AppViewX on ServiceNow Guides

Version: 2025.05.1

Copyright AppViewX, Inc.

Trademarks

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.7	Updated the document for version 2025.05.1.	May 2025
1.6	Updated the document for version 2025.02.1.	February 2025
1.5	Updated the document for version 2024.08.1.	November 2024
1.4	Updated the document for version 2024.04.1.	May 2024
1.3	Updated the document for version 2024.02.1.	February 2024
1.2	Updated the document for version 2023.9.0.	September 2023
1.1	Updated document for version 2023.8.1	August 2023
1.0	Initial release of document for version 2023.1.0	January 2023

About this Guide

This section includes the following guides that will assist you in installing, configuring, and using the AppViewX plugin available on ServiceNow's App store:

- AppViewX on ServiceNow Install and Configuration Guide
- AppViewX on ServiceNow User Guide

Audience

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

Third-Party Software Acknowledgments

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

For example,

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

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: AppViewX on ServiceNow Install and Configuration Guide

This guide describes the process of installing and configuring AppViewX's plugin available on ServiceNow's App store.

Prerequisites

- ServiceNow must be reachable via AppViewX through REST APIs.
- AppViewX must be reachable from ServiceNow either directly (SaaS deployment) or via MID server (On-prem deployment).

> **Note:**
> For more information on downloading and installing the MID server, click here.

- oAuth 2.0 authentication must be available between AppViewX and ServiceNow.
- All CA accounts must be configured in AppViewX.
- All CA Groups and Policies must be defined in AppViewX.
- Certificate Discovery must be complete and certificates managed in the AppViewX CERT+ inventory.
- The AppViewX plugin must be downloaded and installed on the ServiceNow instance.

For more information, refer to the Installing AppViewX Plugin section.

- User Groups must be configured in ServiceNow.
- Roles must be mapped to the User Groups on ServiceNow.
- User on-boarding must be completed on AppViewX.

Supported ServiceNow Versions

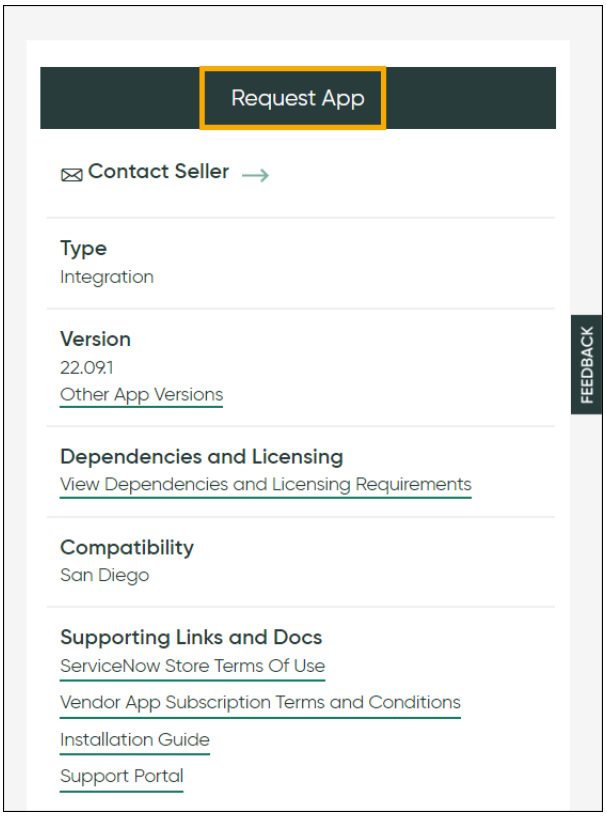
The following ServiceNow versions are supported:

- San Diego
- Tokyo
- Utah
- Vancouver
- Washington DC

• Xanadu
• Yokohama

Installing the AppViewX Plugin

1. Open the ServiceNow Store web page and search for the application by typing **AppViewX** in the search bar.
2. On the Search results page, click on the app.
3. To install the app, on the app page, click **Request App**.

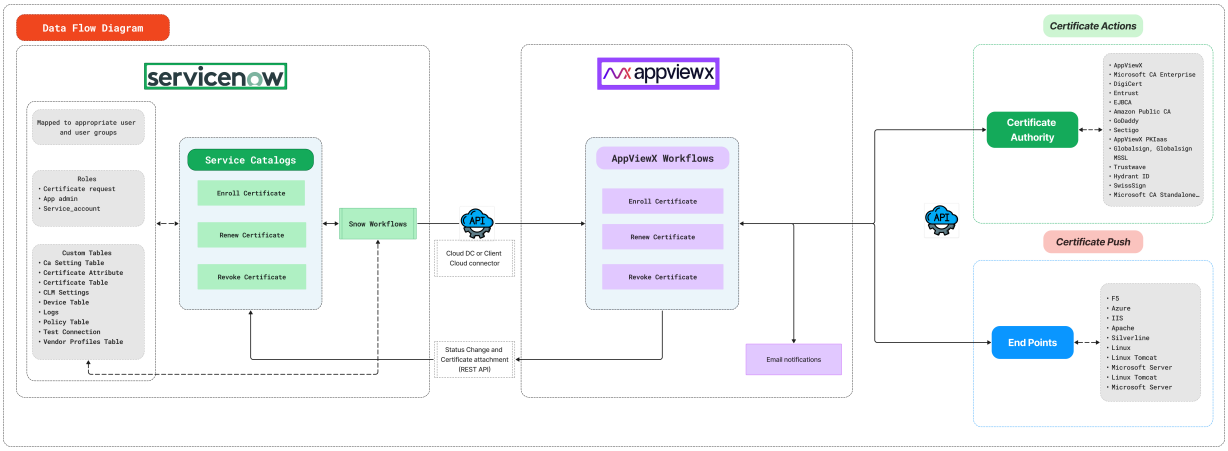


Enabling AppViewX Modules

After installing AppViewX Plugin, it is recommended to execute the Fix Scripts to enable the AppViewX module for connection settings page.

1. Log into ServiceNow and search for the Fix Scripts by using the search bar in the left navigation panel.
2. On the search result, click the **Fix Scripts**.
3. On the **Fix Script** page, click the **Run Fix Script** button.
4. On the **Run Fix Script** popup window, click **Proceed**.

Communication Flow with ServiceNow and AppViewX



Establishing Communication from ServiceNow to AppViewX

Overview

To ensure that ServiceNow is able to communicate with AppViewX, you must create a Service Account on AppViewX. In order to create a Service Account, you must first configure the user group that will be associated with the service account. The user group must be associated with a resource that will perform the necessary CLM operations on ServiceNow.

Creating a Resource

You need to create a resource and assign permission(s) for the resource to be able to trigger the AppViewX workflows from ServiceNow.

1. Go to the **Resource** page.

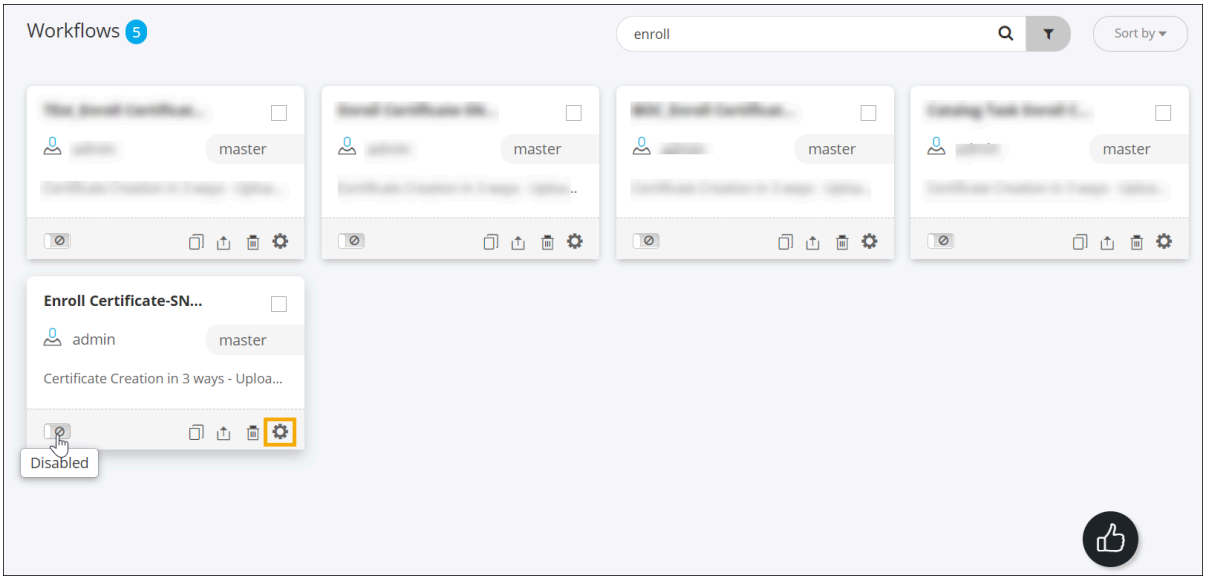
New Menu	Old Menu
a. From the main menu, select **Platform**. b. In the **Platform** module, from the left menu, under **IDENTITY**, click **Resource**. The **Resource** page is displayed.	a. From the main menu, select **Account** > **Resource**. b. In the **Platform** module, from the left menu, under **IDENTITY**, click **Resource**. The **Resource** page is displayed.
For more information on how to switch between menus, click here.	

2. On the **Resource** page, to create a new user group, from the command bar on the top right, click  .
3. On the **Add** page, under the **Information** tab, enter the name of the resource you want to create. For example: **snow_resource**.
4. Click **Save**.
5. On the **Add** page, under the **Access Control** tab, click **Certificate** under **List**.
6. To give this resource Read/Write (**RW**) permission for all certificate groups, on the **Add** page, under the **Access Control** tab, from the **List** menu, click **Certificate**.
7. To give the resource access to the certificate groups automatically, even when new certificate groups are added, in the search bar, type the regex (.*) and click **Add as regex**.
   The **RW** icon turns green and the resource is granted access to all the configured certificate groups.
8. To give this resource **RW** access to the CLM workflows, on the **Add** page, under the **Access Control** tab, from the **List** menu, click **Workflow Studio**.
9. Select and give **RW** access to the following workflows:
   - Enroll Certificate-SNOW APP
   - Renew Certificate-SNOW APP
   - Revoke Certificate-SNOW APP
   - certificate_new_request
   - certificate_renew_request
   - certificate_revoke_request
10. Click **Save**.
11. To allow this resource to trigger workflow requests, under the **Access Control** tab, from the **List** menu, click **Workflow Requests**.
12. Select the checkbox next to the workflow name to give **RW** access to the following workflows:
    - Enroll Certificate-SNOW APP
    - Renew Certificate-SNOW APP
    - Revoke Certificate-SNOW APP
    - certificate_new_request
    - certificate_renew_request
    - certificate_revoke_request
13. Click **Save**.

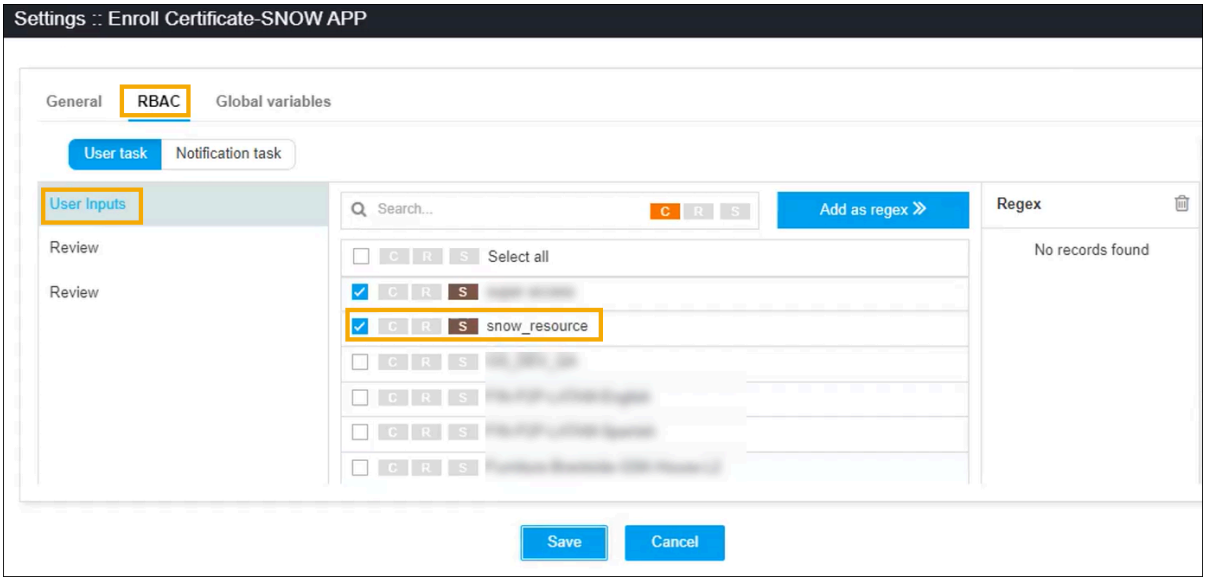
Configuring RBAC for User Inputs

Once this resource is created and given all the necessary certificate and workflow permissions, you also need to give access to this resource to enter user inputs in the input form for each of the three CLM workflows.

1. Navigate to **Workflow** > **Store** in AppViewX's **Automation** module.
2. On the **Store** page, search for the **Enroll Certificate-SNOW APP** workflow.
3. Before configuring the RBAC settings for the workflow, disable it.
4. Hover the mouse over the workflow name, and then click  .



5. From the bottom right corner of the card, click  .
6. In the **Settings** pop-up window that is displayed, click on the **RBAC** tab.
7. Under the **RBAC** tab, for **User Inputs**, select **S** for the resource created.



The resource will now have the permission to submit user inputs for the workflow.

8. Repeat this process for the following workflows as well:
   - Renew Certificate-SNOW APP
   - Revoke Certificate-SNOW APP
   - certificate_new_request
   - certificate_renew_request
   - certificate_revoke_request

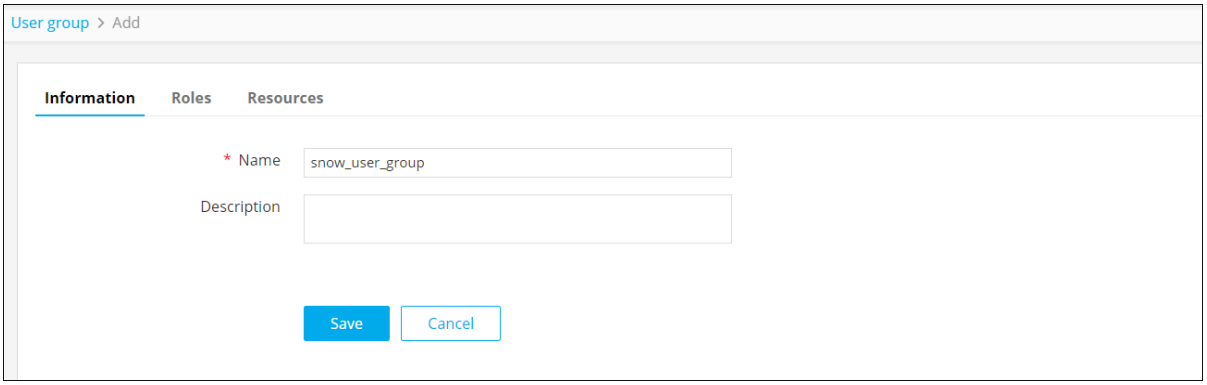
Creating a User Group

You need to create a user group and map it to the role and resource created for ServiceNow in order to run the workflows.

1. Navigate to the **User group** page in AppViewX.

New Menu	Old Menu
a. From the main menu, select **Platform**. b. In the **Platform** module, from the left menu, under **IDENTITY**, click **User group**. The **User group** page is displayed.	From the main menu, select **Account** > **User group**. The **User group** page is displayed.
For more information on how to switch between menus, click here.	

2. On the **User group** page, to create a new user group, from the command bar on the top right, click  .
3. On the **Add** page, under the **Information** tab, enter the name of the user group you want to create. For example: **snow_user_group**.



4. On the **Add** page, under the **Roles** tab, select the **CLM Manager** role to map to this user group.

> **Note:**
> The CLM Manager role is shipped out of the box with AppViewX, with all the necessary permissions required for CLM operations on ServiceNow.

5. Click **Save**.
6. On the **Add** page, under the **Resources** tab, select the role created for ServiceNow operations here.
7. Click **Save**.

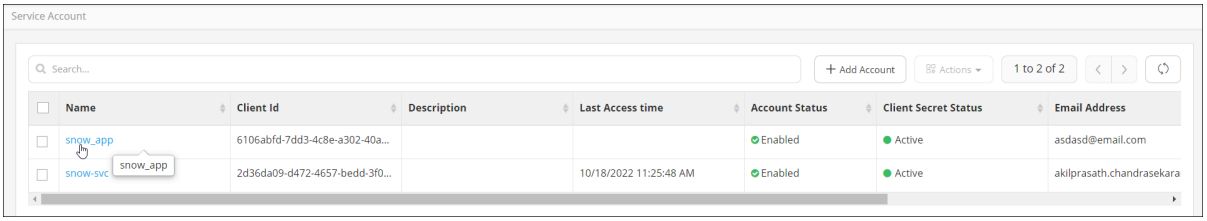
Creating a Service Account

A Service Account is necessary for communication between AppViewX and ServiceNow.

1. Navigate to the **Service Account** page in AppViewX.

New Menu	Old Menu
a. From the main menu, select **Platform**. b. In the **Platform** module, from the left menu, under **IDENTITY**, click **Service Account**. The **Service Account** page is displayed.	From the main menu, select **Account** > **Service Account**. The **Service Account** page is displayed.
For more information on how to switch between menus, click here.	

2. On the **Service Account** page, from the command bar on the top right, click **Add Account**.
3. On the **Add** page, under the **Information** tab, in the **Account Information** section, enter the **Name** for the service account. For example: snow_app.
4. In the **Contact Information** section, enter the email address of the service account holder.
5. Click **Save**.
6. On the **Add** page, under the **User Group** tab, associate the service account with the user group configured here.
7. Click **Save**.
   The service account is created and is displayed on the **Service Account** page.



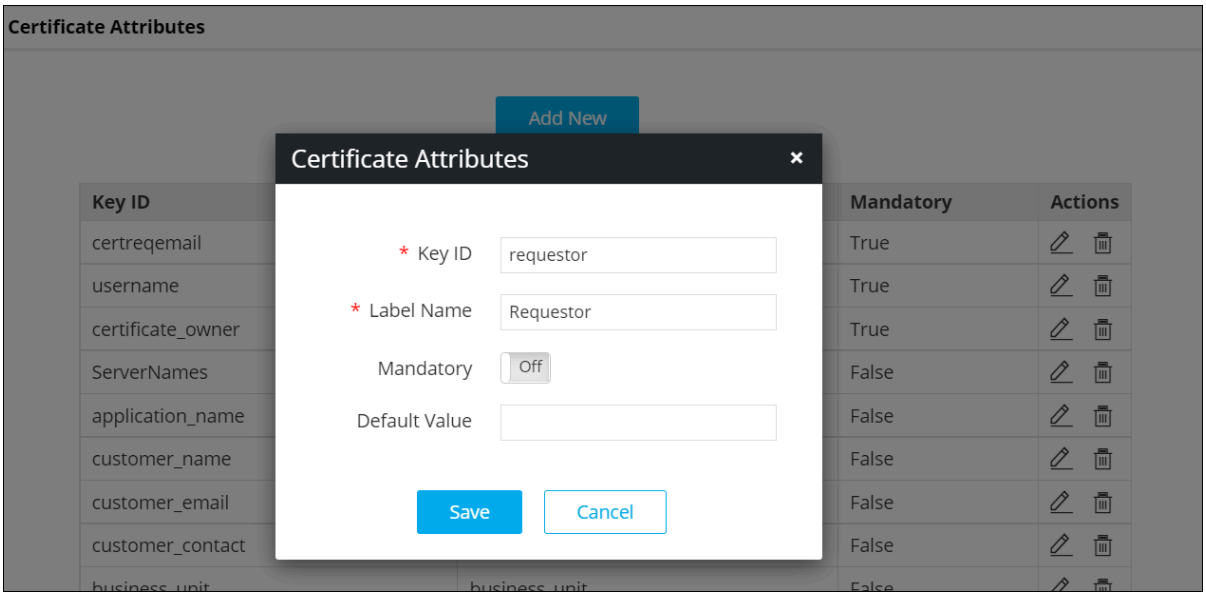
8. To generate the Client Id and Client Secret for this account, click on the service account.
   The **Client Id** and **Client Secret** are displayed under the **Information** tab in the **Account Information** section.
9. To make the Client Secret visible, click **Show**.
10. To regenerate the Client Secret, in case of a security compromise, click **Regenerate**.

> **Note:**
> - The Regenerate button is enabled only when the Client Secret is visible.
> - If you regenerate the Client Secret, it must be updated on the AppViewX Settings page in ServiceNow.

Configuring Certificate Attributes

Adding the email address of the logged in user in ServiceNow as a certificate attribute allows the user to fetch certificates from AppViewX when the same user is not configured in AppViewX.

1. From the main menu, go to the **CERT+** module.
2. On the **CERT+** page, from the menu on the left, scroll down to the **Administration** section and click **Certificate Attributes**.
3. On the **Certificate Attributes** page, click **Add New**.
4. In the **Certificate Attributes** pop-up window that is displayed, add any of the following the key IDs and label names as:
   - **Key ID**: requestor and **Label Name**: Requestor
   - **Key ID**: requestor_assignment_group and **Label Name**: Requestor Assignment Group
   - **Key ID**: ritm_number and **Label Name**: RITM Number



5. Click **Save**.
   The requestor email address will be added as a certificate attribute and can be used to fetch certificates when renewing or revoking certificates from ServiceNow.

Configuring Client Secret Validity in AppViewX

The default validity for the Client Secret is set to 180 days. You can change this number as per your requirement from AppViewX Settings.

1. Go to the **Settings :: Authentication** page in AppViewX.

New Menu	Old Menu
a. From the main menu, select **Platform**. b. In the **Platform** module, from the left menu, under **ACCESS MANAGEMENT**, select **oAuth**. The **Settings :: Authentication** page is displayed with the oAuth tab open.	a. From the main menu, select **Settings** > **General** > **Authentication**. The **Settings :: Authentication** page is displayed with the LDAP tab open by default. b. On the **Settings :: Authentication** page, click the **oAuth** tab.
For more information on how to switch between menus, click here.	

2. Under the **oAuth Settings** tab, in the **Client Secret validity** field, enter the required validity value.
3. Click **Save**.

Configuring AppViewX Settings - Domain Separation Disabled

Once the AppViewX plugin is installed, you need to configure it on your ServiceNow instance.

1. On the ServiceNow instance, in the **Filter navigator**, search for the app by typing the keyword.
   The AppViewX plugin page is displayed with the **AppViewX Catalog** page open by default.
2. From the navigation pane on the left, under **Administration**, click **AppViewX Settings**.
   The **AppViewX Settings** page is displayed.
3. On the **AppViewX Settings** page, enter the required field information.
   The following table describes the fields in this section:

Connection Settings - Field and Description Table

Field	Description
Instance URL	Enter the AppViewX instance URL where the plugin is configured. **Note:** • For both on-premise and SaaS deployments, ensure that the URL does not include / at the end. • For on-premise deployments, ensure that the port number is included in the URL.
Client ID	Enter the Client ID generated during the creation of the Service Account. For more information, click here.
Client Secret	Enter the Client Secret generated during the creation of the Service Account. For more information, click here.
MID Server	Enter the MID Server name. The MID Server allows you to reach AppViewX from ServiceNow even when AppViewX is not exposed to the internet. **Note:** This is required only for on-prem deployments.
Enable AppViewX Inventory Sync	Select the **Yes | No** checkbox to enable the AppViewX inventory sync. For more information on how to schedule the sync, click here.

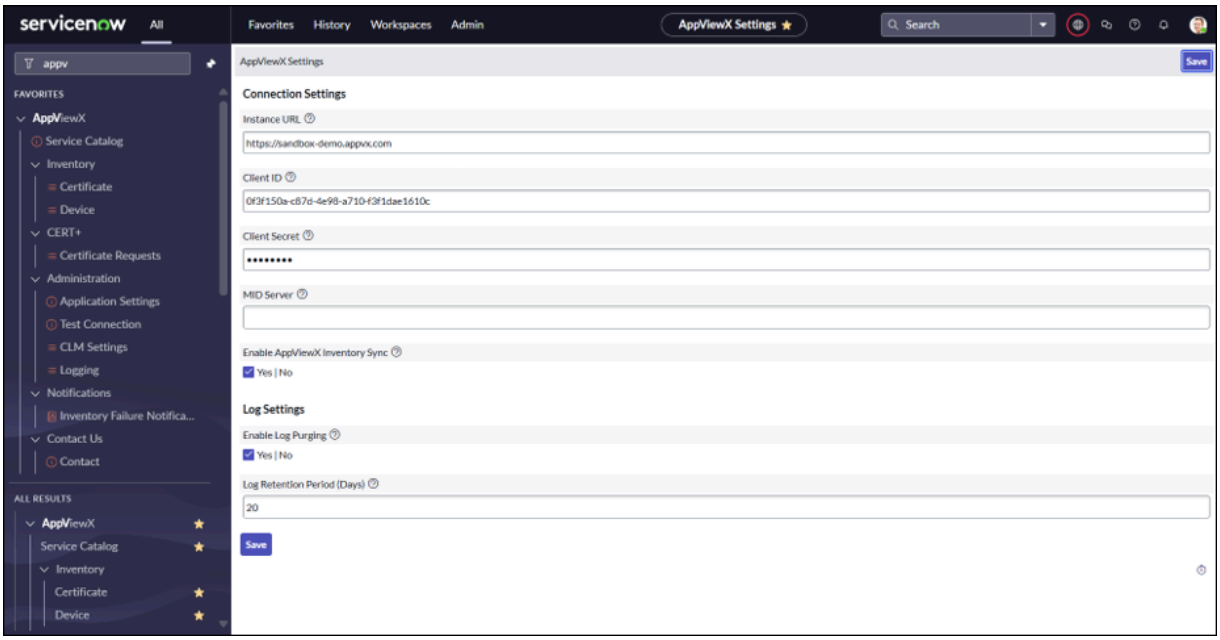
Field	Description
Enable Log Purging	Select thSelect the**Yes | No** checkbox to enable the Log Purging.
Log Retention Period (Days)	Enter the number of days to hold logs for the given time period.
**: Mandatory fields*	

4. Click **Save**.

Configuring AppViewX Settings - Domain Separation Enabled

Domain separation allows users to configure settings for multiple companies.

1. On the ServiceNow instance, in the **Filter navigator**, search for the app by typing the keyword.
   The AppViewX plugin page is displayed with the **AppViewX Catalog** page open by default.
2. From the navigation pane on the left, under **Administration**, click **AppViewX Settings**.
   The **AppViewX Settings** page appears, displaying the list of configured settings.
3. On the **AppViewX Settings** page, click **New**.
4. On the **Connection Settings** page,enter the required field information.



The following table describes the fields in this section:

Connection Settings - Field and Description Table

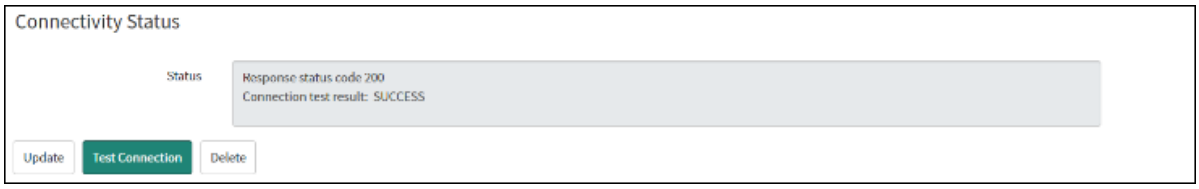
Field	Description
***Instance URL**	Enter the AppViewX instance URL where the plugin is configured. **Note:** • For both on-premise and SaaS deployments, ensure that the URL does not include / at the end. • For on-premise deployments, ensure that the port number is included in the URL.
***Client ID**	Enter the Client ID generated during the creation of the Service Account. For more information, click here.
***Client Secret**	Enter the Client Secret generated during the creation of the Service Account. For more information, click here.
***MID Server**	Enter the MID Server name. The MID Server allows you to reach AppViewX from ServiceNow even when AppViewX is not exposed to the internet. **Note:** This is required only for on-prem deployments.
Enable AppViewX Inventory Sync	Select the **Yes | No** checkbox to enable the AppViewX inventory sync. For more information on how to schedule the sync, click here.
Enable Log Purging	Select thSelect the**Yes | No** checkbox to enable the Log Purging.
Log Retention Period (Days)	Enter the number of days to hold logs for the given time period.
**: Mandatory fields*	

5. Click **Submit**.

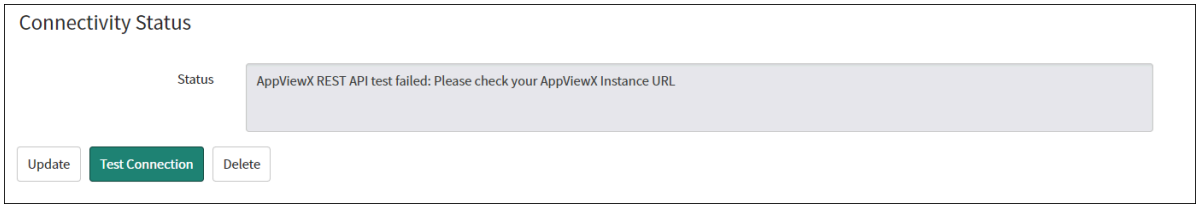
Testing the AppViewX-ServiceNow Connection

To test the connectivity between AppViewX and ServiceNow:

1. From the navigation pane on the left, under **Administration**, click **Test Connection**.
   The **Test Connection** page is displayed.
2. Click **Test Connection**.
   The **Connectivity Status** is updated as per the Success or Failure of the connection.
   - **Success**



   - **Failure**



> **Note:**
> If, at any point of time, the AppViewX plugin does not work or displays an error message, the administrator must test the connection and verify the Instance URL and Client ID details.

Troubleshooting the AppViewX-ServiceNow Connection

The following table captures the causes of connectivity failure between AppViewX and ServiceNow and solution for troubleshooting:

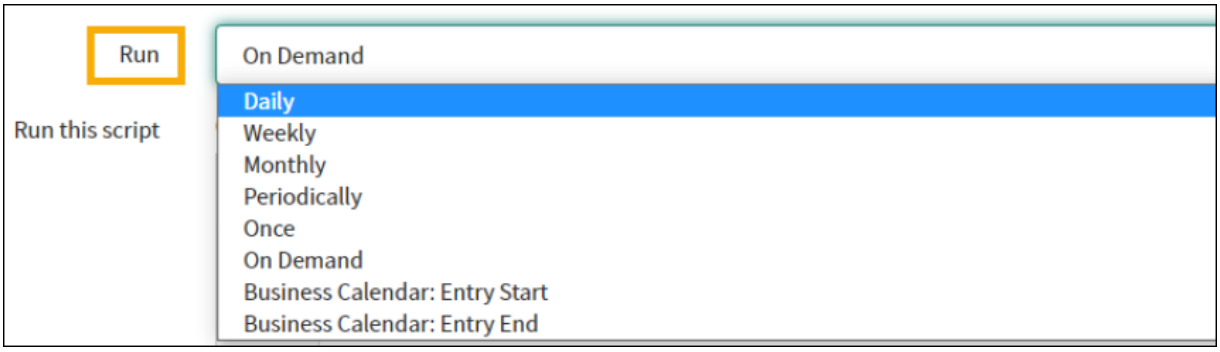
Cause	Solution
Firewall blocker	Ensure that the following port numbers are used: • 31443 - For ServiceNow to AppViewX communication • 443 - For AppViewX to ServiceNow communication
Incorrect Client ID and/or Client Secret	Check if the Client ID and Client Secret entered is correct.

Cause	Solution
Client Secret has expired or is incorrect	Regenerate the Client Secret. **Note:** For more information on regenerating the client secret, refer to Step 11 of the Creating a Service Account in AppViewX section. The Client Secret expires in 180 days (default). However, you can modify the validity period as per your requirement.

Configuring the AppViewX Inventory Sync

You can configure the inventory sync to trigger on a daily, weekly or monthly basis or even on-demand.

1. On the ServiceNow instance, in the **Filter navigator**, search for the Schedule jobs.
2. From the results, displayed, under **System Definition**, click **Scheduled Jobs**.
   The **Scheduled Jobs** page is displayed.
3. On the **Scheduled Jobs** page, search for the **AppViewX Inventory Scheduler** and click the options in the results displayed.
4. On the **AppViewX Inventory Scheduler** page, from the **Run** field, select the frequency of the inventory sync from the options available in the dropdown. For example: **Daily**.

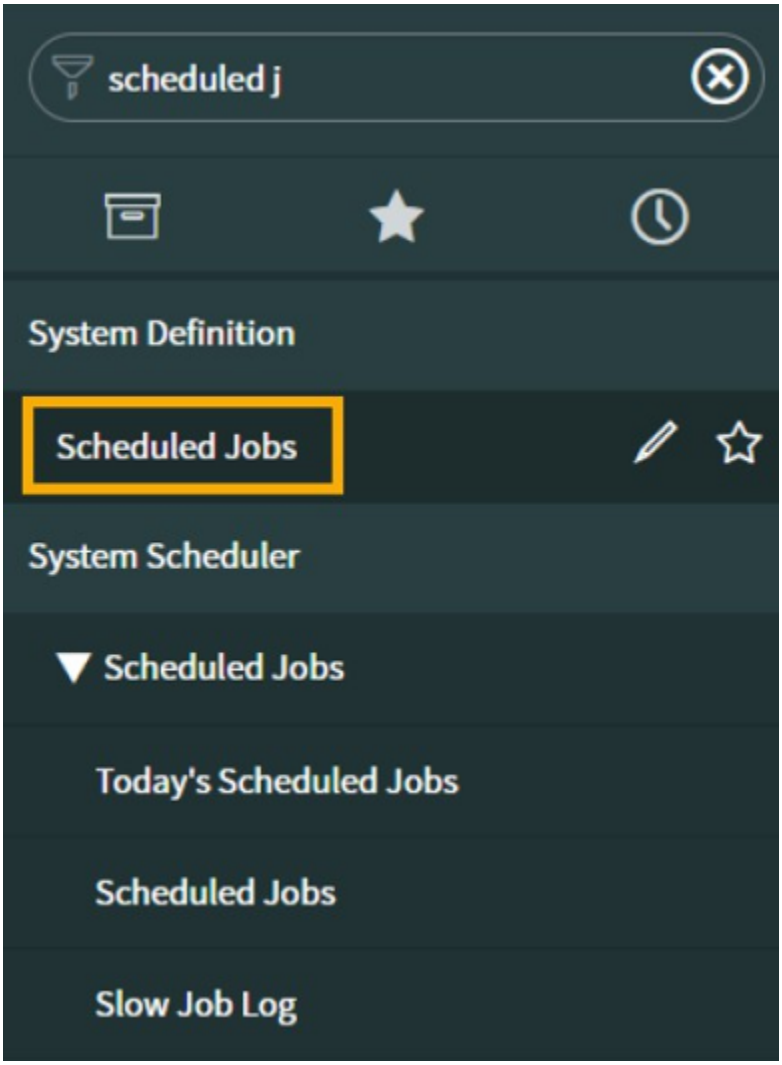


5. In the **Time Zone** field, select the time zone from the options available in the dropdown.
6. Select the **Time** at which you want the inventory sync to take place and click **Update**.
   The inventory sync will be triggered daily at the scheduled time.

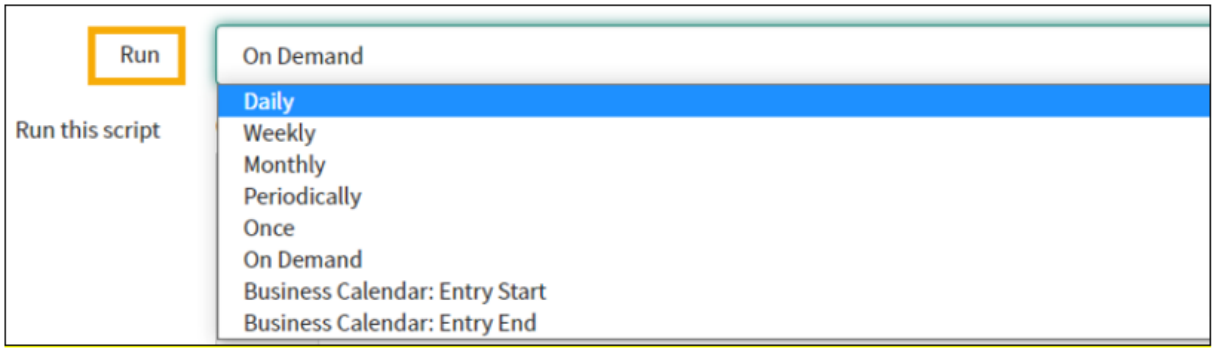
Configuring the AppViewX Log Purging

You can configure the log purging to trigger on a daily, weekly or monthly basis or even on-demand.

1. On the ServiceNow instance, in the **Filter navigator**, search for the Schedule jobs.
2. Fromthe results, displayed, under **SystemDefinition**, click **ScheduledJobs**.
   The **Scheduled Jobs** page is displayed.
3. On the **ScheduledJobs** page, search for the **AppViewX Logs Purging** and click the options in the results displayed.



4. Onthe **AppViewX Logs Purging** page, from the **Run**field, select the frequency of the inventory sync from the options available in the dropdown. For example: **Daily**.



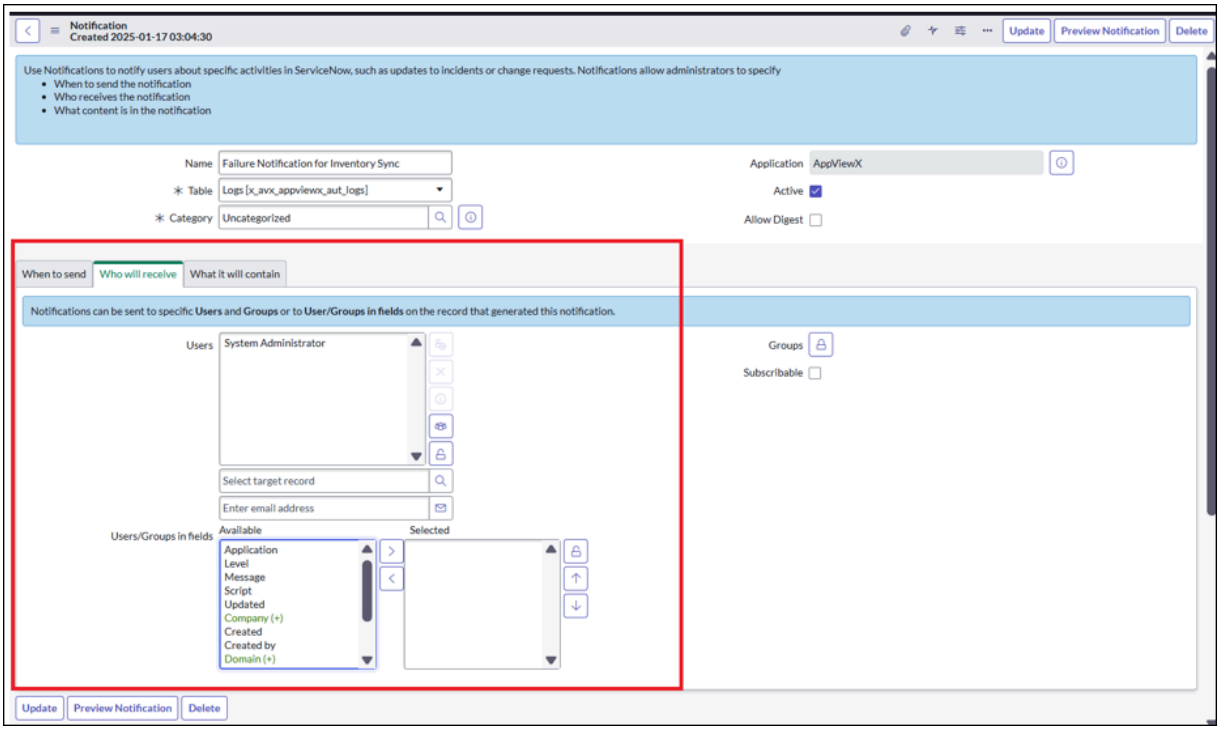
5. In the **Time Zone** field, select the time zone from the options available in the dropdown.
6. Selectthe **Time**at which you want the inventory sync to take place and click **Update**.

   The inventory sync will be triggered daily at the scheduled time.

Configuring Sync Failure Notification

You can configure the Failure Notification for Inventory Sync to trigger.

1. On the ServiceNow instance, in the**Filter navigator**, search for the **Inventory Failure Notification**.
2. On the Inventory Failure Notification click the **“Who will receive”** tab.
3. Select the User or User group names in the tab to receive the failure email notification.



4. Onthe **AppViewX Logs Purging** page, from the **Run**field, select the frequency of the inventory sync from the options available in the dropdown. For example: **Daily**.
5. In the **Time Zone** field, select the time zone from the options available in the dropdown.
6. Selectthe **Time**at which you want the inventory sync to take place and click **Update**.
   The inventory sync will be triggered daily at the scheduled time.

Establishing Communication from AppViewX to ServiceNow

Overview

To ensure that AppViewX is able to communicate with ServiceNow, you must create a User Account on AppViewX. Once created, you must assign roles to the user account for access to the AppViewX plugin features.

Creating User Account on ServiceNow

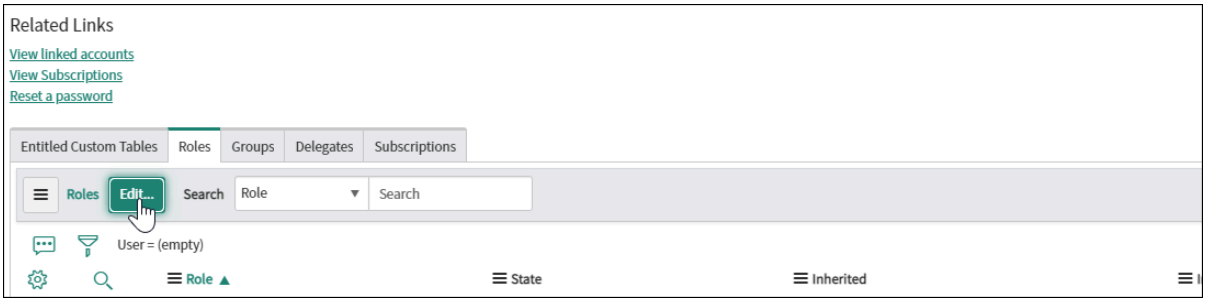
A ServiceNow user account (with assigned roles) enables you to perform the standard functions and update tickets on ServiceNow.

1. On the ServiceNow instance, in the filter navigator, type **Users**.
2. From the results displayed in the left navigation pane, under **Users and Groups**, select **Users**.
3. On the **Users** page that is displayed, click **New**.
4. On the **New Record** page, enter the **User ID** for this new user account.
5. Select the **Web service access only** checkbox.
6. Click **Submit**.
   The new user is created.
7. To set the password for this user account, form the bottom of the screen, click **Set Password**.
8. In the **Set Password** dialog box that pops up on the screen, click **Generate**.
   The password is generated successfully.
9. Click **Save Password** and then click **Close**.

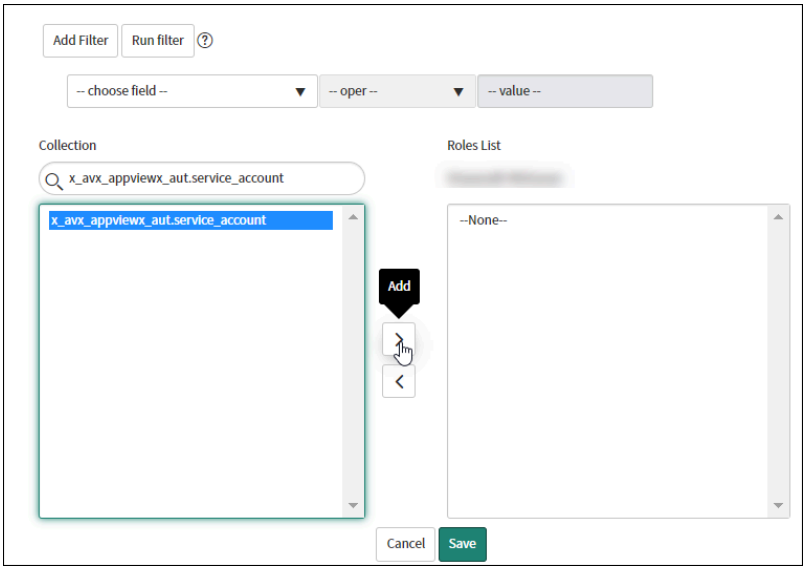
Assigning Roles to the ServiceNow User Account

Once you have created the user account, you must assign roles to this user account.

1. Scroll down on the **User** page and under **Related Links**, click the **Roles** tab.



2. To allow the user account to perform standard ITIL functions, on the **Edit Members** page, search for the **x_avx_appviewx_aut.service_account** role.
3. Select the role and click .



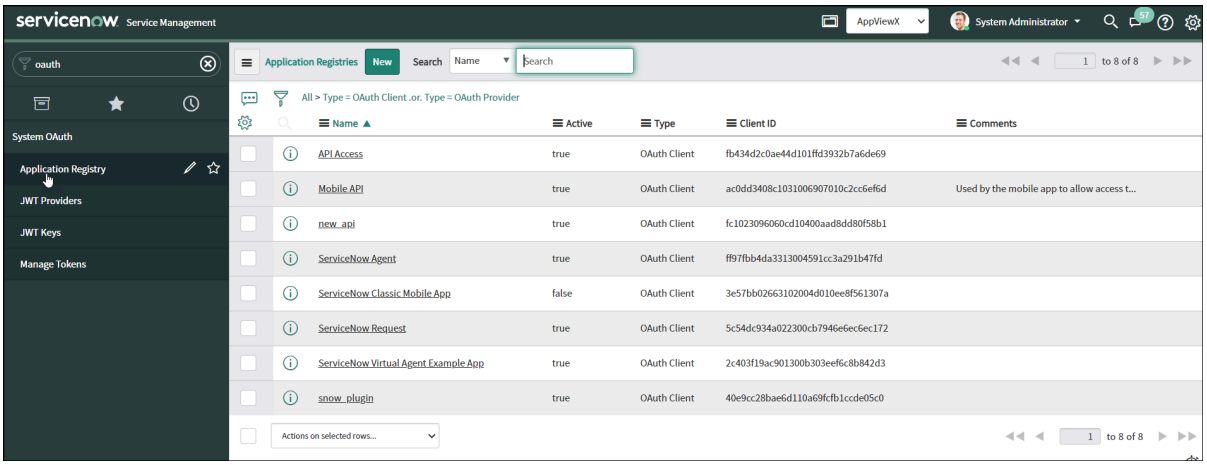
4. Click **Save**.

Generating Client ID and Client Secret on ServiceNow

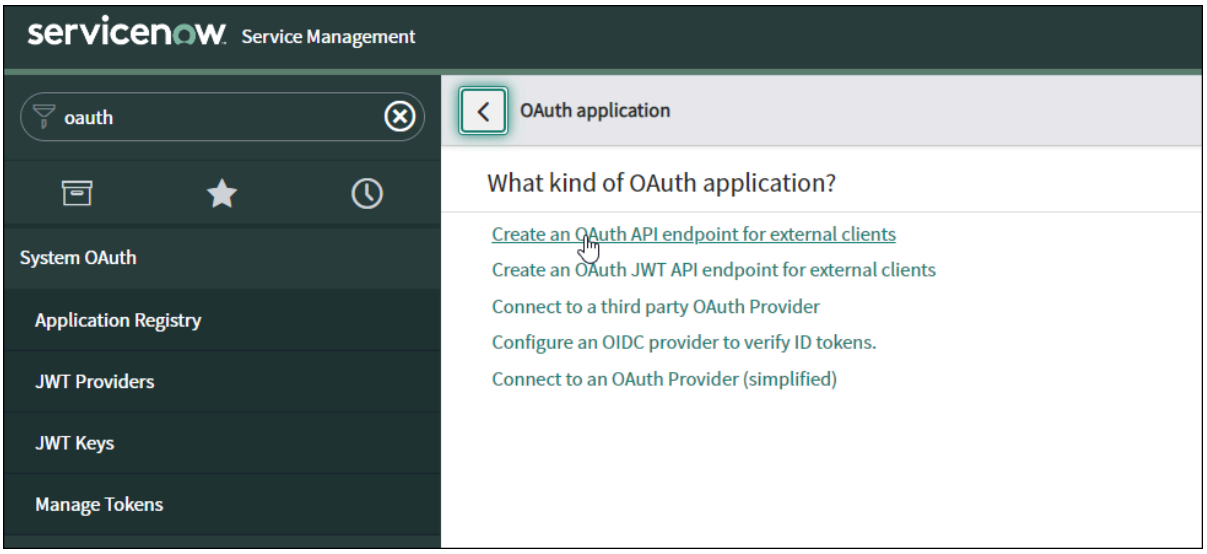
To configure the ServiceNow credentials in AppViewX, you need to first generate the Client ID and Client Secret via oAuth configuration.

Follow these steps for oAuth configuration on ServiceNow:

1. On the ServiceNow instance, in the filter navigator, type **oAuth**.
2. From the results displayed in the left navigation pane, select **Application Registry**.
   The **Application Registries** page is displayed, with the oAuth client names listed.



3. To generate a new Client ID and Client Secret, click **New**.
4. Select the purpose for which you want to generate the oAuth token. For example: Create an oAuth API endpoint for external clients.



5. On the **Application Registries New Record** page, enter a **Name** for the new oAuth application.

> **Note:**
> The Client ID is automatically generated here and will be associated with the client Name that you enter in the Name field. The Client Secret will be generated automatically once the record is submitted.

6. Click **Submit**.
   The new client is added to the Application Registries page.

7. To get the Client ID and Client Secret for this client, on the **Application Registries** page, click on the client Name.
   The **Client ID** and **Client Secret** are displayed.
8. To make the **Client Secret** visible, click .

Configuring the ServiceNow Credentials in AppViewX

The process for configuring the ServiceNow credentials in AppViewX varies between on-prem and SaaS deployments.

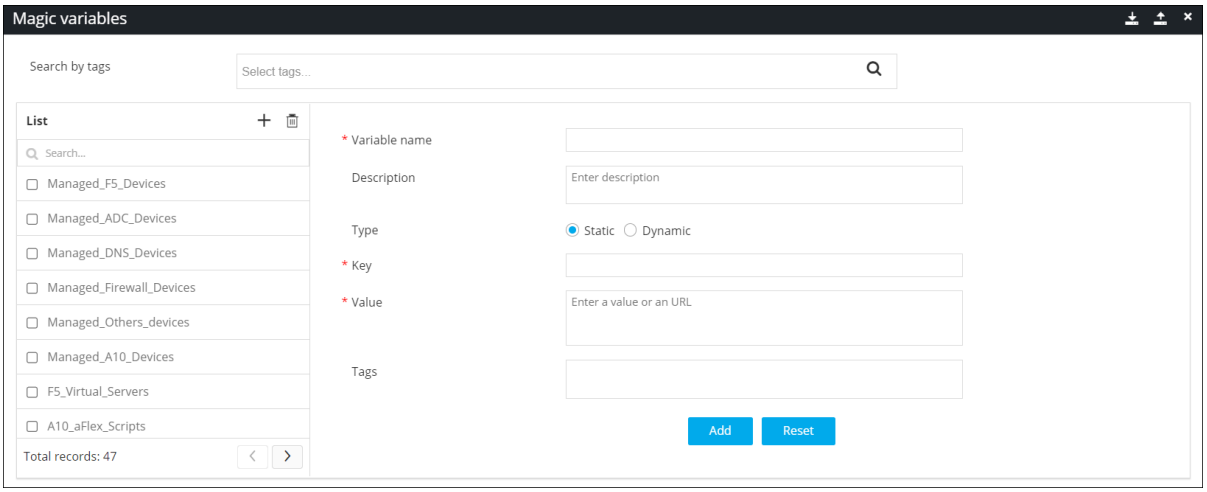
Using Magic Variables (On-prem deployment)

For an on-prem deployment, the Client credentials can be configured in AppViewX using magic variables. Magic variables allow a custom or pre-defined hook to be used as a 'variable' anywhere within the workflow automation process, thus facilitating reusability within workflow.

You can create magic variables for both the Client Id and the Client Secret.

To configure the magic variables:

1. Navigate to the **Workflow** page in AppViewX.
2. On the **Workflow** page, from the navigation pane on the left, click **Magic variables**.
   The **Magic variables** pop-up window is displayed with a list of Magic variables displayed on the left.
3. To configure a new Magic variable, in the **Magic variable** window, click .
4. Enter the required field information to create the magic variable.



The following table describes the field information requested here:

Magic Variable - Field and Description Table

Field	Description
***Variable name**	Enter the name for the magic variable. For example: snow_client_id for the Client ID and snow_client_secret for the Client Secret.
Description	Enter a description for the magic variable.
Type	Select the type of the magic variable as **Static**.
***Key**	Enter the key. **Note:** The value entered here must match the **Variable name**.
***Value**	Enter the **Value** for the magic variable. For example: Enter the Client ID or the Client Secret magic variables respectively. **Note:** For more information on generating the Client ID or the Client Secret in the ServiceNow Application Registry, click here.
Tags	Enter any tags that you want to associate with the magic variable.
**: Mandatory fields*	

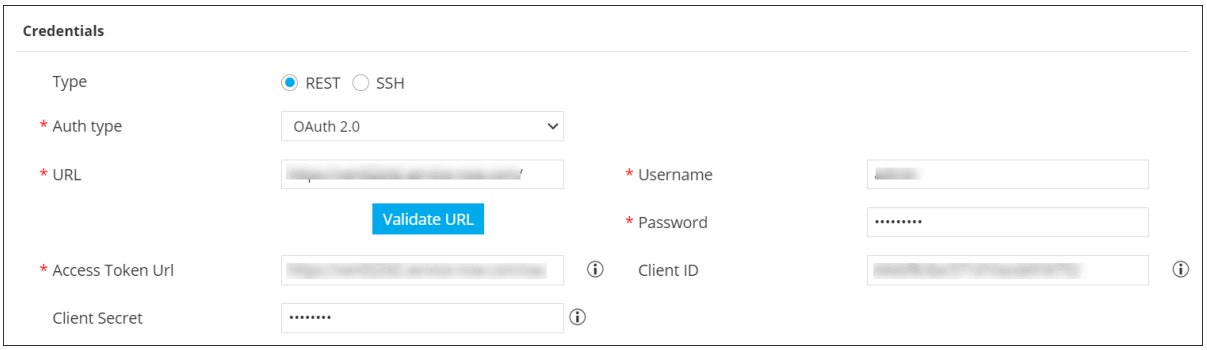
5. Click **Add**.

Vendor Integration (SaaS deployment)

For a SaaS deployment, the Client credentials need to be configured from the vendor integration page.

To access the integration page:

1. Go to the **Integration** page in AppViewX.
2. On the **Integration** page, click on **ServiceNow**.
3. On the **Vendor Configuration** page, under the **Credentials** section, enter or select the field information as shown in image.



The following table describes the field information here:

Credentials - Field and Description Table

Field	Description
Type	Select the type of credentials to be configured as: • REST (default) • SSH
Auth type	Select **oAuth 2.0** as the mode of authentication.
***URL**	Enter the vendor URL (ServiceNow instance) that will be used for communication with ApViewX.
Validate URL	Click this button to validate the URL entered in the previous field.
***Username**	Enter the username.
***Password**	Enter the password.
***Access Token URL**	Enter the Access Token URL. For example: https://<URL>/oauth_token.do
Client ID	Enter the Client ID generated in the Application Registry.
Client Secret	Enter the Client Secret generated in the Application Registry
**: Mandatory fields*	

4. Click **Save**.

Assigning Roles in ServiceNow

Once the user account is created on ServiceNow, you must assign roles to it manually.

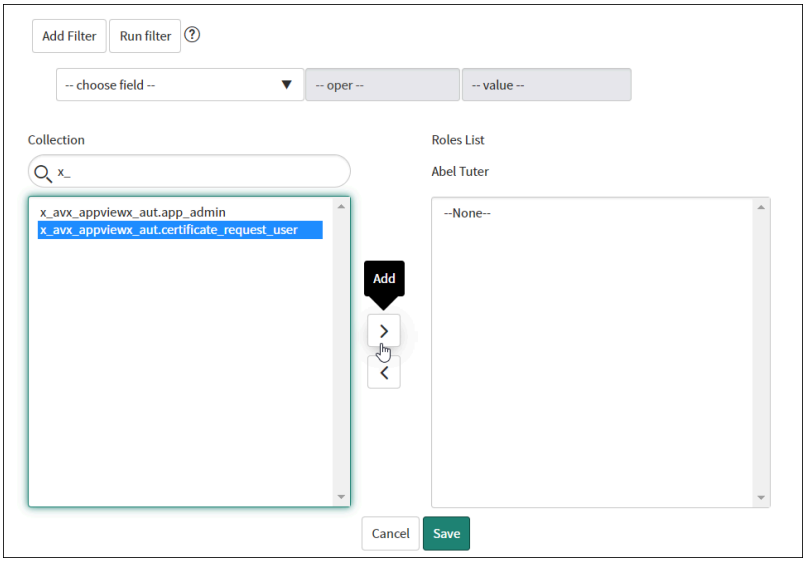
1. On the ServiceNow instance, in the filter navigator, type **Users**.
2. From the results displayed in the navigation pane on the left, select **Users**.
3. On the **Users** page, select a role under the **User ID** column.
4. On the **User** page, scroll down and click the **Roles** tab.
5. To assign role(s) to this user, under the **Roles** tab, click **Edit**.
6. On the **Edit members** page, search for the role that you want to assign to the user by typing in the keywords in the **Collection** search field.

   The following roles are available:

   - **x_avx_appviewx_aut.app_admin:** This is an admin role and has access to all the features of the AppViewX plugin such as configuring AppViewX settings, CLM settings, Service Catalog, logs and so on.
   - **x_avx_appviewx_aut.certificate_request_user:** This role will have access only to the Service Catalog and Certificate Requests pages.
   - **x_avx_appviewx_aut.super_admin:** This is a super admin role and has access to multiple configured domains for the user. It allows configuration of CLM setting records for the domains.

   Note:
   The ServiceNow admin must impersonate as an end user for the enrollment/renewal/revocation of a certificate. Direct enrollment/renewal/revocation of a certificate on behalf of the end user is not permitted.

7. Click the role from the roles displayed and click to assign it to the user.

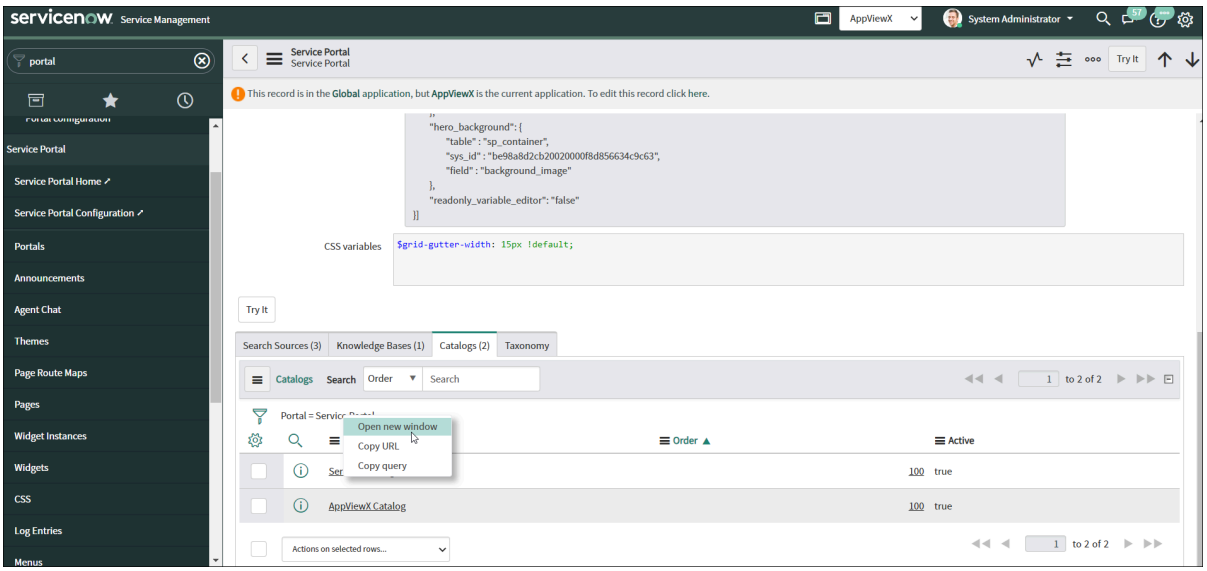


8. To unassign a role from the user, click on the role under the **Roles list** box and click .
9. Click **Save** once the role(s) have been assigned to the user.

Adding AppViewX Catalog to the Service Portal

For the CLM workflows to be available on ServiceNow's Service portal, the AppViewX catalog must be added there.

1. On the ServiceNow instance, in the filter navigator, type **Portal**.
2. From results displayed in the navigation pane on the left, select **Portals**.
3. On the **Service Portal** page, under the **Title** column, click **Service Portal**.
4. On the **Service Portal** page, scroll down and click the **Catalogs** tab.
5. Under the **Catalogs** tab, right click on **Portal=Service Portal** and from the options displayed, click **Open new window**.



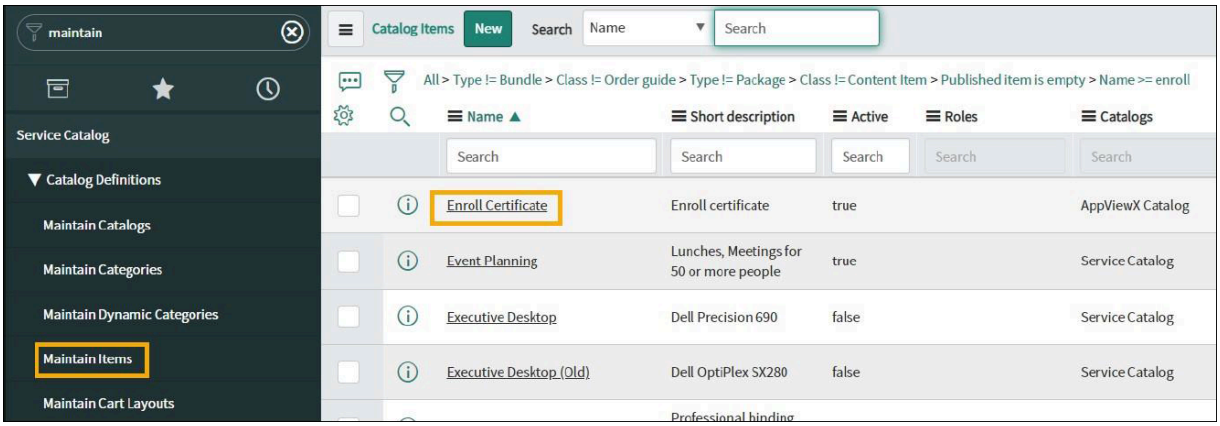
   The **Portal Catalogs** page opens in a new tab.
6. On the **Portal Catalogs** page, from the menu on the top, click **New**.
7. On the **New Record** page that is displayed, click  next to the **Catalog** field.
8. In the pop-up window that is displayed, select **AppViewX Catalog**.
9. Click **Submit**.

   The AppViewX Catalog will be available on the Service Portal page.

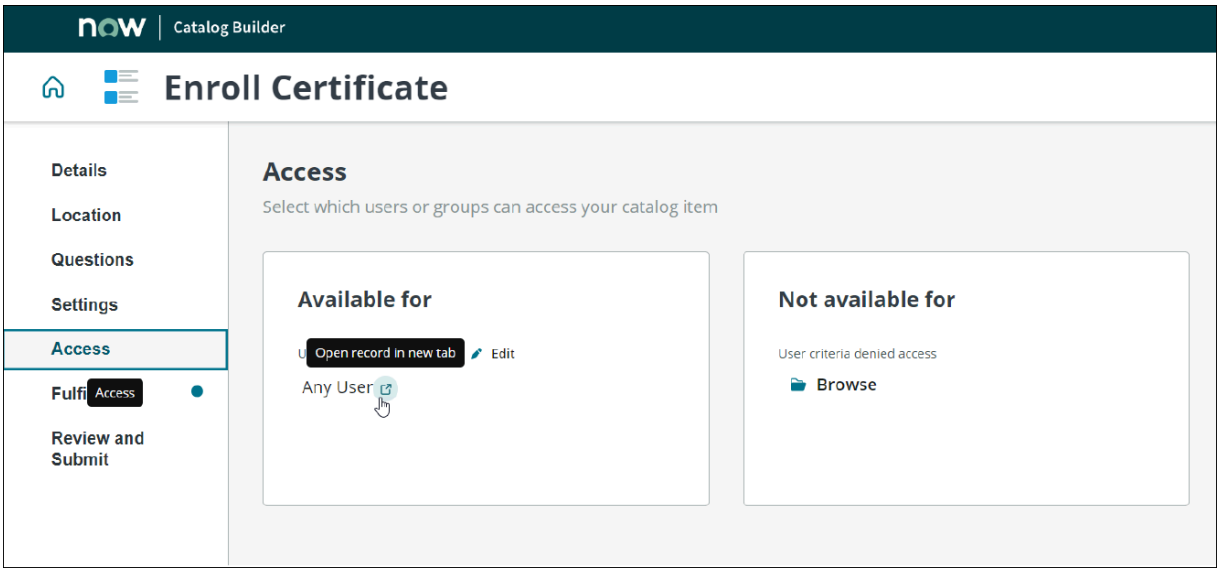
Defining RBAC for Workflows in the Service Portal

Once the AppViewX Catalog is added to the Service Portal, you can define Role Based Access Control (RBAC) to the workflows in the catalog.

1. On the ServiceNow instance, in the Filter Navigator, type **Maintain Items**.
2. Search for the required catalog for which you want to define RBAC. For example: **Enroll Certificate**.

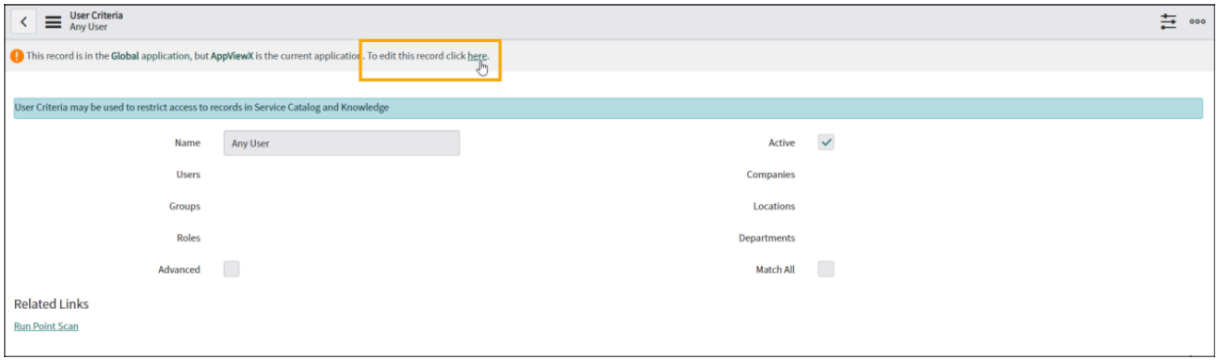


3. On the **Enroll Certificate** page, from the top right corner of the screen, click **Edit in Catalog Builder**. The **Catalog Builder** page for the selected workflow opens in a new tab.
4. On the **Catalog Builder** page for the selected workflow, from the menu on the left, select **Access**.
5. On the **Access** page, to view and modify access for the workflow, under **Available for**, click .



The **User Criteria** page opens in a new tab displaying the users that have access to this workflow.

6. To modify access, from the top of the screen, click **here**.



7. To modify the access for users, user groups, roles and so on click next to the respective field.
8. Once all permissions have been modified, click **Update**.

Configuring CLM Settings

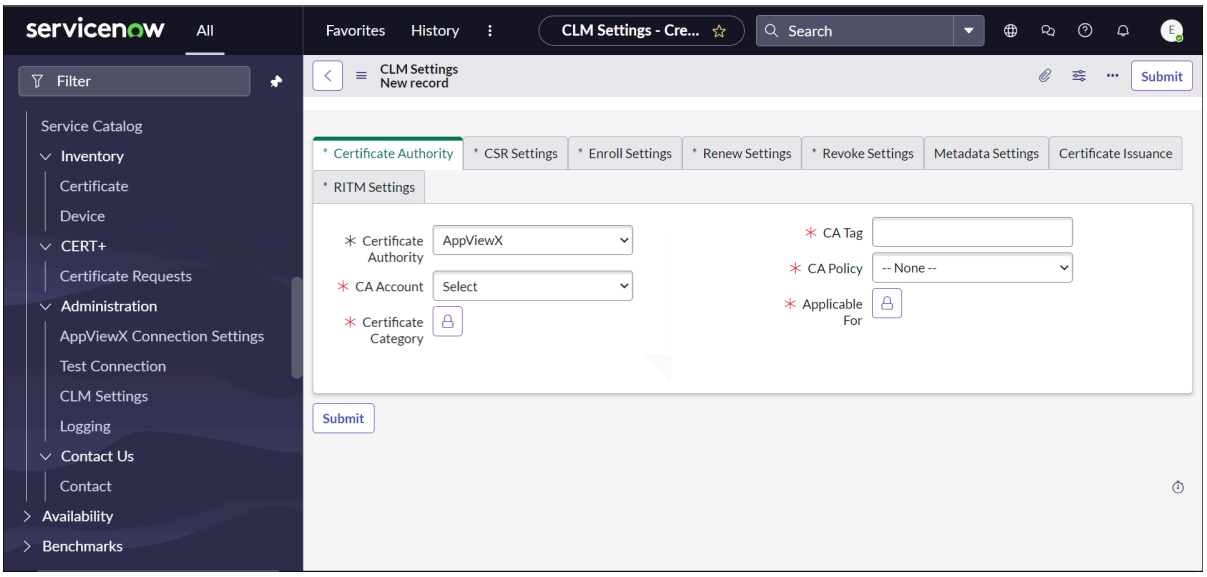
Overview

To enroll, renew or revoke a certificate in AppViewX from ServiceNow, you need to ensure that the CA has been configured in the app. The AppViewX app supports the following certificate authorities:

- AppViewX
- DigiCert
- Microsoft Enterprise
- Entrust
- EJBCA
- Amazon CA
- AppViewX PKIaas
- Globalsign
- Globalsign MSSL
- Trustwave
- Sectigo
- GoDaddy
- Hydrant ID
- SwissSign
- Microsoft Standalone
- AppViewX Native PKI+ CA (PQC - Ready AVX CA)

To configure CLM settings:

1. From the navigation pane on the left, under **Administration**, click **CLM Settings**.
   The **CLM Settings** page is displayed.
2. To configure a new CA in the app, on the **CLM Settings** page, click **New**.
   The **CLM Settings New Record** page is displayed with the **Certificate Authority** tab open by default.



Note:
To add a CA to the app, it must already be configured in AppViewX.

Adding a New CA - Domain Separation Disabled

When adding a new CA you can also configure other settings such as the CSR input method, certificate group selection, method of fetching certificates, certificate issuance method and so on. The options displayed in the input form fields when enrolling, renewing, or revoking certificates(s) will be based on the settings configured here for the CA.

1. On the **CLM Settings New Record** page, under the **Certificate Authority** tab, enter the required field information.
   The following table describes the fields in this section:

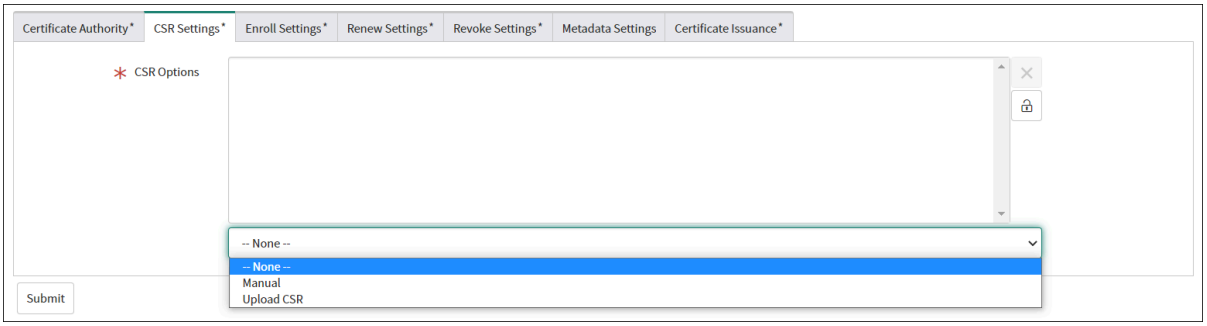
CLM Settings New Record - Enroll Settings

Field	Description
***Certificate Authority**	Select the **Certificate Authority** to be added to the app from the options available in the dropdown.

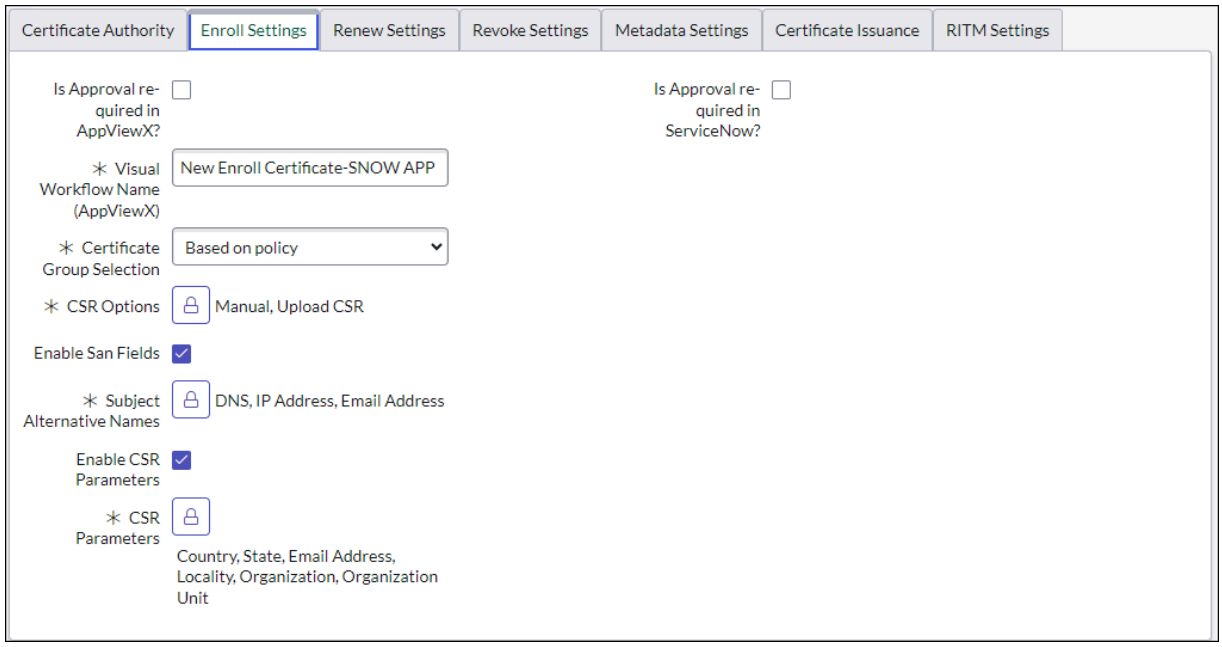
Field	Description
	Note: The values in the dropdown are populated based on the CAs already configured in AppViewX. The following CAs are supported: • DigiCert • Microsoft Enterprise • AppViewX • EJBCA • Entrust • Amazon CA • SwissSign • Hydrant ID • AppViewX Native PKI+ CA (PQC - Ready AVX CA) • Globalsign MSSL • Globalsign • AppViewX PKIaas • Trustwave • Sectigo • GoDaddy
***CA Tag**	Enter a **CA Tag** or a custom label name for your reference. For example: Internal, Dev etc.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** The values in the dropdown are populated based on the Certificate Authority selected.
***CA Policy**	Select the **CA Policy** from the options available in the dropdown. **Note:** The values in the dropdown are populated based on the CA Account selected.
***Certificate Category**	Select the certificate categories for this CA under which users can perform CLM actions. The options available are:

Field	Description
	• Server • Client • Code Signing To view these options, click 🔒. To select/lock a certificate category, select the category and click 🔒. To remove a certificate category, select the category and click ✕.
***Applicable For**	Operations to perform Enroll, Revoke, or Renew.
**: Mandatory fields*	

2. Under **CSR Settings** you can select the CSR input method options that will be displayed in the input form. To view options for adding CSR details, click 🔒. The options available are:
   - **Manual**: This option requires you to manually enter CSR details such as validity unit and value, hash function, key type, bit length and so on in the input form.
   - **Upload CSR**: This option enables you to skip entering the CSR values manually and instead either upload the CSR or paste it in a text box provided in the input form.



3. To select/lock a CSR input method, select the option and click 🔒. To remove a CSR input method, select the option and click ✕.
4. Under the **Enroll Settings** tab, enter the required field information.



The following table describes the fields in this section:

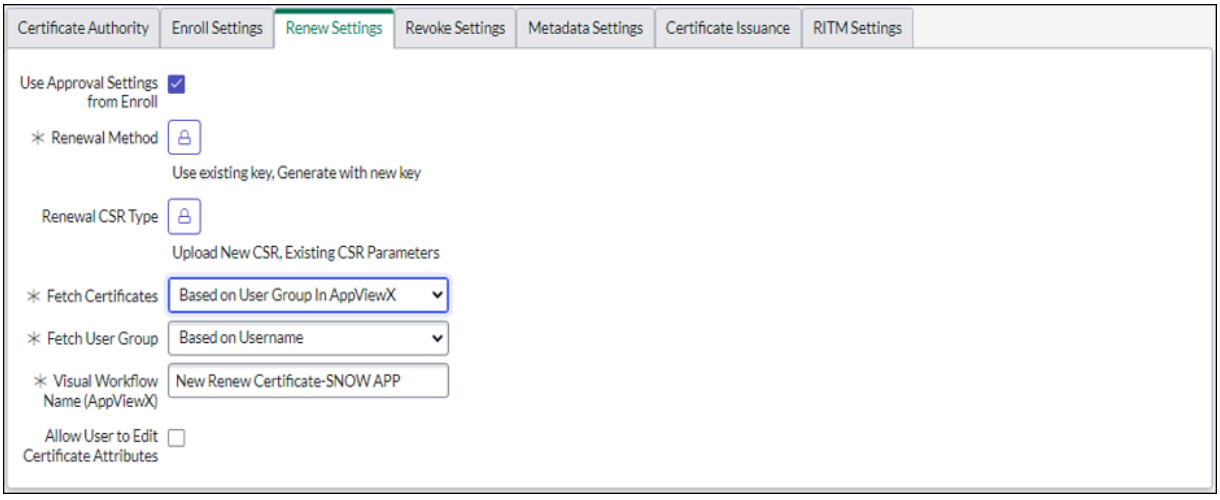
Enroll Settings - Field and Description Table

Field	Description
Is Approval required in AppViewX?	Select this checkbox if you wish to enable approvals in AppViewx.
Number of Levels in AppViewX	Select the levels of approvals required in AppViewX. **Note:** This field is displayed only when the **Is Approval required in AppViewX?** checkbox is selected.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate enrollment in AppViewX.

Field	Description
***Certificate Group Selection**	Select if the certificate group will be selected: • **Based on policy**: If you select this option, the certificate will be added to the certificate group associated with the policy in AppViewX. If there are more than one certificate groups associated with the policy, the certificate will be added to the **Default** certificate group. • **Based on user**: If you select this option, the certificate will be added to the certificate group associated with the user. If the user is mapped to more than one certificate group, the certificate will be added to the **Default** certificate group. **Note:** This method works only if the logged in user in ServiceNow is configured in AppViewX. If the ServiceNow user is not present in AppViewX, certificate group selection will be based on policy.
***CSR Options**	Select the CSR options to be displayed in the form.
Is Approval required in ServiceNow?	Select this checkbox if you wish to enable approvals in ServiceNow.
***Number of Levels in ServiceNow**	Select the levels of approvals required in ServiceNow. **Note:** This field is displayed only when the **Is Approval required in ServiceNow?** checkbox is selected.
***Approver**	Select the Approver from the options available in the dropdown. • Manager • Assignment Group **Note:** This field is displayed only when the **Is Approval required in ServiceNow?** checkbox is selected.

Field	Description
Enable SAN Fields	Select this checkbox to enable the Subject Alternative Fields (SAN).
***Subject Alternative Names**	Select the subject alternative name as DNS. **Note:** This field is displayed only when the **Enable SAN Fields** checkbox is selected.
Enable CSR Parameters	Select this checkbox to enable the CSR parameters.
CSR Parameters	Select the CSR parameters to be displayed in the form. **Note:** This field is displayed only when the **Enable CSR Parameters** checkbox is selected.
**: Mandatory fields*	

5. Under the **Renew Settings** tab, enter the required field information.



The following table describes the fields in this section:

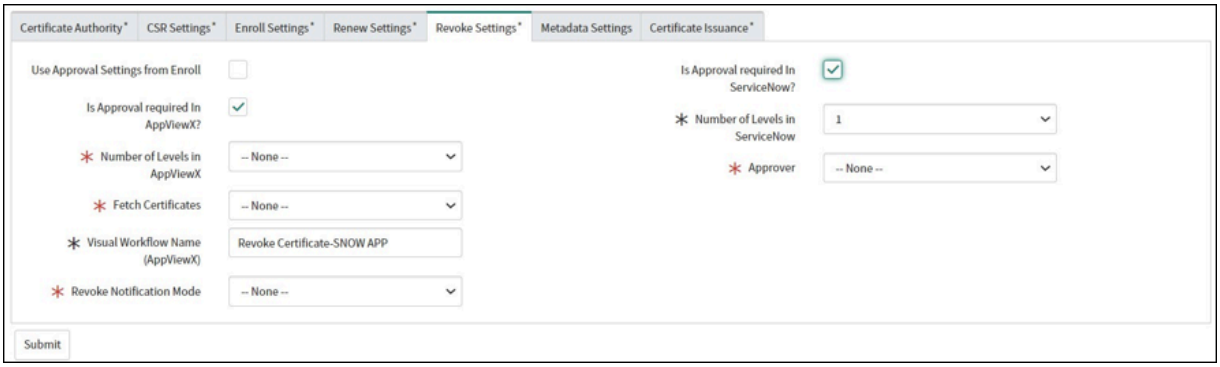
Renew Settings - Field and Description Table

Field	Description
Use Approval Settings from Enroll	Select this checkbox to use the same settings as configured under the **Approval Settings - Enroll** tab.
Is Approval required in AppViewX?	Select this checkbox if you wish to enable approvals in AppViewx. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected.
Number of Levels in AppViewX	Select the levels of approvals required in AppViewX. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in AppViewX?** checkbox is selected.
*** Renewal Method**	Select a certificate renewal method. The options are: • Use exiting key • Generate with new key
*** Renewal CSR Type**	Select a CSR type. The options are: • Upload new CSR • Existing CSR Parameters
***Fetch Certificates**	Select whether the certificates will be fetched: • **Based on user**: This option is useful when the logged in user is not configured in AppViewX. The logged in user's email address is captured as a certificate attribute and all the certificates with this requestor attribute will be fetched. • **Based on usergroup in AppViewX**: This option is useful when the logged in user is configured in AppViewX. The certificates associated with the usergroup that the logged in user is mapped to will be fetched. • **Based on usergroup in ServiceNow**: This option is useful when the logged in user is not configured in AppViewX. The email addresses of all the user groups that

Field	Description
	the logged in user is mapped to are captured as certificate attributes. This allows any user mapped to these user groups to access the certificate for renew/revoke actions.
*** Fetch User Group**	Select a fetch user group: • Based on policy: If you select this option, the certificate will be fetched to the user group associated with the policy in AppViewX. If there are more than one user groups associated with the policy, the certificate will be fetched to the Default user group. • Based on username: If you select this option, the certificate will be fetched to the user group associated with the username. If the user is mapped to more than one user group, the certificate will be fetched to the Default user group.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate renewal in AppViewX.
Is Approval required in ServiceNow?	Select this checkbox if you wish to enable approvals in ServiceNow. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected.
***Number of Levels in ServiceNow**	Select the levels of approvals required in ServiceNow. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected.
***Approver**	Select the Approver from the options available in the dropdown. • Manager • Assignment Group

Field	Description
	Note: This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected.
**: Mandatory fields*	

6. Under the **Revoke Settings** tab, enter the required field information.



The following table describes the fields in this section:

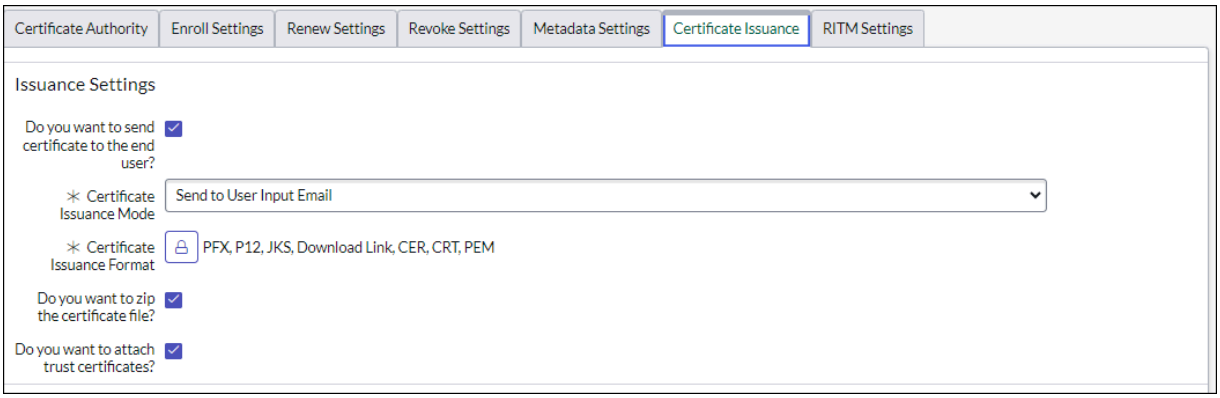
Revoke Settings - Field and Description Table

Field	Description
Use Approval Settings from Enroll	Select this checkbox to use the same settings as configured under the **Approval Settings - Enroll** tab.
Is Approval required in AppViewX?	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected. Select this checkbox if you wish to enable approvals in AppViewX.
Number of Levels in AppViewX	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in AppViewX?** checkbox is selected. Select the levels of approvals required in AppViewX.

Field	Description
***Fetch Certificates**	Select whether the certificates will be fetched: • **Based on user**: This option is useful when the logged in user is not configured in AppViewX. The logged in user's email address is captured as a certificate attribute and all the certificates with this requester attribute will be fetched. • **Based on usergroup in AppViewX**: This option is useful when the logged in user is configured in AppViewX. The certificates associated with the usergroup that the logged in user is mapped to will be fetched. • **Based on usergroup in ServiceNow**: This option is useful when the logged in user is not configured in AppViewX. The email addresses of all the user groups that the logged in user is mapped to are captured as certificate attributes. This allows any user mapped to these user groups to access the certificate for renew/revoke actions.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate revocation in AppViewX.
*** Revoke Notification Mode**	Select a revoke notification mode.
Is Approval required in ServiceNow?	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected. Select this checkbox if you wish to enable approvals in ServiceNow.
***Number of Levels in ServiceNow**	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected. Select the levels of approvals required in ServiceNow.
***Approver**	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected. Select the Approver from the options available in the dropdown. • Manager • Assignment Group
**: Mandatory fields*	

Note:
Information under the **Metadata Settings** tab is pulled directly as per the metadata configured in AppViewX.

7. Under the **Certificate Issuance** tab, in the **Issuance Settings** section, enter the required field information.



The following table describes the fields in this section:

Certificate Issuance - Field and Description Table

Field	Description
Do you want to send the certificate to the end user?	Selecting the checkbox will display the next fields. Select this checkbox to send the certificate to the end user.
***Certificate Issuance Mode**	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the mode of issuing the certificate from the options available in the dropdown. The options available are: • **Send to User Input Email:** The certificate will be sent to the email address entered in the input form. • **Send to Certificate Requester Email:** The certificate will be sent to the requestor's (logged in user) email address. The email address field in the input form will display as a read-only field. • **Attach to RITM Ticket:** The certificate will be attached to the RITM ticket created on ServiceNow.

Field	Description
***Certificate Issuance Format**	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the format in which the certificate file will be issued from the options available in the dropdown. The options available are: • CER • CRT • PFX • Download link
*** Do you want to zip the certificate file?**	Select this checkbox to compress or bundle the certificates into a zip file format.
*** Do you want to attach trusted certificates?**	Select this checkbox to include trusted certificates as attachments.
**: Mandatory fields*	

8. Under the **Certificate Issuance** tab, in the **Push to End Device** section, enter the required field information.
   The following table describes the fields in this section:

Certificate Issuance - Field and Description Table

Field	Description
Push to end device	Selecting the checkbox will display the next fields. Select this checkbox to push the certificate to the end device.
Vendor Name	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. • Unlock the Vendor Name field by clicking  . • Select the vendor(s) from the options available in the dropdown. • To confirm the vendor selection, click  .
Time Zone	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected.

Field	Description
	Select the time zone where the end device is placed.
Assignment Group Selection	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the assignment group to which the certificate will be sent. • Use logged-in user assignment group • Allow user to select assignment group • Use assignment group from CLM settings
**: Mandatory fields*	

9. Under the **RITM Settings** tab, in the **Assignment Group Selection** field, select the assignment group to which the RITM tickets will be assigned as part of the RITM ticket creation.The options available here are:
   • Allow user to select assignment group
   • Use assignment group from CLM settings
   • Use logged-in user assignment group
   • None of the group
10. Under the **RITM Settings** tab, in the **Catalog Task Settings** section, enter or select the required field information.
    The following table describes the fields in this section:

RITM Settings - Field and Description Table

Field	Description
Do you want to create catalog task ticket?	Select this checkbox to create a catalog task ticket. **Note:** Selecting the checkbox will display the next fields.
***Task Priority**	Select the task priority from the following options available in the dropdown: • 1 - Critical • 2 - High • 3 - Moderate • 4 - Low

Field	Description
	Note: This field is displayed only when the **Do you want to create catalog task ticket?** checkbox is selected.
***Task Assigned To**	Enter the user(s) to whom the task will be assigned. For example: **Cert Requestor**. **Note:** This field is displayed only when the **Do you want to create catalog task ticket?** checkbox is selected.
**: Mandatory fields*	

11. Click **Submit**.
    The CA settings are configured in the instance.

Adding a New CA - Domain Separation Enabled

When adding a new CA you can also configure other settings such as the CSR input method, certificate group selection, method of fetching certificates, certificate issuance method and so on. The options displayed in the input form fields when enrolling, renewing, or revoking certificates(s) will be based on the settings configured here for the CA.

1. On the **CLM Settings New Record** page, under the **Certificate Authority** tab, enter the required field information.
   The following table describes the fields in this section:

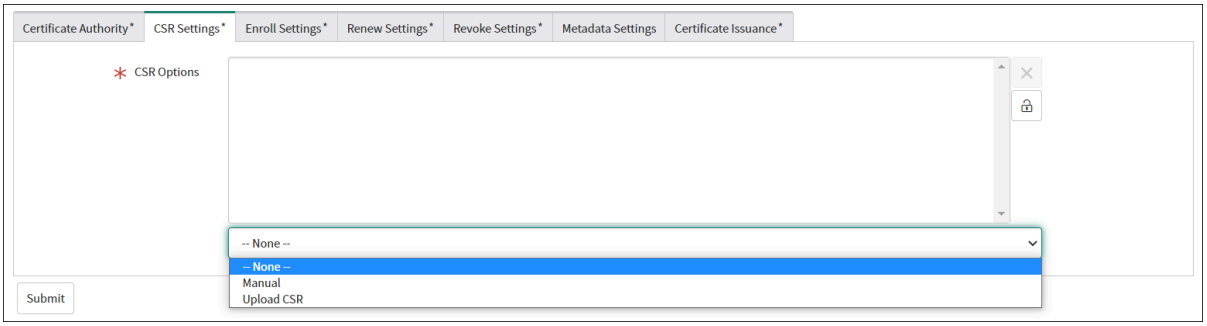
CLM Settings New Record - Enroll Settings

Field	Description
Company	Type in the company and select it from the provided list. Alternatively, you can use the search function by clicking on the search icon to identify the company name.
***Certificate Authority**	Select the **Certificate Authority** to be added to the app from the options available in the dropdown.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Note:
The values in the dropdown are populated based on the CAs already configured in AppViewX.
The following CAs are supported:
• DigiCert
• Microsoft Enterprise
• AppViewX
• EJBCA
• Entrust
• Amazon CA
• SwissSign
• Hydrant ID
• AppViewX Native PKI+ CA (PQC - Ready AVX CA)
• Globalsign MSSL
• Globalsign
• AppViewX PKIaas
• Trustwave
• Sectigo
• GoDaddy</td></tr>
<tr><td>*CA Account</td><td>Select the CA Account from the options available in the dropdown.
Note:
The values in the dropdown are populated based on the Certificate Authority selected.</td></tr>
<tr><td>*Certificate Category</td><td>Select the certificate categories for this CA under which users can perform CLM actions. The options available are:
• Server
• Client
• Code Signing
To view these options, click .
To select/lock a certificate category, select the category and click . To remove a certificate category, select the category and click .</td></tr>
</table>

Field	Description
***CA Tag**	Enter a **CA Tag** or a custom label name for your reference. For example: Internal, Dev etc.
***CA Policy**	Select the **CA Policy** from the options available in the dropdown. **Note:** The values in the dropdown are populated based on the CA Account selected.
***Applicable For**	Operations to perform Enroll, Revoke, or Renew.
**: Mandatory fields*	

2. Under **CSR Settings** you can select the CSR input method options that will be displayed in the input form. To view options for adding CSR details, click . The options available are:
   - **Manual**: This option requires you to manually enter CSR details such as validity unit and value, hash function, key type, bit length and so on in the input form.
   - **Upload CSR**: This option enables you to skip entering the CSR values manually and instead either upload the CSR or paste it in a text box provided in the input form.



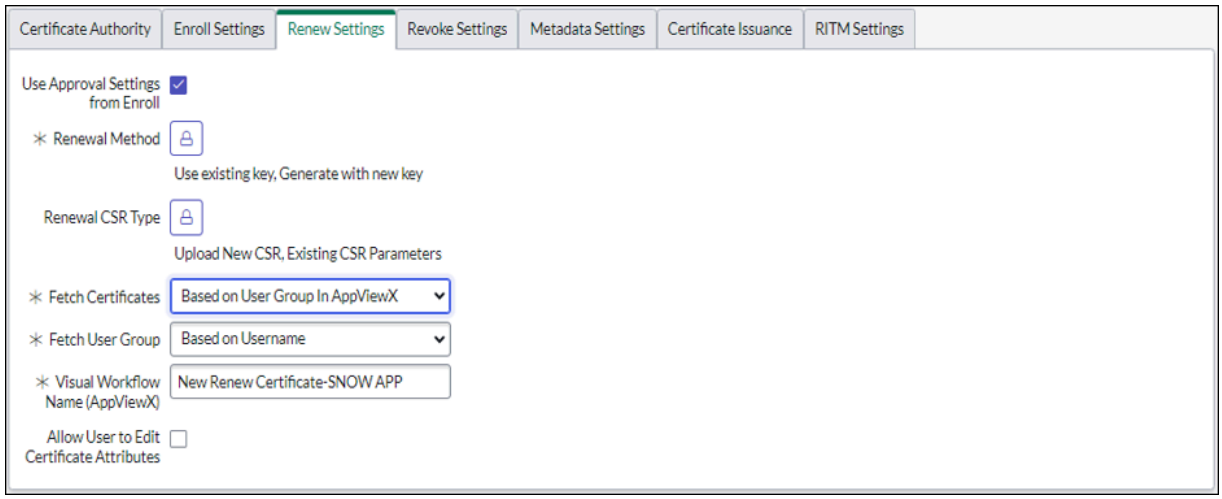
3. To select/lock a CSR input method, select the option and click . To remove a CSR input method, select the option and click .
4. Under the **Enroll Settings** tab, enter the required field information.
   The following table describes the fields in this section:

Enroll Settings - Field and Description Table

Field	Description
Is Approval required in AppViewX?	Select this checkbox if you wish to enable approvals in AppViewx.
Number of Levels in AppViewX	Select the levels of approvals required in AppViewX. **Note:** This field is displayed only when the **Is Approval required in AppViewX?** checkbox is selected.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate enrollment in AppViewX.
***Certificate Group Selection**	Select if the certificate group will be selected: • **Based on policy**: If you select this option, the certificate will be added to the certificate group associated with the policy in AppViewX. If there are more than one certificate groups associated with the policy, the certificate will be added to the **Default** certificate group. • **Based on user**: If you select this option, the certificate will be added to the certificate group associated with the user. If the user is mapped to more than one certificate group, the certificate will be added to the **Default** certificate group. **Note:** This method works only if the logged in user in ServiceNow is configured in AppViewX. If the ServiceNow user is not present in AppViewX, certificate group selection will be based on policy.
***CSR Options**	Select the CSR options to be displayed in the form.
Is Approval required in ServiceNow?	Select this checkbox if you wish to enable approvals in ServiceNow.

Field	Description
***Number of Levels in ServiceNow**	Select the levels of approvals required in ServiceNow. **Note:** This field is displayed only when the **Is Approval required in ServiceNow?** checkbox is selected.
***Approver**	Select the Approver from the options available in the dropdown. • Manager • Assignment Group **Note:** This field is displayed only when the **Is Approval required in ServiceNow?** checkbox is selected.
Enable SAN Fields	Select this checkbox to enable the Subject Alternative Fields (SAN).
***Subject Alternative Names**	Select the subject alternative name as DNS. **Note:** This field is displayed only when the **Enable SAN Fields** checkbox is selected.
Enable CSR Parameters	Select this checkbox to enable the CSR parameters.
CSR Parameters	Select the CSR parameters to be displayed in the form. **Note:** This field is displayed only when the **Enable CSR Parameters** checkbox is selected.
**: Mandatory fields*	

5. Under the **Renew Settings** tab, enter the required field information.



The following table describes the fields in this section:

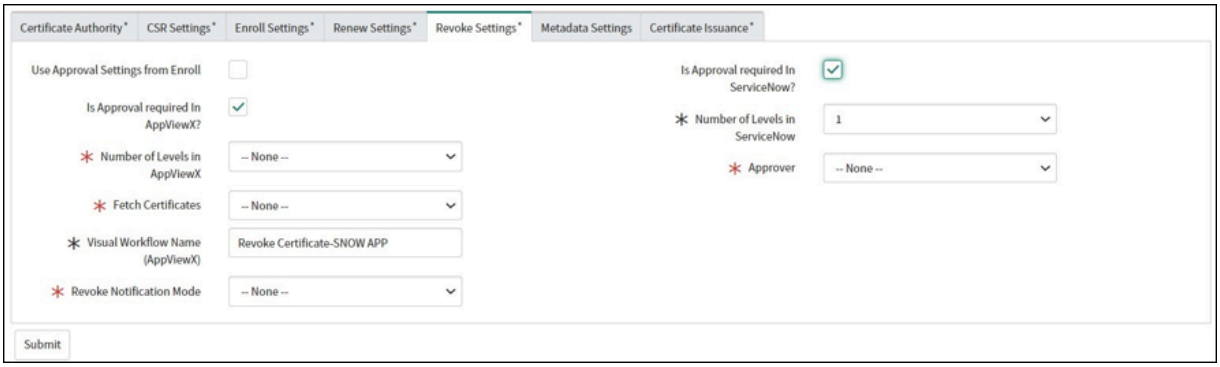
Renew Settings - Field and Description Table

Field	Description
Use Approval Settings from Enroll	Select this checkbox to use the same settings as configured under the **Approval Settings - Enroll** tab.
Is Approval required in AppViewX?	Select this checkbox if you wish to enable approvals in AppViewx. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected.
Number of Levels in AppViewX	Select the levels of approvals required in AppViewX. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in AppViewX?** checkbox is selected.
*** Renewal Method**	Select a certificate renewal method. The options are: • Use exiting key • Generate with new key

Field	Description
*** Renewal CSR Type**	Select a CSR type. The options are: • Upload new CSR • Existing CSR Parameters
***Fetch Certificates**	Select whether the certificates will be fetched: • **Based on user**: This option is useful when the logged in user is not configured in AppViewX. The logged in user's email address is captured as a certificate attribute and all the certificates with this requestor attribute will be fetched. • **Based on usergroup in AppViewX**: This option is useful when the logged in user is configured in AppViewX. The certificates associated with the usergroup that the logged in user is mapped to will be fetched. • **Based on usergroup in ServiceNow**: This option is useful when the logged in user is not configured in AppViewX. The email addresses of all the user groups that the logged in user is mapped to are captured as certificate attributes. This allows any user mapped to these user groups to access the certificate for renew/revoke actions.
*** Fetch User Group**	Select a fetch user group: • Based on policy: If you select this option, the certificate will be fetched to the user group associated with the policy in AppViewX. If there are more than one user groups associated with the policy, the certificate will be fetched to the Default user group. • Based on username: If you select this option, the certificate will be fetched to the user group associated with the username. If the user is mapped to more than one user group, the certificate will be fetched to the Default user group.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate renewal in AppViewX.
Is Approval required in ServiceNow?	Select this checkbox if you wish to enable approvals in ServiceNow.  **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected.

Field	Description
***Number of Levels in ServiceNow**	Select the levels of approvals required in ServiceNow. **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected.
***Approver**	Select the Approver from the options available in the dropdown. • Manager • Assignment Group **Note:** This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected.
**: Mandatory fields*	

6. Under the **Revoke Settings** tab, enter the required field information.



The following table describes the fields in this section:

Revoke Settings - Field and Description Table

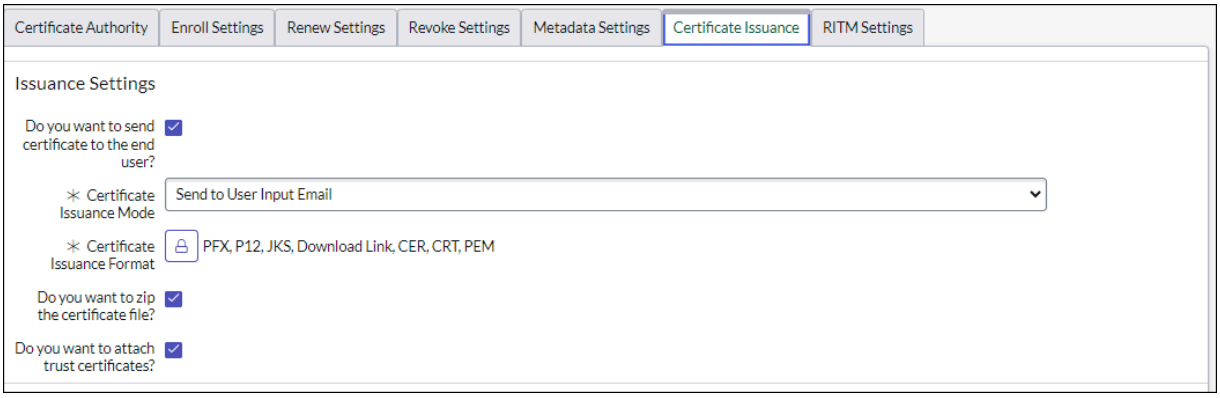
Field	Description
Use Approval	Select this checkbox to use the same settings as configured under the **Approval Settings - Enroll** tab.

Field	Description
Settings from Enroll	
Is Approval required in AppViewX?	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected. Select this checkbox if you wish to enable approvals in AppViewX.
Number of Levels in AppViewX	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in AppViewX?** checkbox is selected. Select the levels of approvals required in AppViewX.
***Fetch Certificates**	Select whether the certificates will be fetched: • **Based on user**: This option is useful when the logged in user is not configured in AppViewX. The logged in user's email address is captured as a certificate attribute and all the certificates with this requester attribute will be fetched. • **Based on usergroup in AppViewX**: This option is useful when the logged in user is configured in AppViewX. The certificates associated with the usergroup that the logged in user is mapped to will be fetched. • **Based on usergroup in ServiceNow**: This option is useful when the logged in user is not configured in AppViewX. The email addresses of all the user groups that the logged in user is mapped to are captured as certificate attributes. This allows any user mapped to these user groups to access the certificate for renew/revoke actions.
***Visual Workflow Name (AppViewX)**	Enter the name of the corresponding Visual Workflow for certificate revocation in AppViewX.
***** **Revoke Notification Mode**	Select a revoke notification mode.
Is Approval required in ServiceNow?	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected. Select this checkbox if you wish to enable approvals in ServiceNow.

Field	Description
***Number of Levels in ServiceNow**	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected. Select the levels of approvals required in ServiceNow.
***Approver**	This field is displayed only when the **Use Approval Settings from Enroll** checkbox is not selected and the **Is Approval required in ServiceNow?** checkbox is selected. Select the Approver from the options available in the dropdown. • Manager • Assignment Group
**: Mandatory fields*	

Note:
Information under the **Metadata Settings** tab is pulled directly as per the metadata configured in AppViewX.

7. Under the **Certificate Issuance** tab, in the **Issuance Settings** section, enter the required field information.



The following table describes the fields in this section:

Certificate Issuance - Field and Description Table

Field	Description
Do you want to send the	Selecting the checkbox will display the next fields. Select this checkbox to send the certificate to the end user.

Field	Description
certificate to the end user?	
***Certificate Issuance Mode**	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the mode of issuing the certificate from the options available in the dropdown. The options available are: • **Send to User Input Email:** The certificate will be sent to the email address entered in the input form. • **Send to Certificate Requester Email:** The certificate will be sent to the requestor's (logged in user) email address. The email address field in the input form will display as a read-only field. • **Attach to RITM Ticket:** The certificate will be attached to the RITM ticket created on ServiceNow.
***Certificate Issuance Format**	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the format in which the certificate file will be issued from the options available in the dropdown. The options available are: • CER • CRT • PFX • Download link
*** Do you want to zip the certificate file?**	Select this checkbox to compress or bundle the certificates into a zip file format.
*** Do you want to attach trusted certificates?**	Select this checkbox to include trusted certificates as attachments.
**: Mandatory fields*	

8. Under the **Certificate Issuance** tab, in the **Push to End Device** section, enter the required field information.
   The following table describes the fields in this section:

Certificate Issuance - Field and Description Table

Field	Description
Push to end device	Selecting the checkbox will display the next fields. Select this checkbox to push the certificate to the end device.
Vendor Name	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. • Unlock the Vendor Name field by clicking . • Select the vendor(s) from the options available in the dropdown. • To confirm the vendor selection, click .
Time Zone	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the time zone where the end device is placed.
Assignment Group Selection	This field is displayed only when the **Do you want to send the certificate to the end user?** checkbox is selected. Select the assignment group to which the certificate will be sent. • Use logged-in user assignment group • Allow user to select assignment group • Use assignment group from CLM settings
**: Mandatory fields*	

9. Under the **RITM Settings** tab, in the **Assignment Group Selection** field, select the assignment group to which the RITM tickets will be assigned as part of the RITM ticket creation.The options available here are:
   • Allow user to select assignment group
   • Use assignment group from CLM settings
   • Use logged-in user assignment group
   • None of the group
10. Under the **RITM Settings** tab, in the **Catalog Task Settings** section, enter or select the required field information.
    The following table describes the fields in this section:

RITM Settings - Field and Description Table

Field	Description
Do you want to create catalog task ticket?	Select this checkbox to create a catalog task ticket. **Note:** Selecting the checkbox will display the next fields.
***Task Priority**	Select the task priority from the following options available in the dropdown: • 1 - Critical • 2 - High • 3 - Moderate • 4 - Low **Note:** This field is displayed only when the **Do you want to create catalog task ticket?** checkbox is selected.
***Task Assigned To**	Enter the user(s) to whom the task will be assigned. For example: **Cert Requestor**. **Note:** This field is displayed only when the **Do you want to create catalog task ticket?** checkbox is selected.
**: Mandatory fields*	

11. Click **Submit**.

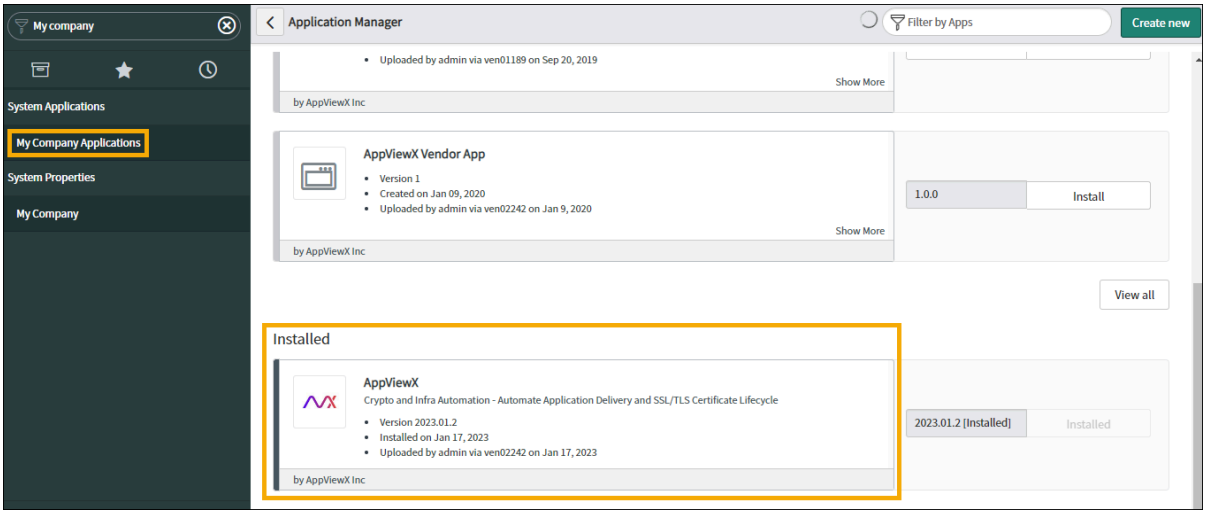
    The CA settings are configured in the instance.

Uninstalling the AppViewX Plugin

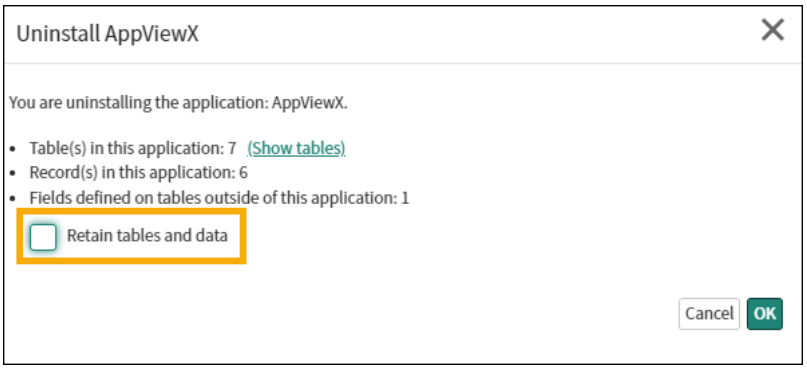
You can uninstall the AppViewX plugin from your ServiceNow instance.

To uninstall the plugin:

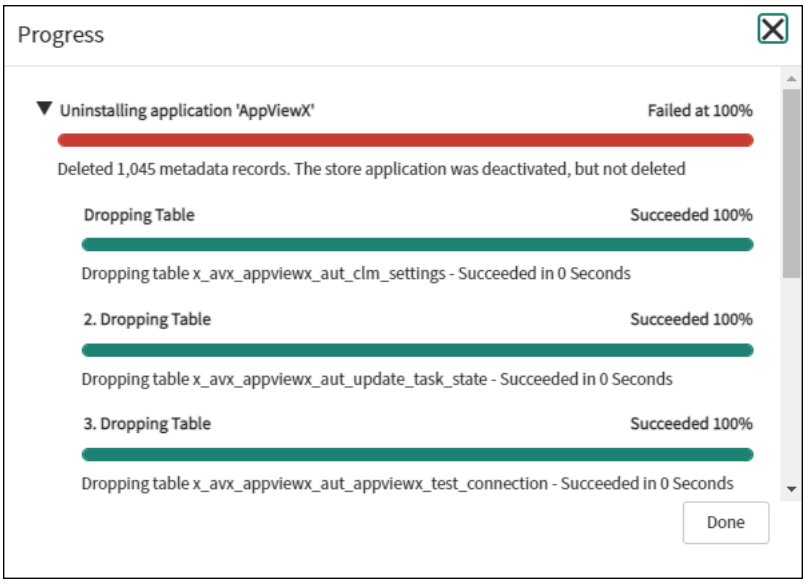
1. On your ServiceNow instance, to search for the applications installed, in the filter navigator type **My Company**.
2. From the search results displayed in the navigation pane on the left, under **System Applications**, select **My Company Applications**.



3. On the **Application Manager** page, select the AppViewX application currently installed.
4. On the application page, scroll down and from the options under **Related Links**, click **Uninstall**.
5. In the **Uninstall AppViewX** pop-up window that is displayed, deselect the **Retain tables and data** checkbox and click **OK**.



6. In the dialog box that is displayed, type **uninstall** in the text box and click **OK**.
   The **Progress** window displays the different stages of the uninstall process and their status.
7. If the **Progress** window displays any error messages, search for the application in your instance.



8. On the Application page, scroll down and click **Remove tables and data**.
9. In the **Remove tables and data** window, click **OK**.
10. In the dialog box that is displayed, type **uninstall** in the text box and click **OK**.

    The AppViewX plugin will be uninstalled.

Chapter 2: AppViewX on ServiceNow Store User Guide

This guide describes the AppViewX plugin available on ServiceNow's App store. It provides detailed information on how to perform various CLM operations such as enrolling, renewing, and revoking certificates.

AppViewX on ServiceNow Store

Prerequisites

Version Support

AppViewXplugin 2025.5.1 version is compatible with the ServiceNow Yokohama version.

AppViewX: 2020.3.0 FP 10 (on-prem) onwards and 2022.1.0 (SaaS)

ServiceNow: Tokyo, San Diego, Utah, Vancouver, Washington DC, Xanadu, and Yokohama

Version Support Timeline

Version	AppViewX Support	ServiceNow Release	AppViewX On-Prem	AppViewX SaaS
San Diego	Yes	Q2-2022	From 2020.3.0 FP 10	From v22.1
Tokyo	Yes	Q4-2022	From 2020.3.0 FP 10	From v22.1
Utah	Yes	Q2-2023	From 2020.3.0 FP 10	From v22.1
Vancouver	Yes	Q4-2023	From 2020.3.0 FP 10	From v22.1
Washington	Yes	Q2-2024	From 2020.3.0 FP 10	From 2020.3.0 FP 10
Xanadu	Yes	Q4-2024	From 2020.3.0 FP 10	From v22.1
Yokohama	Yes	Q1-2025	From 2020.3.0 FP 10	From v22.1

Environment Dependency

- AppViewX gateway port should be reachable from the ServiceNow instance.
- To connect from ServiceNow, it is recommended to have a service account for AppViewX.
- AppViewX needs to be exposed on the internet to allow communication between AppViewX and ServiceNow.
- If AppViewX has been installed on-prem, then a MID server needs to be installed to allow AppViewX communication.

Note:
For more information on downloading and installing the MID server, click here.

Modules Required on Service Now

- Service Catalog
- Request Item
- Catalog Tasks
- Service Portal

Salient Features

Certificate Automation

- Submit new certificate request across Certificate Authorities.
- Submit requests for certificate renewal and revocation.
- Supported CAs - Microsoft Enterprise, DigiCert, AppViewX, Entrust, EJBCA, Amazon CA, AppViewX PKIaas (*PQC-Ready AVX CA is not supported*), Globalsign, Globalsign MSSL, Trustwave, Sectigo, GoDaddy, Hydrant ID, Microsoft Standalone CA, SwissSign, and AppViewX Native PKI+ CA (PQC - Ready AVX CA)
- Manage approvals on ServiceNow.
- Manage approvals on AppViewX.
- Check for request status and details.

Service Catalog

- CLM automation - Enroll, Renew, and Revoke SSL Certificates

MID Server Support

- Facilitate communication between a ServiceNow instance and AppViewX when AppViewX is not exposed on the internet.

Installing and Configuring the AppViewX Plugin

For information on installing and configuring the AppViewX plugin on ServiceNow, refer to the AppViewX on ServiceNow Installation and Configuration Guide.

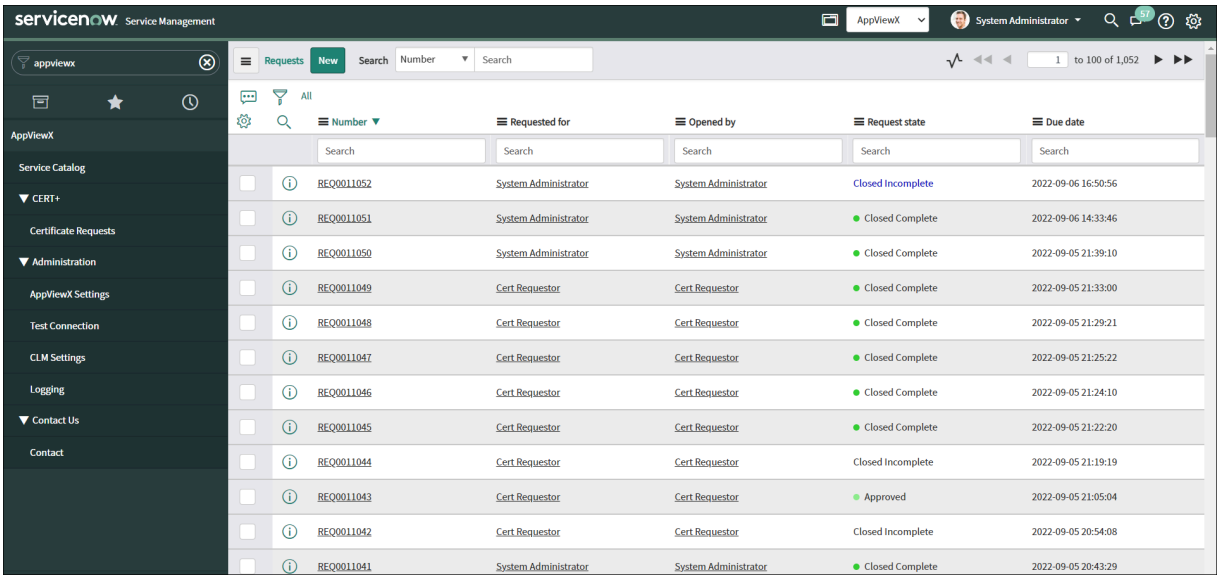
Configuring CLM Settings

For information on configuring the CLM Settings and adding a new Certificate Authority, refer to the Adding a New CA section in the **AppViewX on ServiceNow Installation and Configuration Guide**.

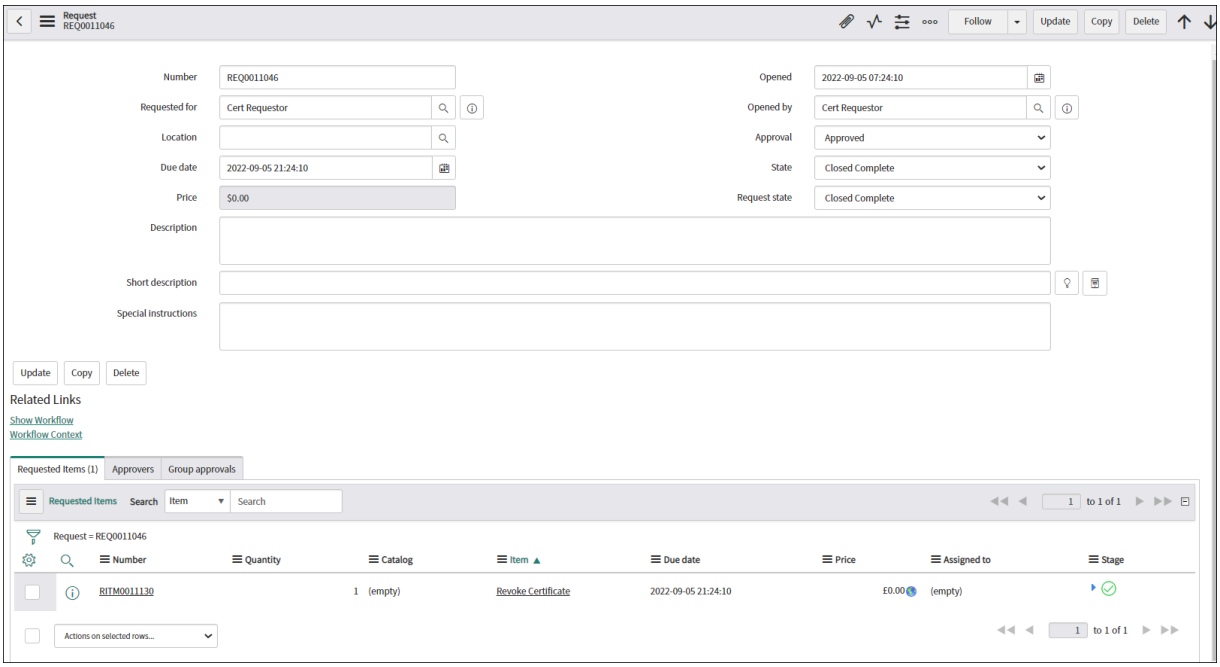
Viewing Certificate Requests

To view the logs for certificate requests from the plugin:

1. From the navigation pane on the left, under **CERT+**, click **Certificate Requests**.
   The **Requests** page is displayed with a list of certificate requests with their status.



2. For detailed information about a particular request, click on the request **Number**.
   The **Request** page is displayed with detailed information such as the associated RITM number, type of request, and status.



3. Click the **RITM number**.

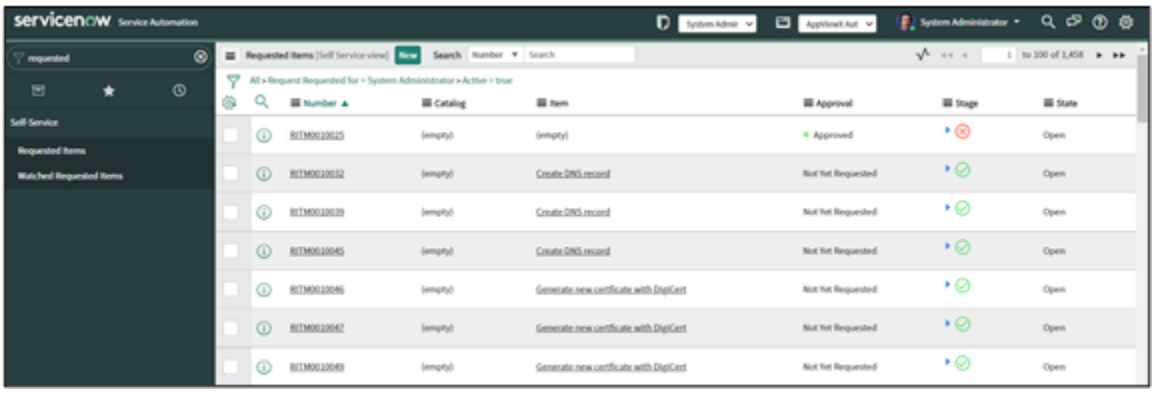
   The Requested Item page is displayed with detailed information about the certificate request such as Request Details, Certificate Information, and AppViewX Response. You can use the Request ID to view the request log in AppViewX on the Workflow Request page.

Service Catalog

Overview

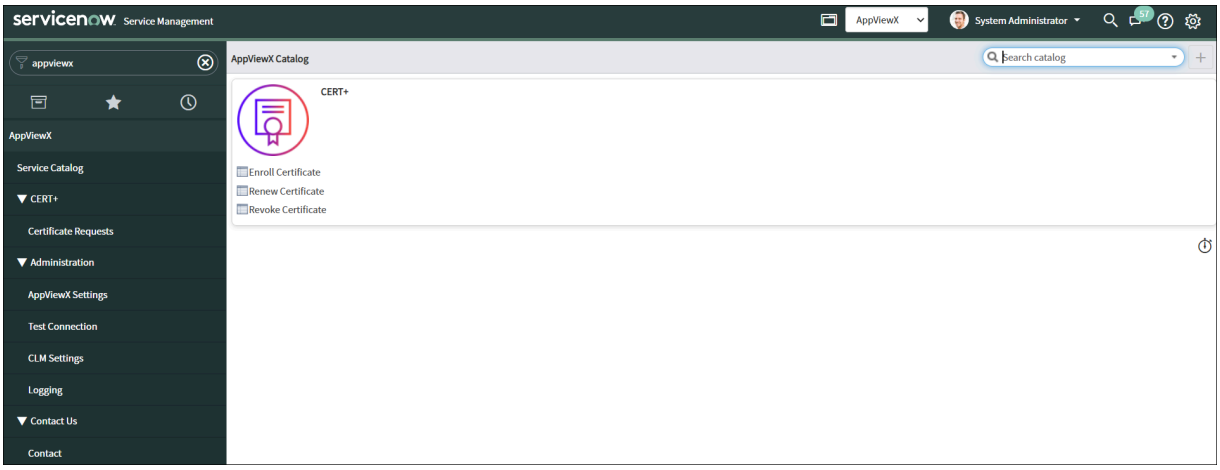
The Service Catalog allows you to quickly self-service automation workflow requests for Certificate Lifecycle Management.

All requests are created under RITM (**Requested Items**) under **Self Service view**.



Accessing the Service Catalog

1. From the navigation pane on the left, click **Service Catalog**.
   The **Catalogs** page is displayed.
2. On the **Catalogs** page, click **AppViewX Catalog**.
   The **AppViewX Catalog** page is displayed with the following certificate request items:
   - Enroll Certificate
   - Renew Certificate
   - Revoke Certificate



3. To request for a certificate service, click on the required catalog item.
4. Enter or select the field information in the input form.
5. To trigger the corresponding workflow in AppViewX, click **Order Now**.

Self-Servicing a Certificate Enrollment Workflow Request

To self-service a workflow request for enrolling a certificate from the AppViewX Catalog:

1. On the **AppViewX Catalog** page, click **Enroll Certificate**.
   The **Enroll Certificate** input form page is displayed.

   The following table describes the field information requested on this page:

Enroll Certificate - Field and Description Table

Category	Field	Description
Request Details	**Created By**	This is a read-only field and is auto-populated based on the login information.

Category	Field	Description
		Displays details of the request creator.
	Certificate Request Type	This is a read-only field and is auto-populated based on the certificate request. Displays the type of certificate request.
CA Details	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Policy	This is a read-only field and is auto-populated based on the **CA Tag** selected. Displays the certificate policy associated with the selected CA.
	***CSR Input Method**	Select if the method of submitting CSR is: • Manual • Upload CSR
	***Certificate Category**	This field is displayed only when the **CSR Input Method** is selected. Select the category of certificate from the options available in the dropdown: • Server • Client • Code Signing
AppViewX Response	**Request ID**	This is a read-only field and the value is fetched from AppViewX's Request module. Displays the Request ID of the workflow executed in AppViewX.

Category	Field	Description
	AppViewX Response	Displays the AppViewX Response.
**: Mandatory fields*		

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

CSR Input Method - Manual

If you select the CSR input method as **Manual**:

1. In the **CSR Parameters** section, enter the required field information.

   The following table describes the fields in this section:

   CSR Parameters - Field and Description Table

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Do you want to add SAN Values?	Select the appropriate checkbox for adding SAN Values. • Add DNS Values • Add IP Address
DNS	Enter the DNS value. **Note:** This field is displayed only if you select the Add DNS Values checkbox.
IP Address	Enter the IP Address.

Field	Description
	Note: This field is displayed only if you select the Add IP Address checkbox.
***Organization**	Enter the name of the **Organization** with which the certificate will be associated.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
**: Mandatory fields*	

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

CSR Input Method - Upload CSR

If you select the CSR input method as **Upload CSR**:

1. In the **CSR Parameters** section, enter the required field information.

   The following table describes the fields in this section:

   CSR Parameters - Field and Description Table

Field	Description
***CSR Upload Option**	Select the option for uploading the CSR from the options available in the dropdown: • Paste CSR • File Upload
***Paste CSR**	Paste the CSR in this field.

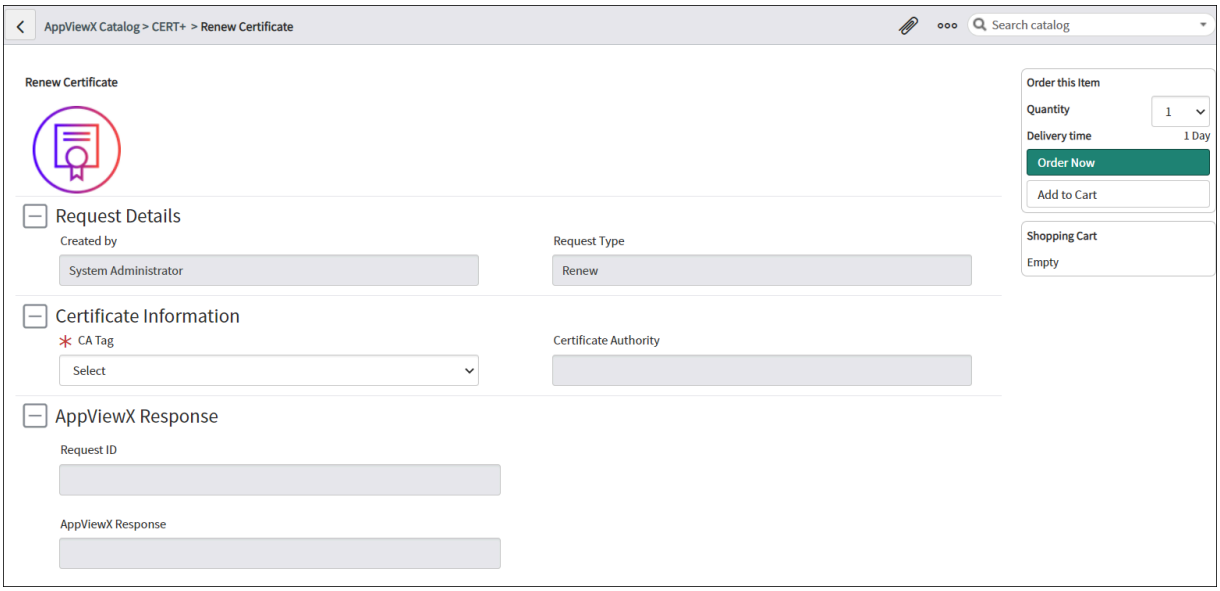
Field	Description
	Note: This field is displayed only when you select the **Paste CSR** option in the **CSR Upload Option** field. The CSR file is validated for file type and size and a warning is issued if validation fails.
***Upload CSR**	To upload the CSR, click **Click to add**. **Note:** This field is displayed only when you select the **Upload CSR** options in the **CSR Upload Option** field. The CSR file is validated for file type and size and a warning is issued if validation fails.
***Validity Unit**	This field is displayed only when the CSR is pasted or uploaded. Select the validity unit as: • Months • Days • Years
***Validity Value**	This field is displayed only when the CSR is pasted or uploaded. Select the validity value for the certificate as per the validity unit selected.
**: Mandatory fields*	

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

Self-Servicing a Certificate Renewal Workflow Request

To self-service a workflow request for renewing a certificate from the AppViewX Catalog.

1. On the **AppViewX Catalog** page, click **Renew Certificate**.
   The **Renew Certificate** input form page is displayed.



The following table describes the field information requested on this page:

Renew Certificate - Field and Description Table

Category	Field	Description
Request Details	**Created By**	Displays details of the request creator. **Note:** This is a read only field and is auto-populated based on the login information.
	Certificate Request Type	Displays the type of certificate request. **Note:** This is a read-only field and is auto-populated based on the certificate request.
Certificate Information	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Authority	Displays the certificate authority with which the CA tag is associated.

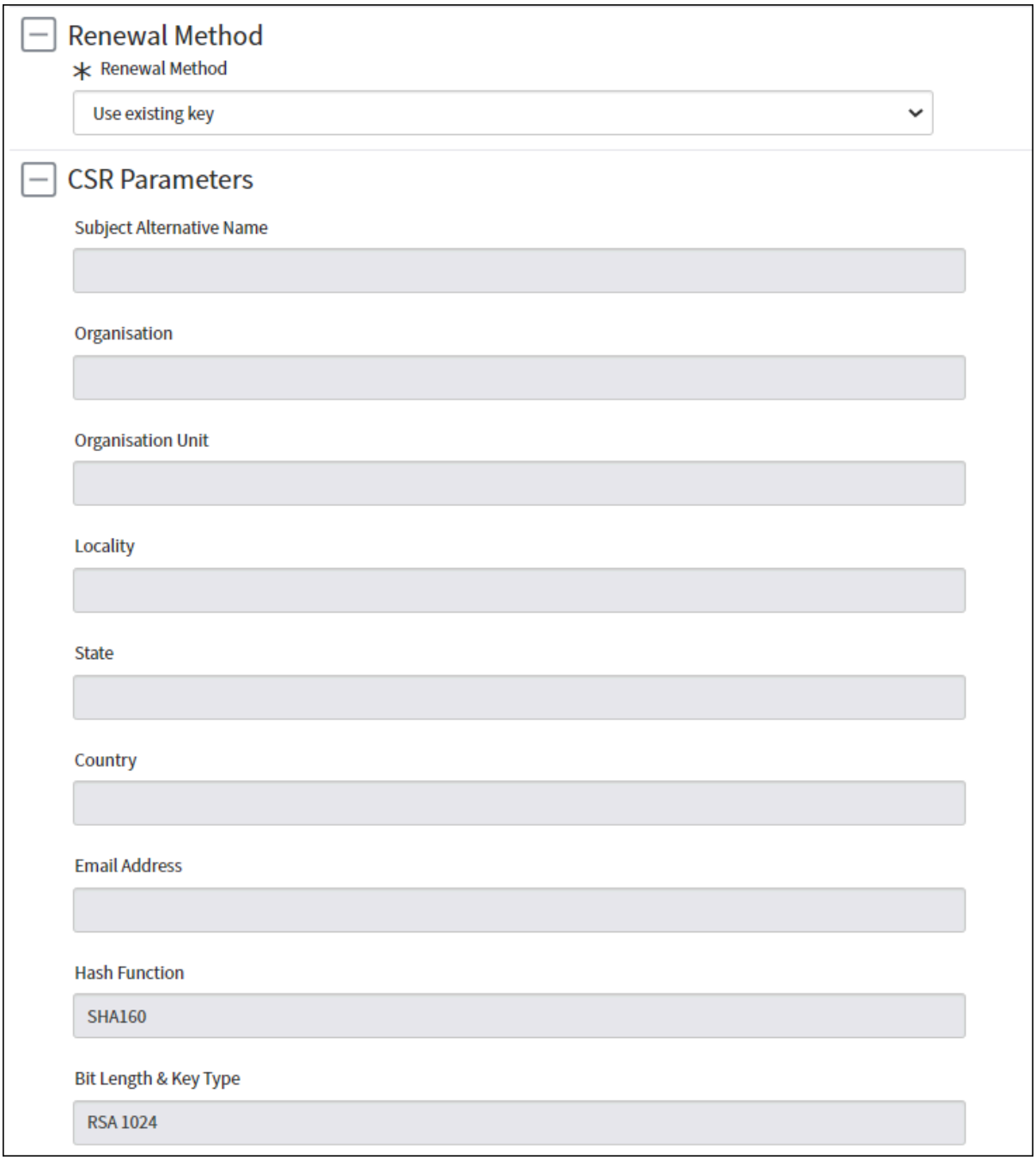
Category	Field	Description
		Note: This is a read-only field and is auto-populated based on the **CA Tag** selected.
	***Certificates**	Select the certificate you wish to renew from the options available in the dropdown. **Note:** The values in this field are fetched from AppViewX based on the **CA Tag** selected and **Certificate Category** configured in **CLM Settings**.
	Common Name	Displays the **Common Name** for the selected certificate. **Note:** This is a read-only field and is auto-populated based on the certificate selected.
	Serial Number	Displays the **Serial Number** for the selected certificate. **Note:** This is a read-only field and is auto-populated based on the certificate selected.
Renewal Method	**Renewal Method**	Select the method for renewing the certificate. The options available are: • Use existing key • Generate with new key
AppViewX Response	**Request ID**	Displays the Request ID of the workflow executed in AppViewX. **Note:** This is a read-only field and the value is fetched from AppViewX's Request module.

Category	Field	Description
	AppViewX Response	Displays the AppViewX Response.
**: Mandatory fields*		

2. To submit the workflow request for renewing the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

Certificate Renewal using Existing Key

If you renew the selected certificate using the existing key, the CSR parameters are automatically fetched and displayed in the **CSR Parameters** section.



1. To submit the workflow request for renewing the certificate, from the right side of the screen, click **Order Now**.

   The **Order Status** page is displayed with details of the certificate request and the request number.
2. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

Certificate Renewal with a New Key

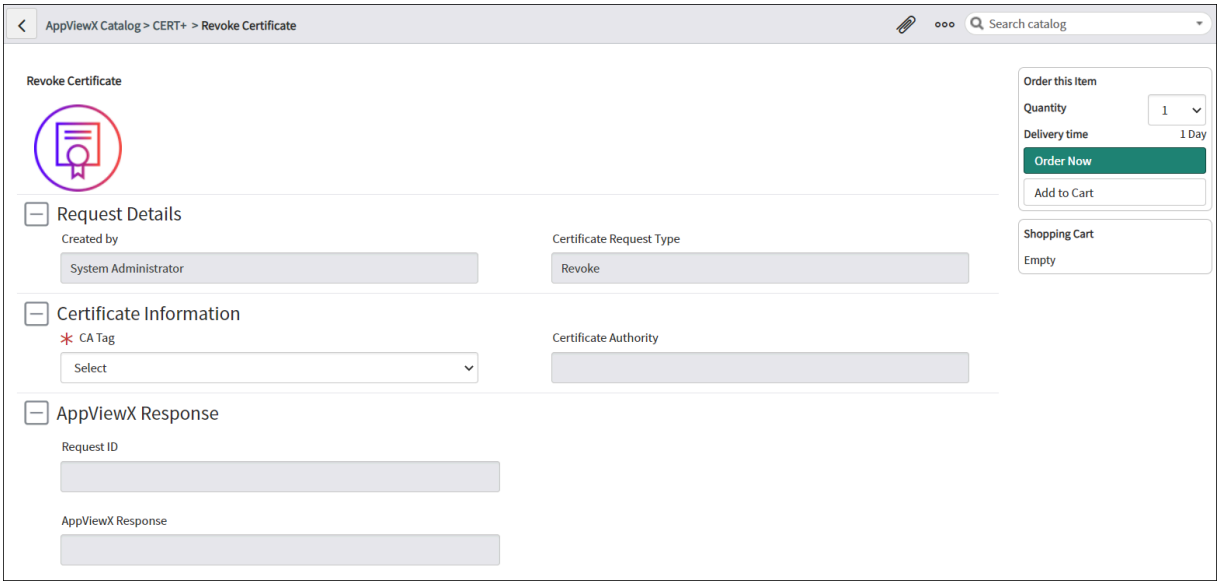
If you renew the selected certificate by generating a new key:

1. In the **CSR Type** field, select if you wish to use the existing CSR or upload a new CSR.
2. If you select the CSR Type as **Existing CSR**, the CSR parameters are automatically fetched and displayed in the **CSR Parameters** section.
3. If you select the CSR Type as **Upload New CSR**, in the **CSR Upload Option** field, select the required option.
   - **Paste CSR**: Paste the CSR in the Paste CSR field.
   - **File Upload**: Click to add the .csr file.
4. To submit the workflow request for renewing the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
5. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

Self-Servicing a Certificate Revocation Workflow Request

To self-service a workflow request for revoking a certificate from the AppViewX Catalog:

1. On the **AppViewX Catalog** page, click **Revoke Certificate**.
   The **Revoke Certificate** input form page is displayed.



   The following table describes the field information requested on this page:

Revoke Certificate - Field and Description Table

Category	Field	Description
Request Details	**Created By**	This is a read-only field and is auto-populated based on the login information. Displays details of the request creator.
	Certificate Request Type	This is a read-only field and is auto-populated based on the certificate request. Displays the type of certificate request.
Certificate Information	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Authority	This is a read-only field and is auto-populated based on the **CA Tag** selected. Displays the certificate authority with which the CA tag is associated.
	***Certificates**	The values in this field are fetched from AppViewX based on the **CA Tag** selected and **Certificate Category** configured in **CLM Settings**. Select the certificate you wish to revoke from the options available in the dropdown.
	Common Name	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Common Name** for the selected certificate.
	Serial Number	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Serial Number** for the selected certificate.
Revocation Reason	***Reason**	This field is displayed only when the certificate to be revoked is selected.

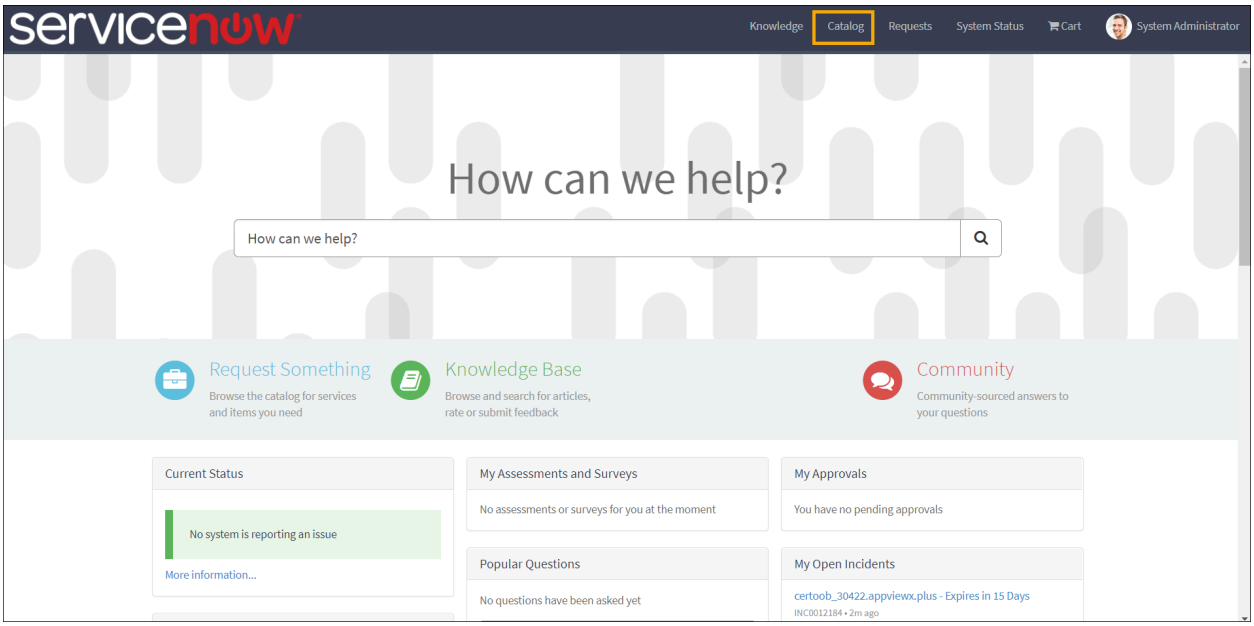
Category	Field	Description
		Select the reason for revoking the certificate from the options available in the dropdown.
	Comments	This field is displayed only when the certificate to be revoked is selected. Enter any comments to further explain the reasons for revoking the certificate.
Revoke Notification	***Email ID**	This field is displayed only when the certificate to be revoked is selected. Enter the Email ID where the revoke notification is to be sent.
AppViewX Response	**Request ID**	This is a read-only field and the value is fetched from AppViewX's Request module. Displays the Request ID of the workflow executed in AppViewX.
	AppViewX Response	Displays the AppViewX Response.
**: Mandatory fields*		

2. To submit the workflow request for revoking the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To check the request status for this request, from the navigation pane on the left, under **CERT+**, click **Certificate Requests**.

Service Portal

Overview

You can also self-service certificate automation workflow requests from the Service Portal. You can access these requests by clicking **Catalog** from the menu bar.



The **Catalog** displays the list of certificate automation workflow requests and recent self-serviced requests. You can also browse for CLM requests by typing the keyword(s) in the search bar. The following certificate requests can be self-serviced from the Service Portal:

- Enroll Certificate
- Renew Certificate
- Revoke Certificate

Self-Servicing a Certificate Enrollment Workflow Request

To self-service a workflow request for enrolling a certificate from the Service Portal **Catalog**:

1. On the Catalog page, click **Enroll Certificate**.
   The **Enroll Certificate** input form page is displayed.

   The following table describes the field information requested on this page:

Category	Field	Description
Request Details	**Created By**	This is a read-only field and is auto-populated based on the login information. Displays details of the request creator.
	Certificate Request Type	This is a read-only field and is auto-populated based on the certificate request.

Category	Field	Description
		Displays the type of certificate request.
CA Details	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Policy	This is a read-only field and is auto-populated based on the **CA Tag** selected. Displays the certificate policy associated with the selected CA.
	***CSR Input Method**	Select if the method of submitting CSR is: • **Manual** • **Upload CSR**
	***Certificate Category**	This field is displayed only when the **CSR Input Method** is selected. Select the category of certificate from the options available in the dropdown: • Server • Client • Code Signing
Certificate Attributes	**Test Data 2**	Enter the Certificate Attributes, if required.
AppViewX Response	**Request ID**	This is a read-only field and the value is fetched from AppViewX's Request module. Displays the Request ID of the workflow executed in AppViewX.
	AppViewX Response	Displays the AppViewX Response.

Category	Field	Description
All * marked fields are mandatory.		

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
3. For information about the RITM number for this request, click **Enroll Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflows in AppViewX's Request module), and the status of the workflow request.

CSR Input Method - Manual

If you select the CSR input method as **Manual**:

1. In the **CSR Parameters** section, enter the required field information.

   The following table describes the fields in this section:

   CSR Parameters - Field and Description Table

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Do you want to add SAN Values?	Select the appropriate checkbox for adding SAN Values. • Add DNS Values • Add IP Address
DNS	This field is displayed only if you select the Add DNS Values checkbox. Enter DNS value.
IP Address	This field is displayed only if you select the Add DNS Values checkbox. Enter IP Address.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
**: Mandatory fields*	

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Order Now**.
   The **Order Status** page is displayed with details of the certificate request and the request number.
3. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
4. For information about the RITM number for this request, click **Enroll Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflows in AppViewX's Request module), and the status of the workflow request.

CSR Input Method - Upload CSR

If you select the CSR input method as **Upload CSR**:

1. In the **CSR Parameters** section, enter the required field information.

   The following table describes the fields in this section:

CSR Parameters - Field and Description Table

Field	Description
***CSR Upload Option**	Select the option for uploading the CSR from the options available in the dropdown: • Paste CSR • File Upload
***Paste CSR**	This field is displayed only when you select the **Paste CSR** option in the **CSR Upload Option** field. The CSR file is validated for file type and size and a warning is issued if validation fails. Paste the CSR in this field.
***Upload CSR**	This field is displayed only when you select the **Upload CSR** options in the **CSR Upload Option** field. The CSR file is validated for file type and size and a warning is issued if validation fails. To upload the CSR, click **Required - Upload**.
***Validity Unit**	This field is displayed only when the CSR is pasted or uploaded. Select the validity unit as:

Field	Description
	• Months • Days • Years
***Validity Value**	This field is displayed only when the CSR is pasted or uploaded. Select the validity value for the certificate as per the validity unit selected.
**: Mandatory fields*	

2. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
3. For information about the RITM number for this request, click **Enroll Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflows in AppViewX's Request module), and the status of the workflow request.

Self-Servicing a Certificate Renewal Workflow Request

To self-service a workflow request for renewing a certificate from the Service Portal catalog:

1. On the Service Portal's Catalog page, click **Renew Certificate**.
   The **Renew Certificate** input form page is displayed.

   The following table describes the field information requested on this page:

   Renew Certificate - Field and Description Table

Category	Field	Description
Request Details	**Created By**	This is a read-only field and is auto-populated based on the login information. Displays details of the request creator.
	Certificate Request Type	This is a read-only field and is auto-populated based on the certificate request. Displays the type of certificate request.

Category	Field	Description
Certificate Information	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Authority	This is a read-only field and is auto-populated based on the **CA Tag** selected. Displays the certificate authority with which the CA tag is associated.
	***Certificates**	Select the certificate you wish to renew from the options available in the dropdown. **Note:** The values in this field are fetched from AppViewX based on the **CA Tag** selected and **Certificate Category** configured in **CLM Settings**.
	Common Name	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Common Name** for the selected certificate.
	Serial Number	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Serial Number** for the selected certificate.
Renewal Method	**Renewal Method**	Select the method for renewing the certificate. The options available are: • Use existing key • Generate with new key
Certificate Issuance	***Email ID**	Enter the email ID of the user to whom the certificate will be sent.
AppViewX Response	**Request ID**	This is a read-only field and the value is fetched from AppViewX's Request module.

Category	Field	Description
		Displays the Request ID of the workflow executed in AppViewX.
	AppViewX Response	Displays the AppViewX Response.
**: Mandatory fields*		

2. To submit the workflow request for renewing the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
3. For information about the RITM number for this request, click **Renew Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflows in AppViewX's Request module), and the status of the workflow request.

Certificate Renewal using Existing Key

If you renew the selected certificate using the existing key, the CSR parameters are automatically fetched and displayed in the **CSR Parameters** section.

1. To submit the workflow request for renewing the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
2. For information about the RITM number for this request, click **Renew Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflow in AppViewX's Request module), and the status of the workflow request.

Certificate Renewal with a New Key

If you renew the selected certificate by generating a new key:

1. In the **CSR Type** field, select if you wish to use the existing CSR or upload a new CSR.
2. If you select the CSR Type as **Existing CSR**, the CSR parameters are automatically fetched and displayed in the **CSR Parameters** section.
3. If you select the CSR Type as **Upload New CSR**, in the **CSR Upload Option** field, select the required option.

- **Paste CSR**: Paste the CSR in the Paste CSR field.
- **File Upload**: Click **Required-Upload** to upload the .csr file.

4. To submit the workflow request for enrolling the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
5. For information about the RITM number for this request, click **Renew Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflows in AppViewX's Request module), and the status of the workflow request.

Self-Servicing a Certificate Revocation Workflow Request

To self-service a workflow request for revoking a certificate from the AppViewX Catalog:

1. On the **AppViewX Catalog** page, click **Revoke Certificate**.
   The **Revoke Certificate** input form page is displayed.

   The following table describes the field information requested on this page:

Revoke Certificate - Field and Description Table

Category	Field	Description
Request Details	**Created By**	This is a read-only field and is auto-populated based on the login information. Displays details of the request creator.
	Certificate Request Type	This is a read-only field and is auto-populated based on the certificate request. Displays the type of certificate request.
Certificate Information	***CA Tag**	Select the CA Tag from the options available in the dropdown. **Note:** This tag is defined at the time of configuring CLM settings.
	Certificate Authority	This is a read-only field and is auto-populated based on the **CA Tag** selected.

Category	Field	Description
		Displays the certificate authority with which the CA tag is associated.
	***Certificates**	Select the certificate you wish to revoke from the options available in the dropdown. **Note:** The values in this field are fetched from AppViewX based on the **CA Tag** selected and **Certificate Category** configured in **CLM Settings**.
	Common Name	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Common Name** for the selected certificate.
	Serial Number	This is a read-only field and is auto-populated based on the certificate selected. Displays the **Serial Number** for the selected certificate.
Revocation Reason	***Reason**	This field is displayed only when the certificate to be revoked is selected. Select the reason for revoking the certificate from the options available in the dropdown.
	Comments	This field is displayed only when the certificate to be revoked is selected. Enter any comments to further explain the reasons for revoking the certificate.
Revoke Notification	***Email ID**	This field is displayed only when the certificate to be revoked is selected. Enter the Email ID where the revoke notification is to be sent.
AppViewX Response	**Request ID**	This is a read-only field and the value is fetched from AppViewX's Request module.

Category	Field	Description
		Displays the Request ID of the workflow executed in AppViewX.
	AppViewX Response	Displays the AppViewX Response.
**: Mandatory fields*		

2. To submit the workflow request for revoking the certificate, from the right side of the screen, click **Submit**.
   The **Request Summary** page is displayed with details of the certificate request and the request number.
3. For information about the RITM number for this request, click **Revoke Certificate**.
   The page displays the RITM number, Request ID (for stage-wise view of the workflow in AppViewX's Request module), and the status of the workflow request.