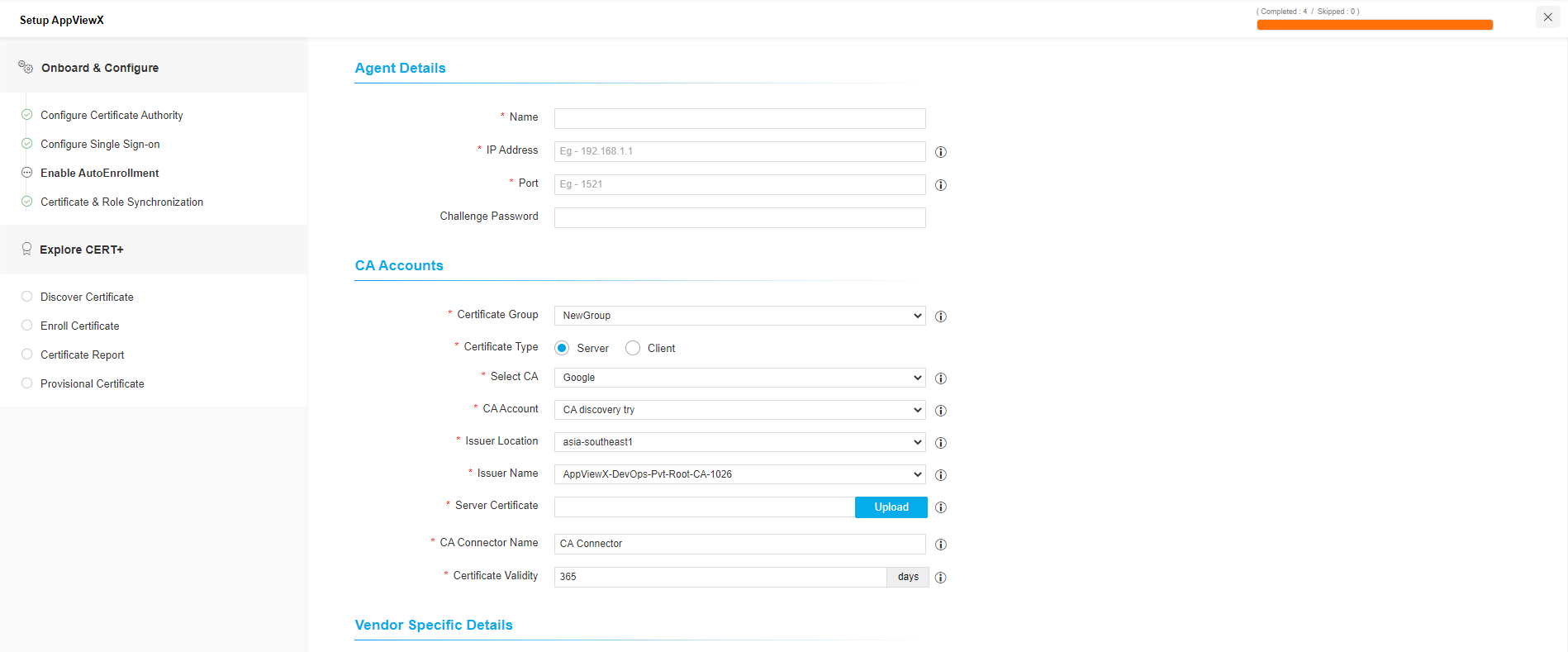
# Enable Auto Enrollment – SCEP

**Onboarding Step 3:**

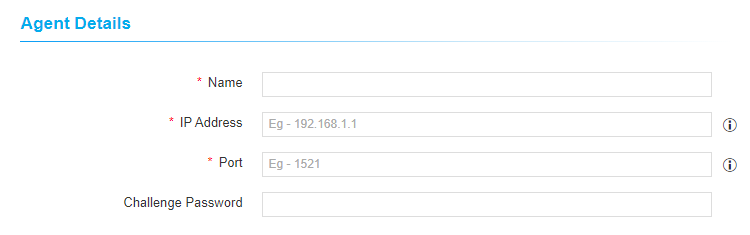
SCEP is Simple Certificate Enrollment Protocol, which is a certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire certificates and associated CA certificates. Architecturally, the SCEP service(agent) is located between a CA and a client. AppViewX supports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

There should be an agent(avx\_vendor\_cert\_scep\_agent) up and running for SCEP in appviewx.

This SCEP plugin can either be in HTTPS or HTTP, but it needs a HTTP gateway running in order to communicate with the client.

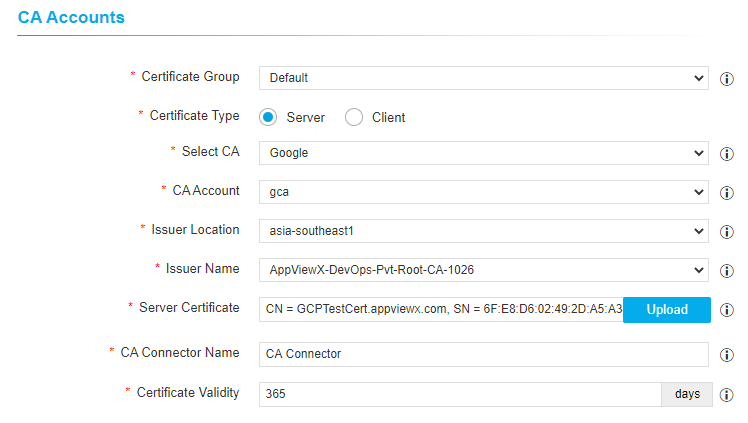


Configure the **Agent Details** details as follows



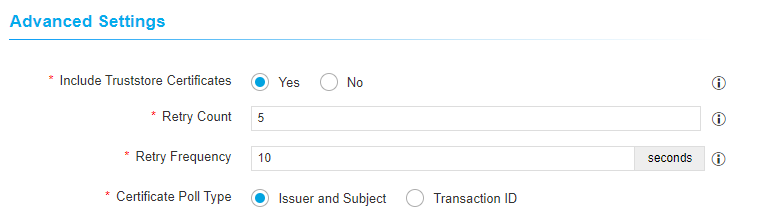
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Type** | **Mandatory** | **Description** | **Validation** |
| Name | Text | Yes | Unique name to identify the Agent setting | No special characters other than ‘.’, ‘-’,’\_’ are allowed. Name should not start with special characters. |
| IP Address | Text | Yes | IP address of the appviewx node | Invalid IP address(example: xxx.xxx.xxx.xxx) |
| Port | Text | Yes | HTTP gateway port of the appviewx node | Port will accept only numerical values between 0 to 65535. |
| Challenge Password | Text | No | A challenge token to be used while enrolling certificates | NA |

Configure the **CA Accounts** details as follows



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Type** | **Mandatory** | **Description** | **Validation** |
| Certificate Group | Select | Yes | Select a specific group under which certificate needs to be enrolled. | NA |
| Certificate Type | Select | Yes | Select a specific certificate type (Server / Client) to be enrolled. | NA |
| Select CA | Select | Yes | Select a specific CA from which the certificate needs to be enrolled. | NA |
| CA Account | Select | Yes | Select a specific CA Account from the selected CA which  is to be used for certificate creation operations. | NA |
| Issuer Location | Select | Yes | Select the issuer location to filter the issuing CA | NA |
| Issuer Name | Select | Yes | Select the issuing CA which should issue the requested certificate | NA |
| Server Certificate | Select | Yes | Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine. | NA |
| CA Connector Name | Text | Yes | Name of the CA connector after certificate is being enrolled. | NA |
| Certificate Validity | Text | Yes | Validity of the certificate to be enrolled. | Certificate validity accepts only numerical values |

Configure the Advanced Settings details as follows –



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

To configure the SCEP settings in the product, follow the below steps

1. Pre-requisite: CA setting details and agent details needs to be configured to proceed with.
2. Click the Menu button.
3. Navigate to CERT+ > ADMINISTRATION > AutoEnrolment > SCEP
4. Select Add or Configure Now
5. Add required details as per the steps mentioned above
6. Click Save

# Certificate and Role Synchronization

**Onboarding step 4:**

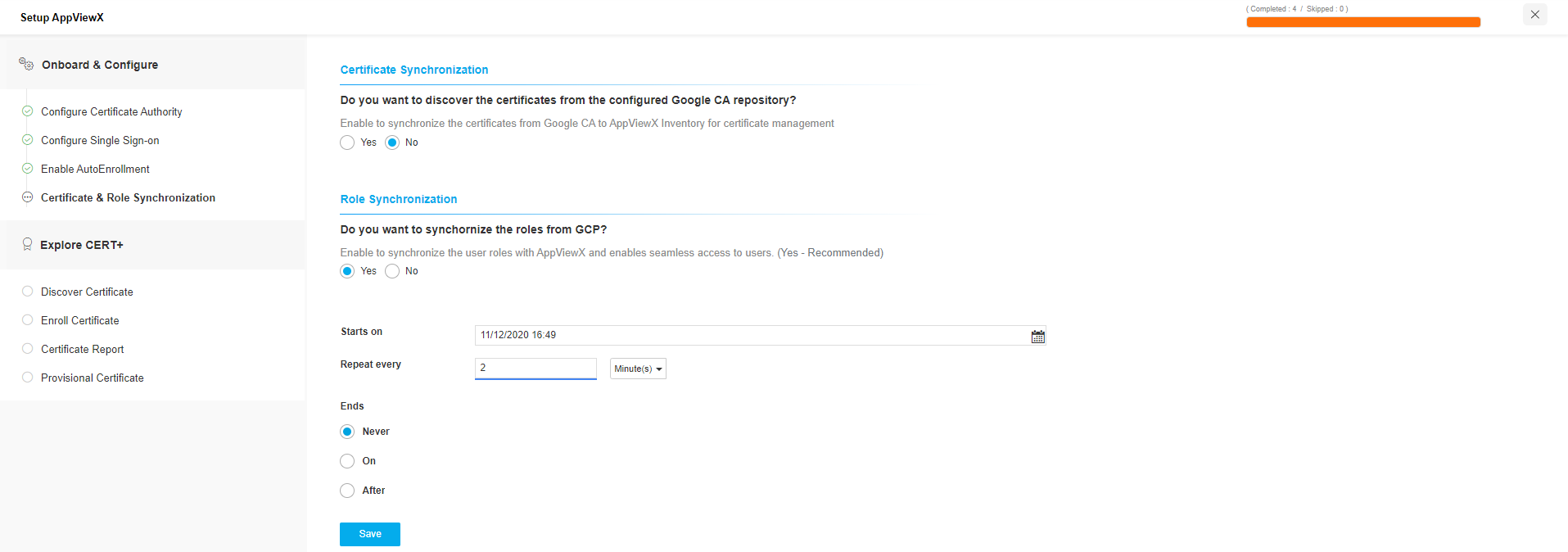
**Certificate Synchronization:**

To keep the certificates of Google CA and AppViewX inventory, user can enable the Certificate synchronization ON. Once enabled, the certificates will be automatically discovered from the configured CA settings and stored in AppViewX certificate inventory.

**Role Synchronization:**

To keep the user policies of Google CA and AppViewX roles synchronized, user can enable the Role synchronization ON and set the frequence of synchronization.

nchronizationnventoryn be automatically discovered from the configured cective pe respective



# Certificate Action

AppViewX allows to create, renew, regenerate, and revoke the certificates through the product. Google CA supports only Create, Regenerate , Suspend and Revoke of certificates in the Beta version and AppViewX limited the support of Renew and Reissue actions.

Supported Actions by Google CA:

* Enroll/Create new certificates
* Regenerate Certificate
* Revoke Certificate

Actions to be supported in future:

* Renew Certificate
* Reissue Certificate

## Enroll

Enroll is termed as Create in the CERT+. It involves the generation of a key pair (private and public key), CSR, and submitting the CSR to the desired CA to procure certificates. The administrator can upload the CSR by generating the key pair on the hosting endpoint or generate the same in AppViewX. While using AppViewX to generate CSR, you can either generate the key on the AppViewX platform or an HSM.

## Regenerate

It is similar to the renew method, but a new CSR from a new private key is generated and sent to a CA for signing.

## Revoke

An administrator can invoke a revocation process if the admin wishes to remove a certificate from the service before its expiration date. This helps when you suspect the private key has been compromised, the certificate is for decommissioned applications or servers, affiliation change with certificate attributes, and the organization or entity bound to the certificate has ceased or suspended operation.

## Renew

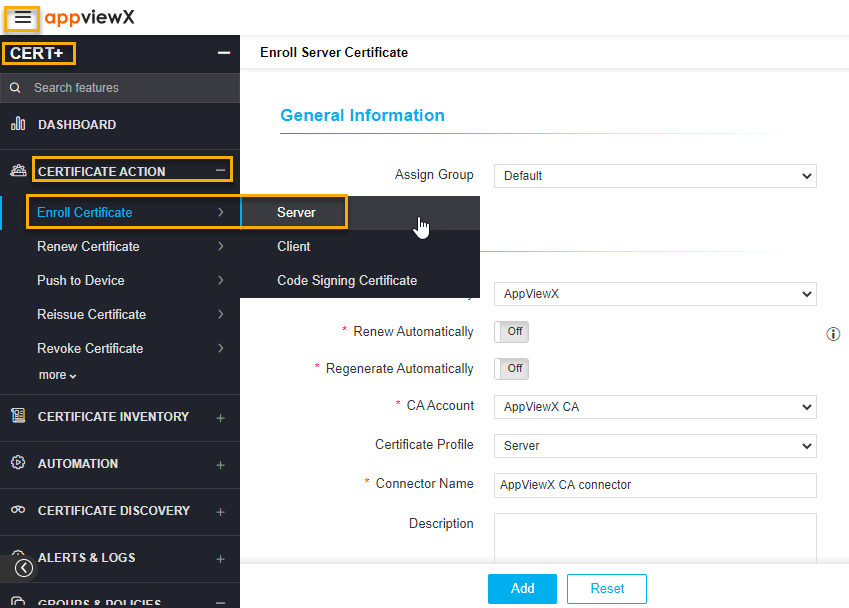
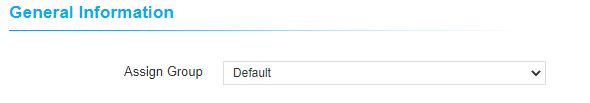
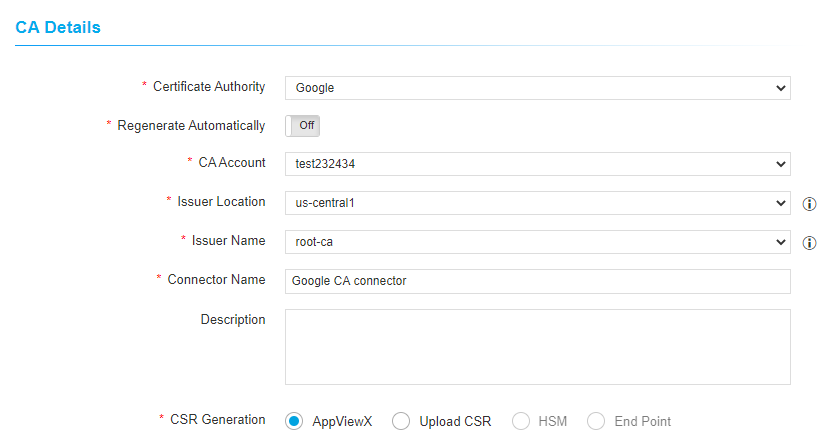
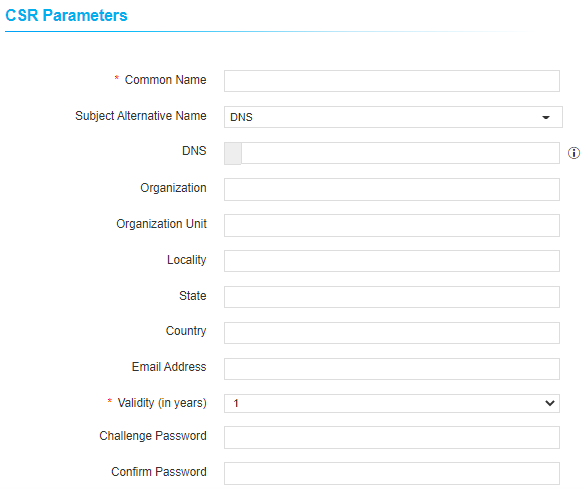
The validity period of the certificate is extended to a new certificate for the same term.

## Reissue

If the private key of the certificate is lost, the certificate is reissued. Reissuing certificates will not extend the validity of the certificate.

# Enroll (or) Create a Certificate

Certificate enrollment in an Google CA is integrated with AppViewX as follows:

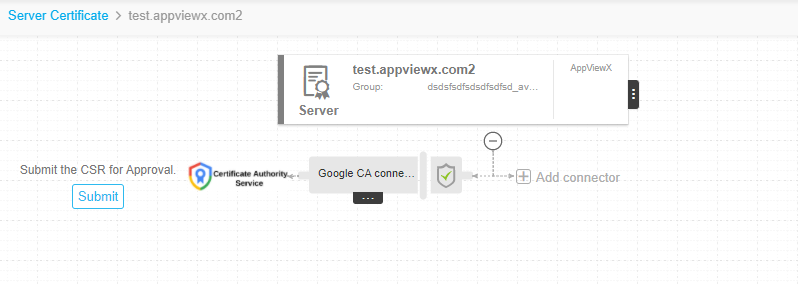
1. Click on the **menu** button.
2. Navigate to **CERT+** > **Certificate Action** > **Enroll Certificate** > **Server** to create a server certificate.
3. Navigate to **CERT+** > **Certificate Action > Enroll Certificate > Client** to create a client certificate.
4. Click **Enroll Certificate** > **Server** in the left navigation panel. The Enroll Server Certificate page appears for the selected certificate category.
5. On the **Enroll Server Certificate** page, enter the details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor Specific Details**, and **Custom Attributes** sections.
6. Under the **General Information** section**,** enter the required details in the respective fields:  
   1. Click the **Assign Group** drop-down.  
      The assigned list of groups is displayed.
   2. Select a desired group from the drop-down option.
7. Under the **CA Details** section**,** enter the required details in the respective fields:  
   
   1. Select **Google** from the **Certificate Authority** drop-down option.
   2. If required, select the **Renew Automatically** toggle button and specify the number of days before expiry.
   3. If required, select the **Regenerate Automatically** toggle button and specify the number of days before expiry.
   4. Select the desired CA Accountfrom the drop-down option.
   5. Enter the Google Connector Name.
   6. Enter Description if needed.
   7. Select desired CSR Generation,
      1. **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given.
      2. **Upload CSR** - Uploaded CSR will be taken as source to populate CSR parameters and submit to CA.
      3. **HSM** - Private key and CSR will be created in the selected HSM device based on CSR parameters given.
      4. **End Point** - Private key and CSR will be created in the selected End Point device based on CSR parameters given.
8. Under the **CSR Parameters** section**,** enter the required details in the respective fields:  
   



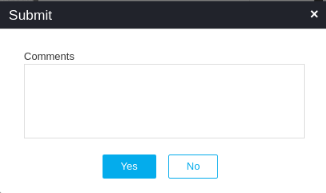
* 1. Select or enter the following fields:

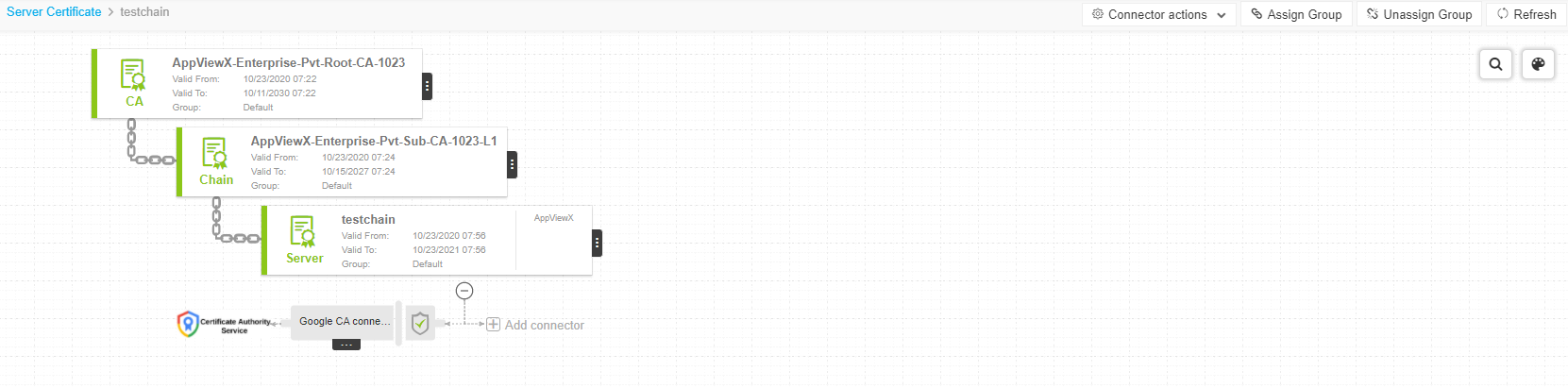
|  |  |  |
| --- | --- | --- |
| **Field** | **Description** | **Type** |
| **\***Common Name | The common name needs to be present in the certificate. | Text box |
| Subject Alternative Name | The subject alternative names have been present in certificate. The available options are DNS and IP Address. | Multi select box |
| DNS | The additional domains need to be present in the certificate. By default, AppViewX adds common names into DNS and User can add additional DNS names if needed. | Text box |
| Organization | The Organization name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Organization Unit | The Organization Unit name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Locality | The Locality name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| State | The State name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Country | The Country name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. For example, US. | Text box |
| Email Address | The name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Validity (in months) | Enter the number of validity in months. | Select box |
| Challenge Password | The challenge password for the certificate, Enter if it's applicable. | Text box |
| Confirm Password | The password to confirm the challenge password entered. | Text box |
| Hash function | The Hash function with which the certificate has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Select box |
| Key Type | The key type has to be used while creating a private and public key pair. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Bit Length | The bit length has to be used while creating a private and public key pair. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |

1. Under the **Attachments** section, enter the required details in the respective fields:
   1. Maintains if there are any additional documents to be maintained in AppViewX.
   2. These documents will not be submitted to CA.
   3. It is a non-mandatory section.
2. Under the **Generic Fields** section, enter the required details in the respective fields:
   1. Application IP address and Device name are the default fields to maintain ip address and device information if needed.
   2. Application IP address and Device name are non-mandatory fields, skip this if you do not want to enter values.
3. Under the Vendor Specific Details section, enter the certificate ID
4. Under the Custom Attributes section, enter the sample details.
5. Click the Add button.
6. Once created successfully, the holistic view page is displayed.



1. Click the Submit button to submit the request to AppViewX Visual workflow.
2. Once the submit action is triggered, the Submit pop-up window appears. Add comments if needed, and then click the **Yes** button.

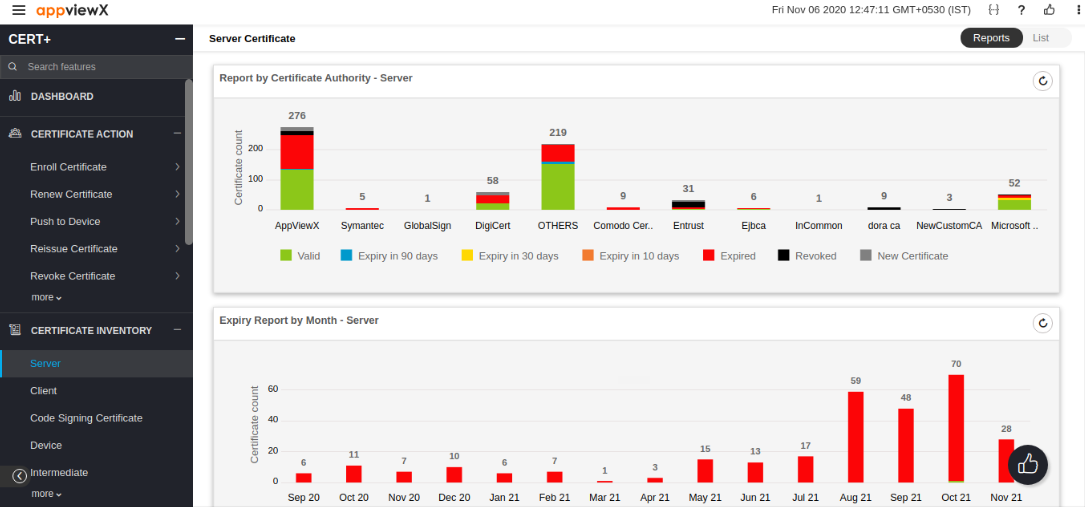
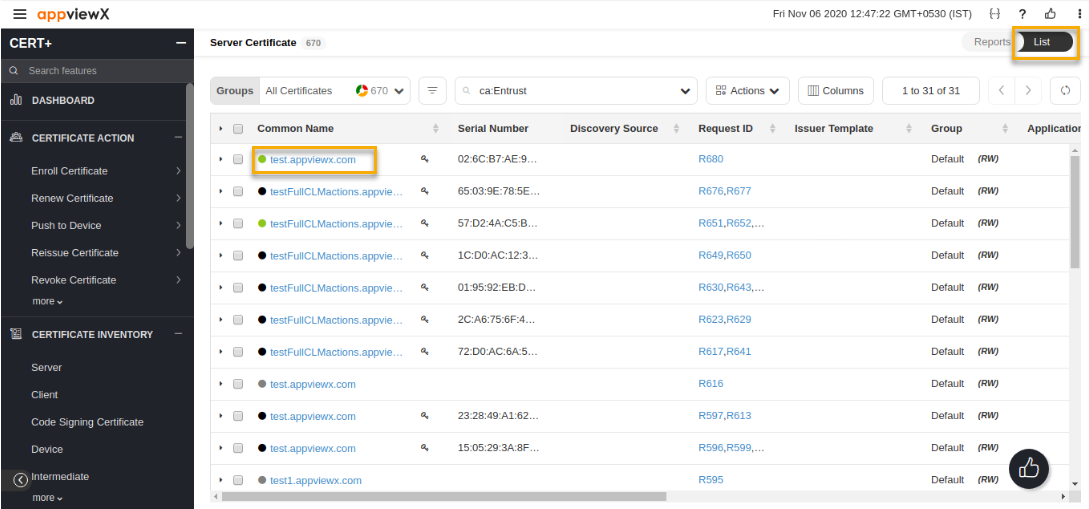
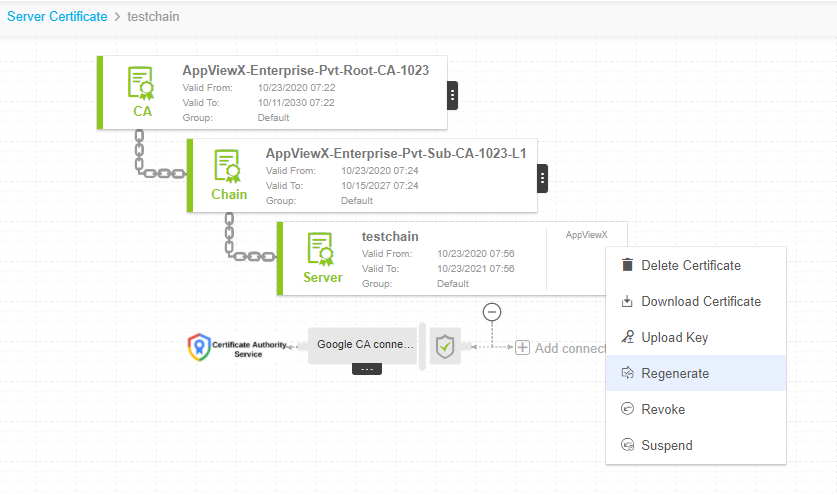
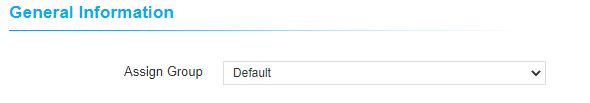
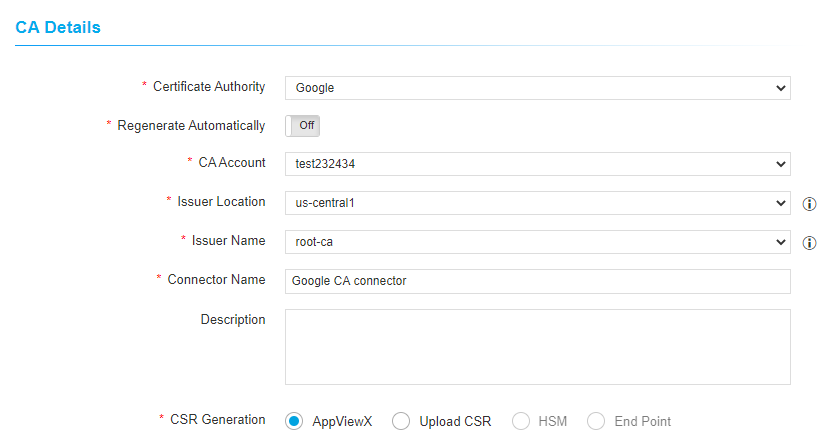


1. Click **Approve** to proceed.
2. The **Approve** pop-up window appears. Click **Schedule later** if the workflow request has to be approved automatically in future.
3. Add comments and click the Yes button
4. Once approved, User can see the Implement option in the holistic view. Click Implement.
5. The Implement pop-up window appears. Click Schedule later if the workflow request has to be implemented automatically in future.
6. Add comments and click the Yes button.
7. The request is in Submit CSR Submission in progress state when the enrollment request is being submitted.
8. Once the CSR submission is successful, the request state will be changed to Submit certificate - retrieval in progress state.
9. If the enrollment request is compliant with conditions defined and auto approval enabled in targeted CA, the certificate will be fetched in a few seconds.
10. If auto approval disabled in targeted CA and CA Manager Approval not configured in the selected CA settings, the respective user has to be logged into CA and approve the request.  
    
11. Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

# Regenerate a Certificate

The regenerate option allows you to create a new certificate with similar parameters of an existing certificate that you can host on a different type of web or application.

To regenerate a certificate,

1. Click on the menu button.
2. Navigate to **CERT+** > **Certificate** **Inventory**.
3. Under the **Certificate Inventory** section, click **Server**, or **Client** depends on the type of certificate you want to renew.  
   
4. On the **Server** **Certificate** page, click **List** on the top right.  
   
5. On the **certificate list** view, click **Common Name** of the certificate to navigate into the holistic view.
6. Hover over the three dots icon on the certificate and click **Regenerate**.
7. Enter the details in the General Information, CA Details, CSR Parameters, Attachments, Generic Fields, Vendor Specific Details, and Custom Attributes sections.
8. Under the General Information section, enter the required details in the respective fields:
9. Click the **Assign Group** drop-down.  
   The assigned list of groups is displayed.
10. Select the desired group from the drop-down option.
11. Under the **CA Details** section**,** enter the required details in the respective fields:  
    1. Select **Google** from the **Certificate Authority** drop-down option.
    2. If required, select the **Renew Automatically** toggle button and specify the number of days before expiry.
    3. If required, select the **Regenerate Automatically** toggle button and specify the number of days before expiry.
    4. Select the desired CA Accountfrom the drop-down option.
    5. Enter the Google Connector Name.
    6. Enter Description if needed.
    7. Select desired CSR Generation,
       1. **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given.
       2. **Upload CSR** - Uploaded CSR will be taken as source to populate CSR parameters and submit to CA.
       3. **HSM** - Private key and CSR will be created in the selected HSM device based on CSR parameters given.
       4. **End Point** - Private key and CSR will be created in the selected End Point device based on CSR parameters given.
12. Under the **CSR Parameters** section**,** enter the required details in the respective fields:  
    



* 1. Select or enter the following fields:

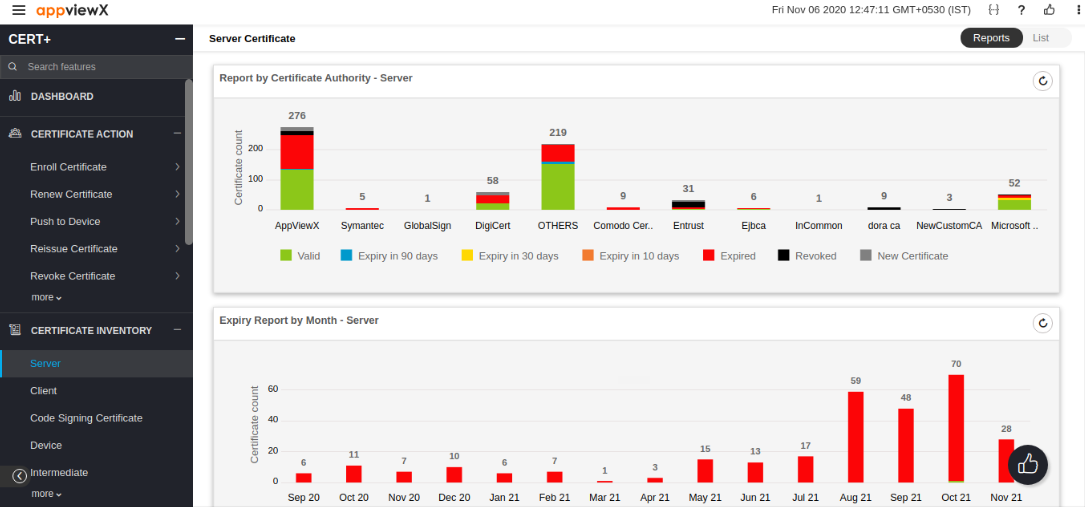
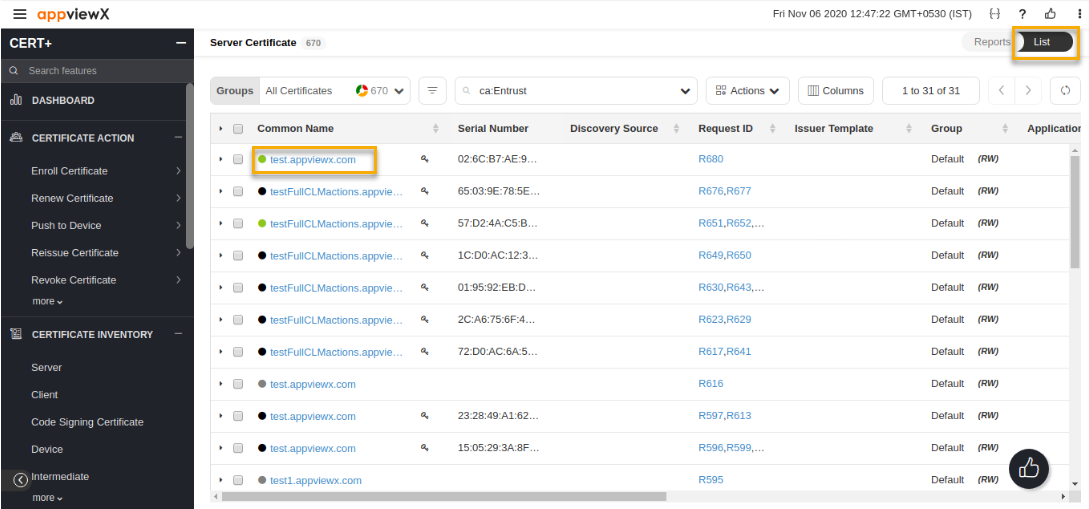
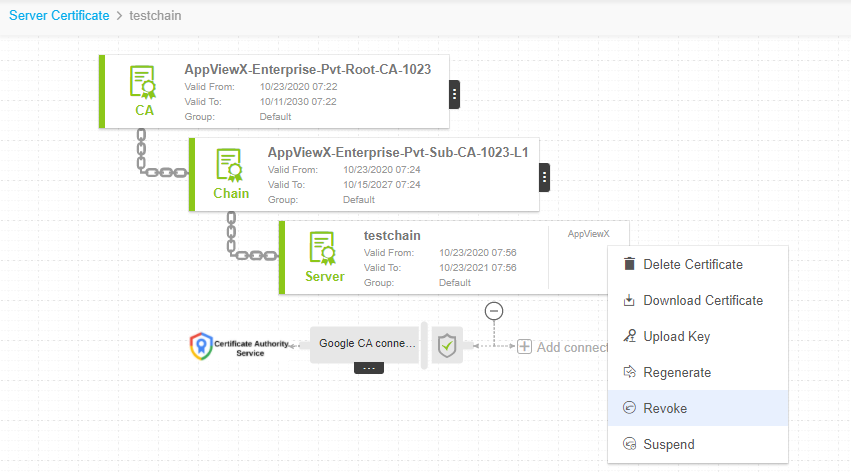
|  |  |  |
| --- | --- | --- |
| **Field** | **Description** | **Type** |
| **\***Common Name | The common name needs to be present in the certificate. | Text box |
| Subject Alternative Name | The subject alternative names have been present in certificate. The available options are DNS and IP Address. | Multi select box |
| DNS | The additional domains need to be present in the certificate. By default, AppViewX adds common names into DNS and User can add additional DNS names if needed. | Text box |
| Organization | The Organization name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Organization Unit | The Organization Unit name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Locality | The Locality name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| State | The State name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Country | The Country name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. For example, US. | Text box |
| Email Address | The name has to be present in the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Validity (in months) | Enter the number of validity in months. | Select box |
| Challenge Password | The challenge password for the certificate, Enter if its applicable. | Text box |
| Confirm Password | The password to confirm the challenge password entered. | Text box |
| Hash function | The Hash function with which the certificate has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto filled and editable based on configuration in the selected group’s policy. | Select box |
| Key Type | The key type has to be used while creating a private and public key pair. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |
| Bit Length | The bit length has to be used while creating a private and public key pair. This field will be auto filled and editable based on configuration in the selected group’s policy. | Text box |

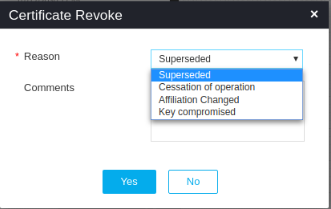
1. Under the Attachments section, enter the required details in the respective fields:
   1. Maintains if there are any additional documents to be maintained in AppViewX.
   2. These documents will not be submitted to CA.
   3. It is a non-mandatory section.
2. Under the Certificate Attributes section, enter the required details in the respective fields:
   1. Enter the Certificate name.
   2. Enter the Type of the certificate.
3. Under the Generic Fields section, enter the required details
4. Click Regenerate.
5. On the Regenerate pop up window, enter comments and click Yes. A request ID, work order ID are generated automatically and then work order status is displayed beside the certificate on the holistic view.
6. Click **Approve** to proceed **Regenerate** action.
7. On the **Approve** page that pops up
8. Click **Schedule later** if the workflow request has to be approved automatically in future.
9. Enter comments to approve the renewal and then click **Yes**. The work order status is displayed beside the connector.
10. Click Implement to proceed with regenerate action.
11. On the **Implement** page that pops up:
12. Click Schedule later if the workflow request has to be approved automatically in future.
13. Enter comments to approve the renewal, then click Yes.
14. Click the Refresh button on the top right until the regenerate status updates.
15. After the regenerate action is completed, the status updates to **Completed**.

# Revoke a Certificate

You can revoke an issued certificate. For example, you might need to revoke a certificate if the certificate is no longer required (or) certificate’s private key is compromised. Make sure that you have permission to revoke the certificate, you can submit a request to the certificate authority to revoke an issued certificate. 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.

To revoke a certificate,

1. Click on the menu button.
2. Navigate to **CERT+** > **Certificate** **Inventory**.
3. Under the **Certificate Inventory** section, click **Server**, or **Client** depends on the type of certificate you want to renew.  
   
4. On the **Server** **Certificate** page, click **List** on the top right.  
   
5. On the **certificate list** view, click the **Common Name** of the certificate to navigate into the holistic view.
6. Hover over the three dots icon on the certificate and click **Revoke**.
7. 

On the **Certificate** **Revoke** pop up window, select **Reason** from the drop down menu, enter the comments and click **Yes**.   


1. Click **Approve** to proceed with **Revoke** action.
2. On the **Approve** page that pops up:
3. Click **Schedule later** if the workflow request has to be approved automatically in future.
4. Enter comments to approve the renewal and then click **Yes**. The work order status is displayed beside the connector.
5. Click **Implement** to proceed with **Revoke** action.
6. On the **Implement** page that pops up:
7. Click **Schedule later** if the workflow request has to be approved automatically in future.
8. Enter comments to approve the renewal, then click **Yes**.
9. Click the Refresh button on the top right until the revoke status updates.
10. After the revoke action is completed, the status updates to **Completed**.

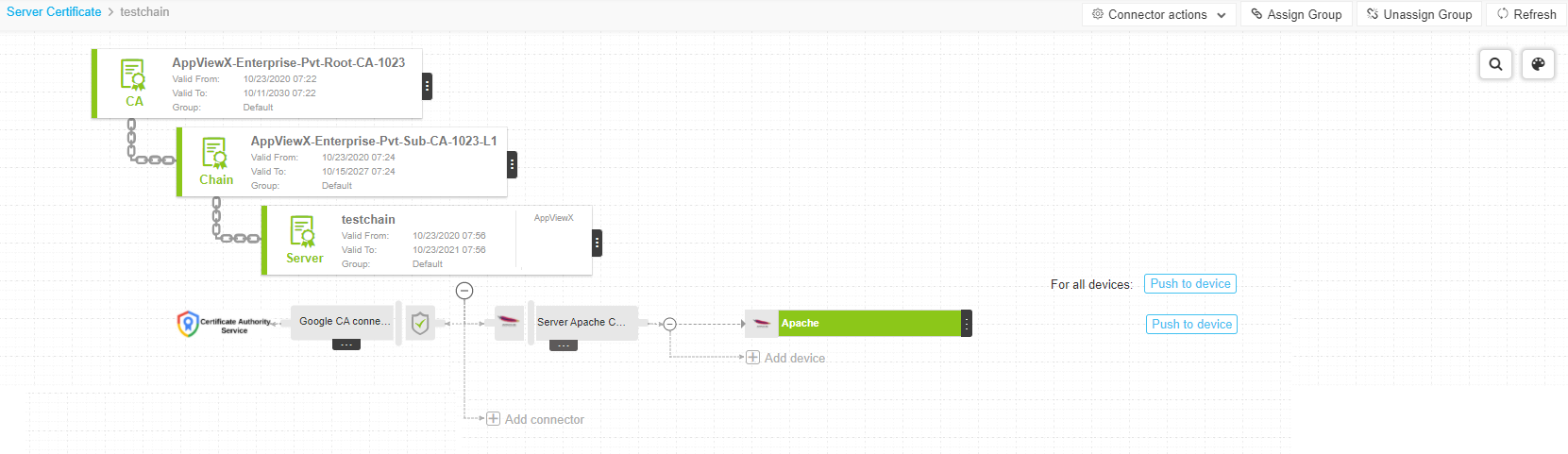
# Push to Device

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 this case, users need not complete the process manually.

### Add an Application Connector to the Certificate Topology

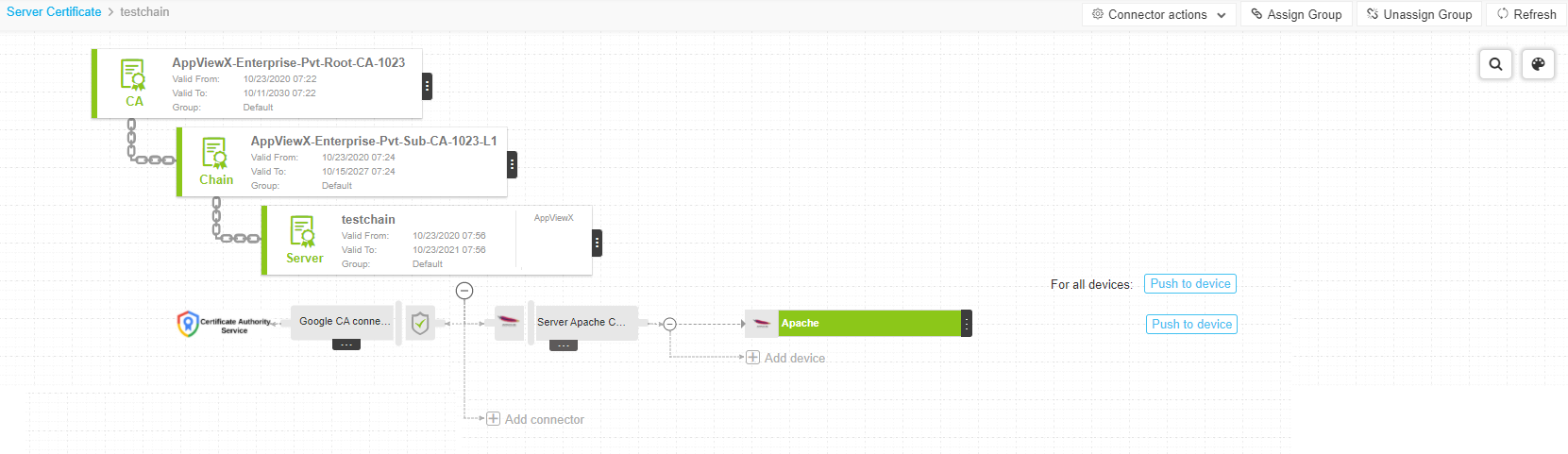
To add an application connector to a server certificate topology,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu**>> **CERT+** >> **CERTIFICATE ACTION.**
3. Under the **Certificate Action** menu select **Push to Device** submenu and then click **Server**, **Client, Intermediate** or **root** depending on the type of certificate you want to push.
4. On the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.
5. On the Certificate topology page, click **Add Connector.**
6. On the **Add Connector** pop-up window, select the device type from the **Category** dropdown.
7. Select the device vendor from the **Vendor** dropdown.
8. In the **Connector Name** field, enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
9. Enter a description for the connector. This description shows up when you hover over the connector within the Certificate topology.
10. From the list of available application objects, click the (Add to list) icon beside each device you want to select.
11. From the Certificate type dropdown, click the type of certificate to be used with the connector.
12. From the Certificate file name field, enter the name of the certificate. The file format of the selected certificate type (in step 13) will be automatically displayed.
13. In the **Key File Name** field, enter a name for the key file.
14. Select the **Push root and intermediate certificates** to be pushed to the device.
15. In the Script location field, specify whether the **Pre - Push script** and **Post - Push script** file is In AppViewX or device.
16. Enter the script location that must be executed before and after the push in the **Pre - Push script** and **Post - Push script** fields respectively.
17. Select the **Overwrite** checkbox to overwrite existing certificates with the new certificate.
18. Select **Push** **automatically** checkbox to push certificates to the device automatically.
19. (Only applicable for F5 application type) The Secure Push checkbox will be selected by default. This option encrypts certificates while pushing them to a device. You can uncheck this option if you have the necessary permissions.
20. \*For .jks Keystore, a valid alias has to be entered to reference the certificate within the key store.
21. Click Save to add the application connector to the Certificate topology.



### Push a certificate to a device

To push a certificate to a device,

1. Log in to the **AppViewX** application with valid credentials.
2. Click the **Menu >> CERT+ >> CERTIFICATE ACTION**
3. Under the **Certificate Action** menu select **Push to Device** submenu and then click **Server**, **Client, Intermediate** or **root** depending on the type of certificate you want to push.
4. On the Certificate list view page, locate the certificate you want to push and click its name on the **Common Name** column.
5. On the certificate topology page, click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed. 
6. On the **Confirmation** pop up window, enter comments and click OK.
7. A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.
8. Click **Approve** to approve the push request.
9. On the Confirmation screen that pops up:

* Click **On** or **Off** button in the **Manual** **Implementation** field to choose the mode of implementation.
* If you select **Off**, set the date and time that you want the cert push to occur.
* Enter comments and click **Yes**.

1. The work order status displayed beside the connector updates to **Push-Review In Progress**.
2. Click **Implement** to implement the push request.
3. On the Confirmation screen that pops up:

* Click **On** or **Off** button in the **Manual** **Implementation** field to choose the mode of implementation.
* If you select **Off**, set the date and time that you want the cert implementation to occur.
* Enter comments and click **Yes**.

1. Click the **Refresh** icon on the top of the page until the topology updates.
2. After the push action is completed, the status updates to **Completed**.

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

|  |  |
| --- | --- |
| **Color** | **Certificate Status** |
| Green | The certificate is available and valid. |
| Red | The certificate has expired. |
| Gray | Certificate push action failed. |
| Blue | The certificate will expire in 90 days. |
| Yellow | The certificate will expire in 30 days. |
| Orange | The certificate will expire in 10 days. |
| Black | The certificate has been revoked. |
| Mid Purple | The certificate associated with profiles is manually removed. |

## Roll Back a Certificate from a Device

The Rollback option allows you to revert to the previous successful certificate pushed to an SSL profile or template. Rolling back to the last known good state can be performed only from the individual profile level and the Rollback option only appears in the dropdown **Action** list if a certificate has already been successfully pushed to the device.

### Prerequisites

Before rolling back a certificate that was pushed to a device, ensure that the following are true:

* You have the necessary role-based access controls and workflow access to the template and request.

### Roll back a certificate from a device

To roll back a certificate from a device,

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu**>> **CERT+** >> **Certificate** **Inventory.**
3. Under **Certificate** **Inventory**, click **Server**.
4. On the certificate list view, click the **Common** **Name** of the certificate to view the topology.
5. Click **Rollback**.
6. On the Confirmation screen that pops up, enter comments to rollback a certificate, then click **OK**. A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.
7. Click **Approve** to approve the rollback request.
8. On the Approve screen that pops up:

* Click **On** or **Off** button in the **Manual** **Implementation** field to choose the mode of implementation.
* If you select **Off**, set the date and time that you want the certificate rollback to occur.
* Enter comments to approve the rollback, then click **Yes**. The work order status is displayed beside the connector.

1. Click **Implement** to implement the rollback request.
2. On the screen that pops up:

* Click **On** or **Off** button in the **Manual** **Implementation** field to choose the mode of implementation.
* If you select **Off**, set the date and time that you want the certificate rollback implementation to occur.
* Enter comments to approve the rollback, then click **Yes**.

1. The work order status is displayed beside the connector.
2. Click the **Refresh** icon on the top-right until the topology updates.
3. After the rollback is completed, the status updates to **Completed** and the color of the connector changes to gray.

# Finding More Information

To access Software Release Notifications for AppViewX Releases, visit our Help center at <https://help.appviewx.com/home>. You need to log in to your AppViewX account. From the Help center, search by the specific release number or navigate to Release Portal and choose the release, for example, v20.3.0.

# Documentation Feedback

We request you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [tech-documentation@appviewx.com](mailto:tech-documentation@appviewx.com).

If you are preferred to send feedback through e-mail, be sure to include the following information with your comments:

* Document or topic name
* URL or page number
* Software release version (if applicable).

# Requesting Technical Support

Technical product support is available through AppViewX help support center, request to send an email to [help@appviewx.com](mailto:help@appviewx.com).

# Self-Help Online Tools and Resources

For quick and easy problem resolution, AppViewX is designed an online self-service portal called the help support center that provides you with the following features:

* Find help support center: <https://help.appviewx.com/home>
* Find product technical documentation: <https://help.appviewx.com/documentation>
* Find solutions and answer questions using our Knowledge Base: <https://internalkb.appviewx.com/knowledge-base>
* Download the latest versions of software: <https://release.appviewx.com>