CERT+ Automation Workflows User Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

External Reference Links

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

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

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

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2022.1.0	June 2022
2.0	Updated release of document for release 2022.1.0 FP2 Beta	November 2022

About this Guide

This guide informs you about the APIs to be used for executing different Cert+ Automation workflows.

Audience

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

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: Prerequisites

The following table describes the web browser requirements to create and execute workflows as well as tasks.

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	V74.0.1 (64-bit) or later
Google Chrome	V85.0.4183.83 (64-bit) or later

Chapter 2: Role-Based Access Control

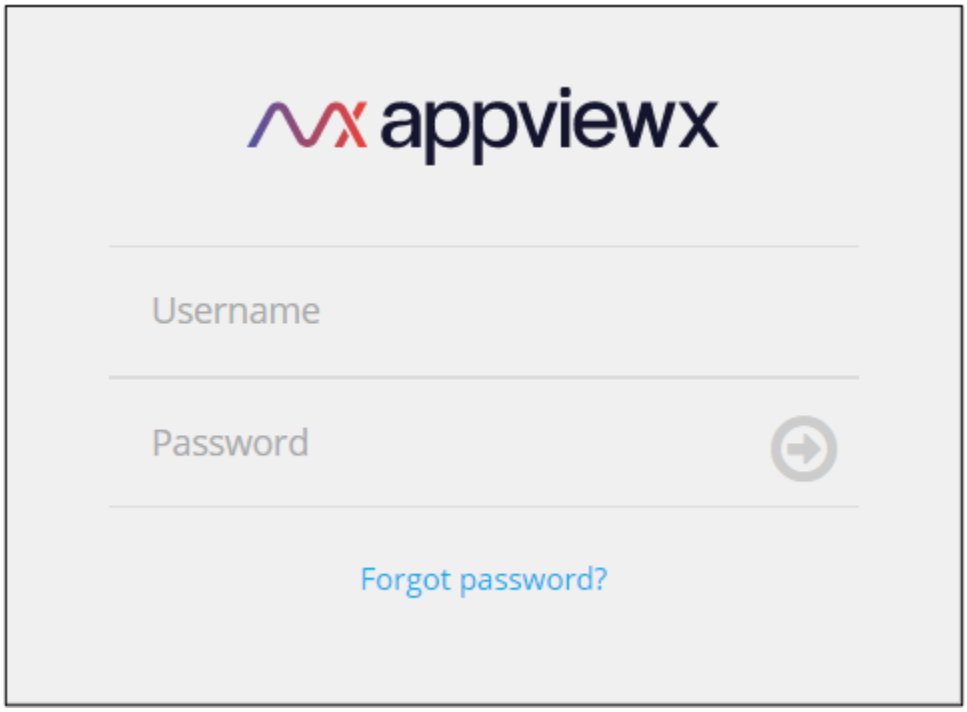
With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to this link and find out more about RBAC.

Chapter 3: Accessing CERT+ Automation Workflows

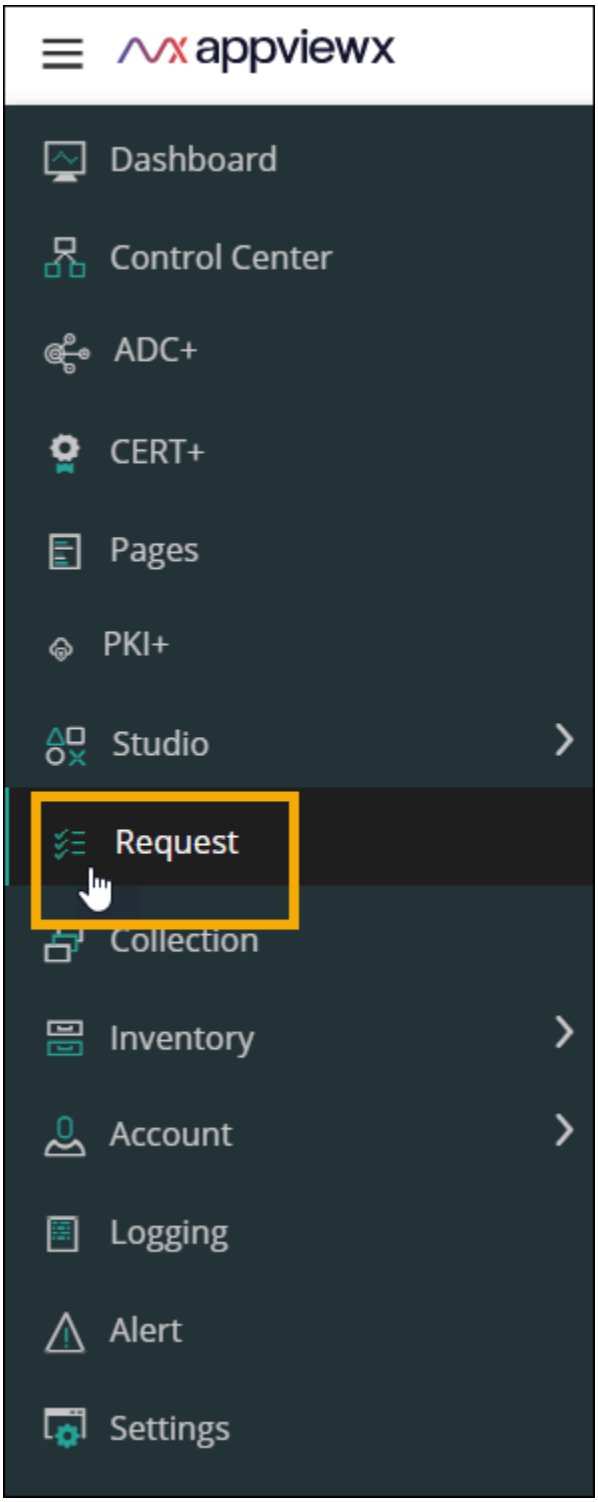
The CERT+ Automation workflows are available on the Workflow **Catalog** page.

To view these workflows:

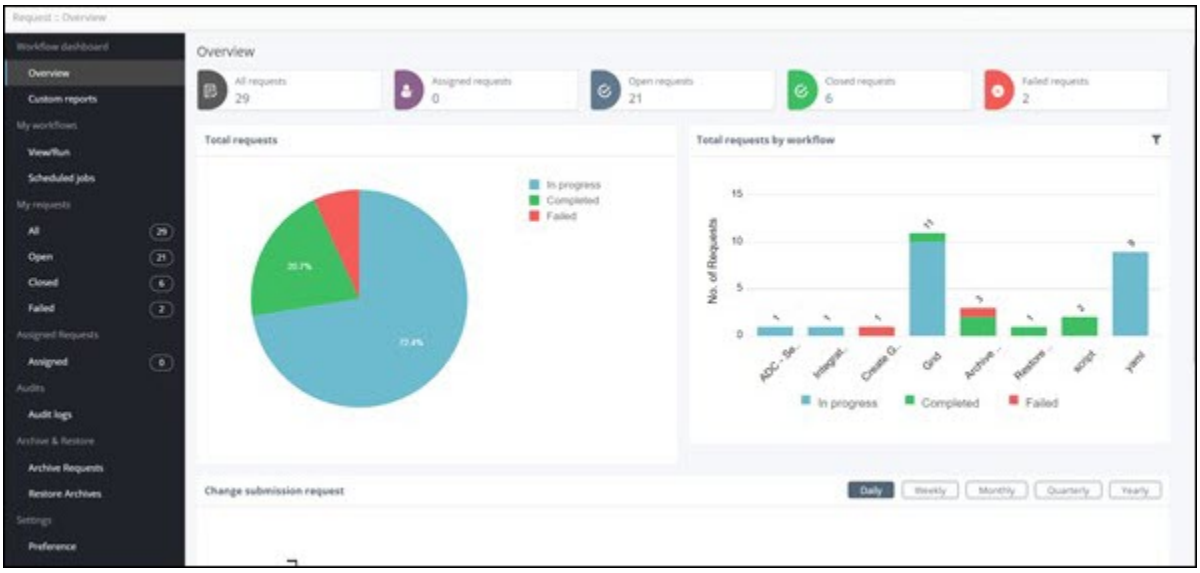
1. Log into AppViewX with valid credentials.



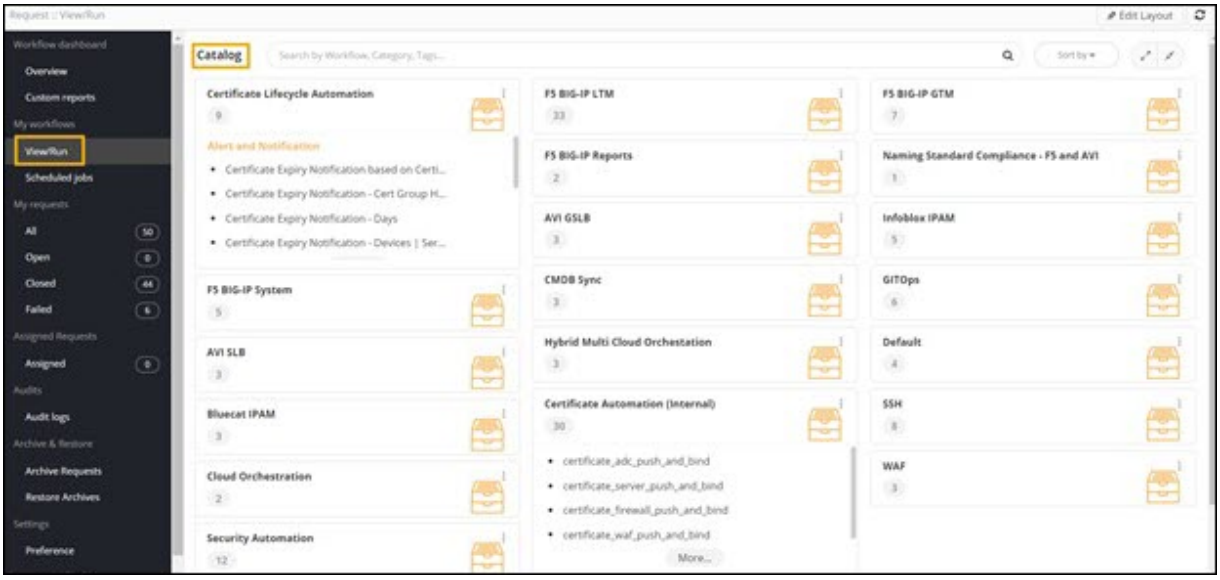
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Request**.



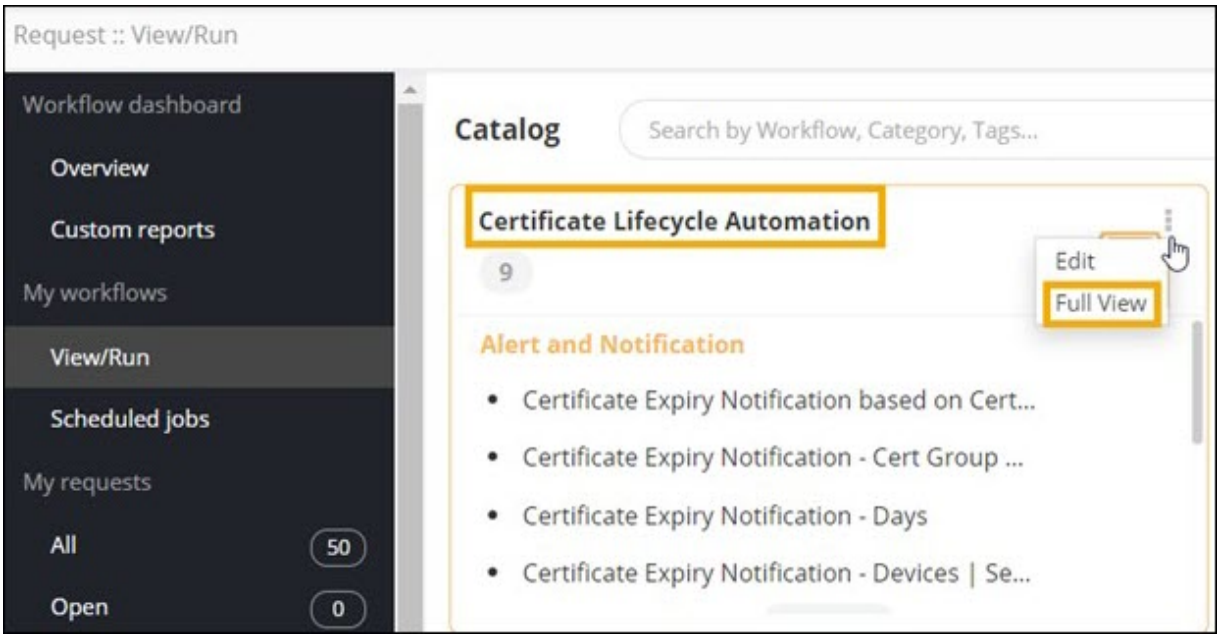
The Workflow **Request** page is displayed, with the **Overview** section open by default.



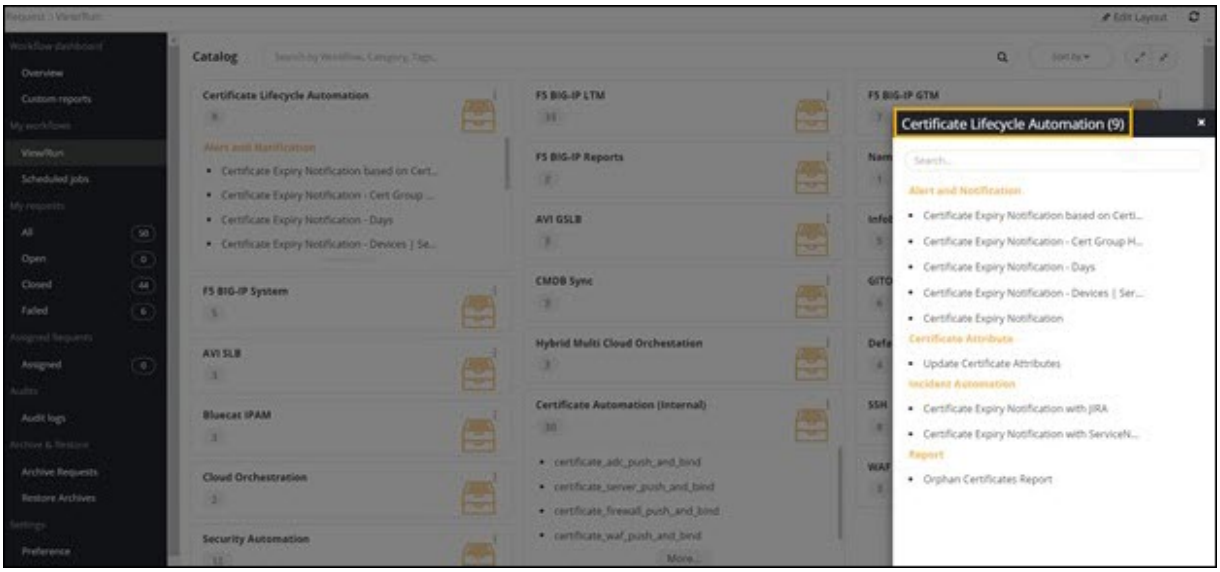
4. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.



5. On the **Catalog** page, under the **Certificate Lifecycle Automation** category, click .
6. From the options displayed, select **Full View**.



The CERT+ Automation workflows are displayed in the **Certificate Lifecycle Automation** window.

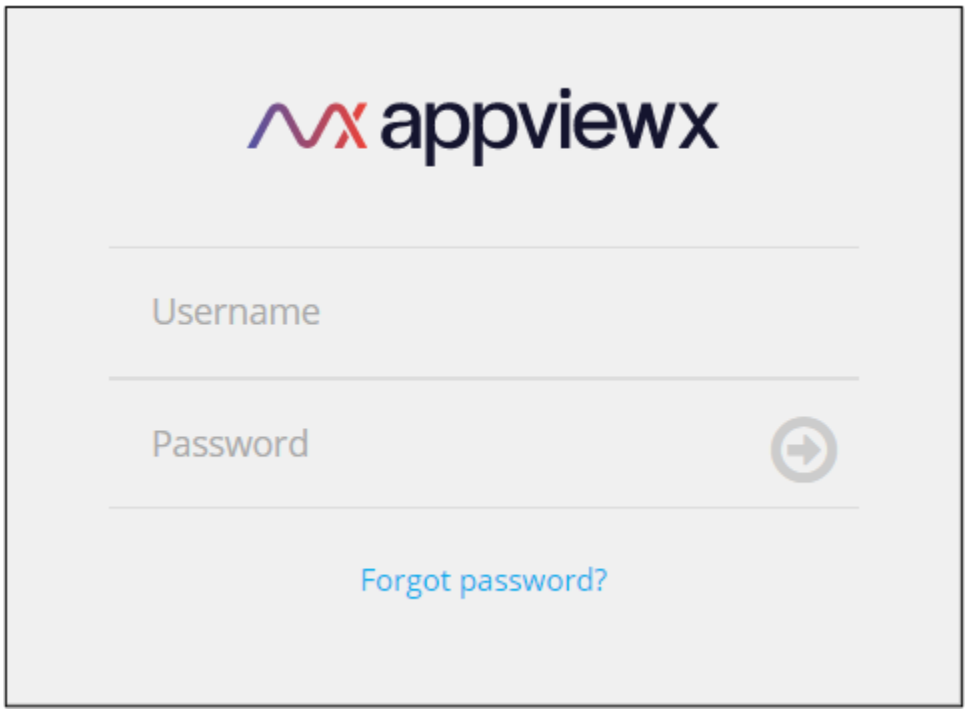


Tip: You can also search for a workflow on the **Catalog** page by typing the keyword(s) in the search bar.

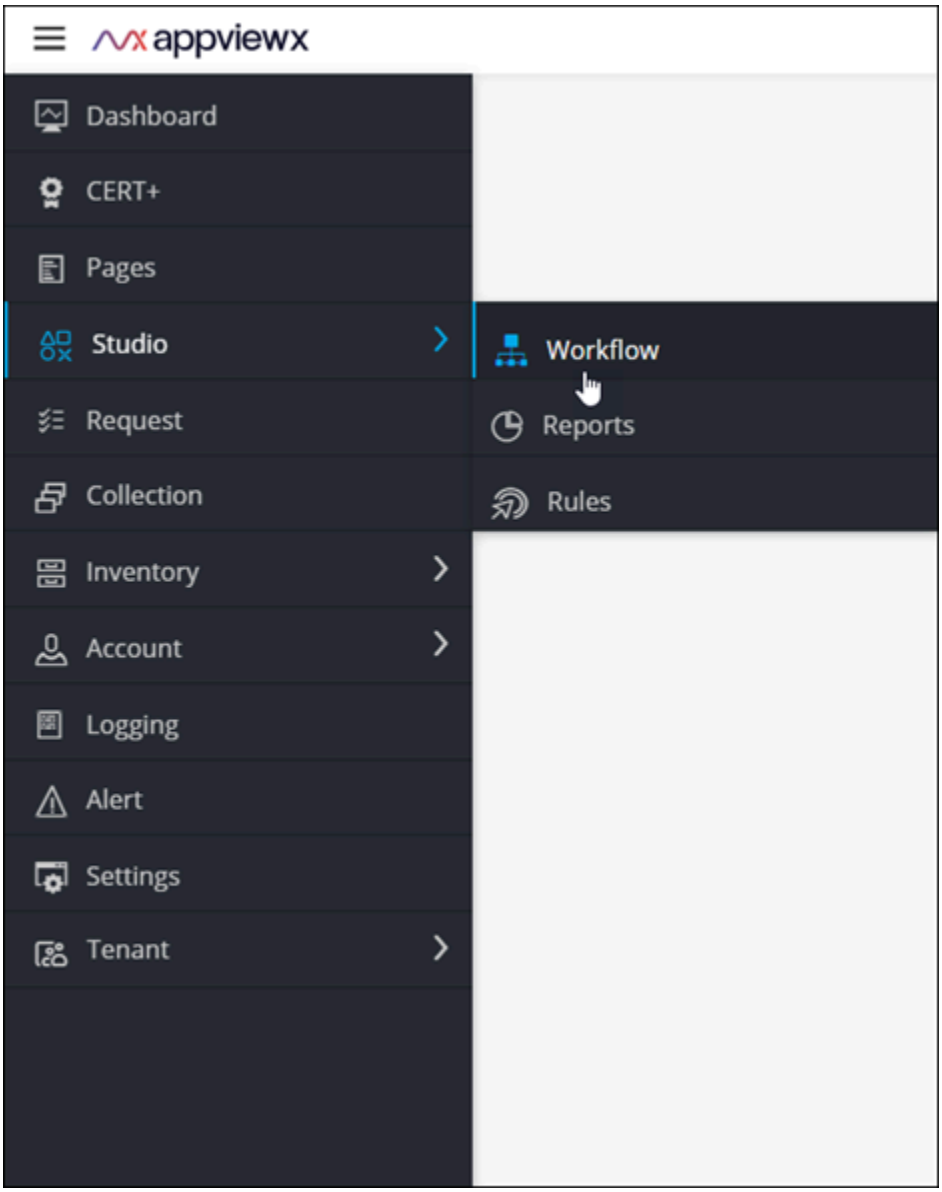
Chapter 4: Accessing CERT Automation Workflow Tasks

The CERT+ Automation workflow tasks enable you to design your own custom workflows. These are available in the Workflow Studio. To view these tasks:

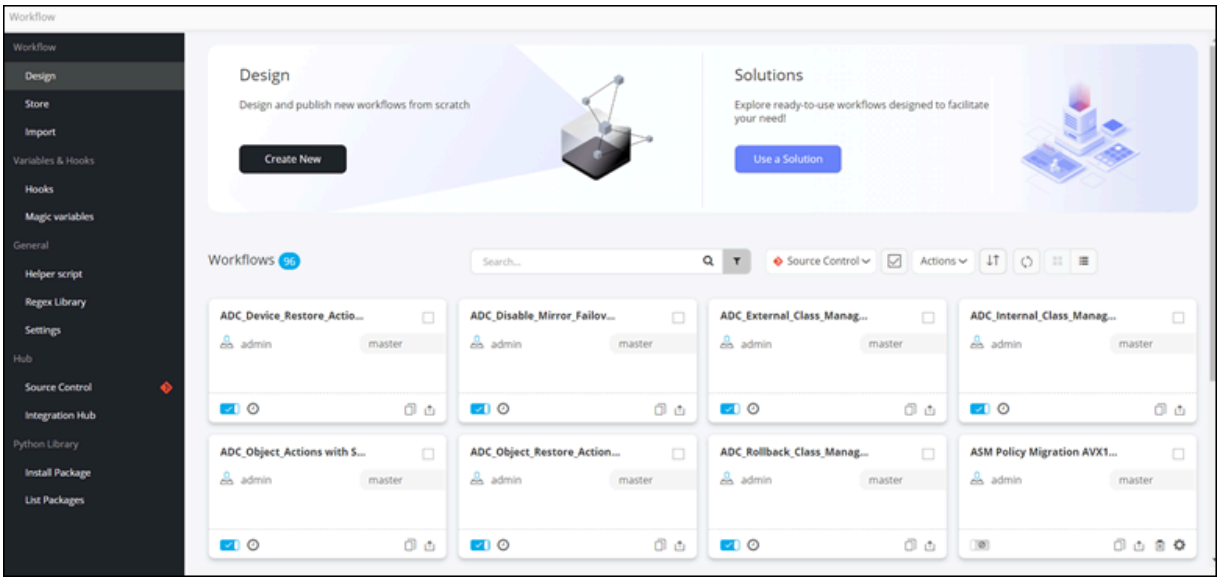
1. Log into AppViewX with valid credentials.



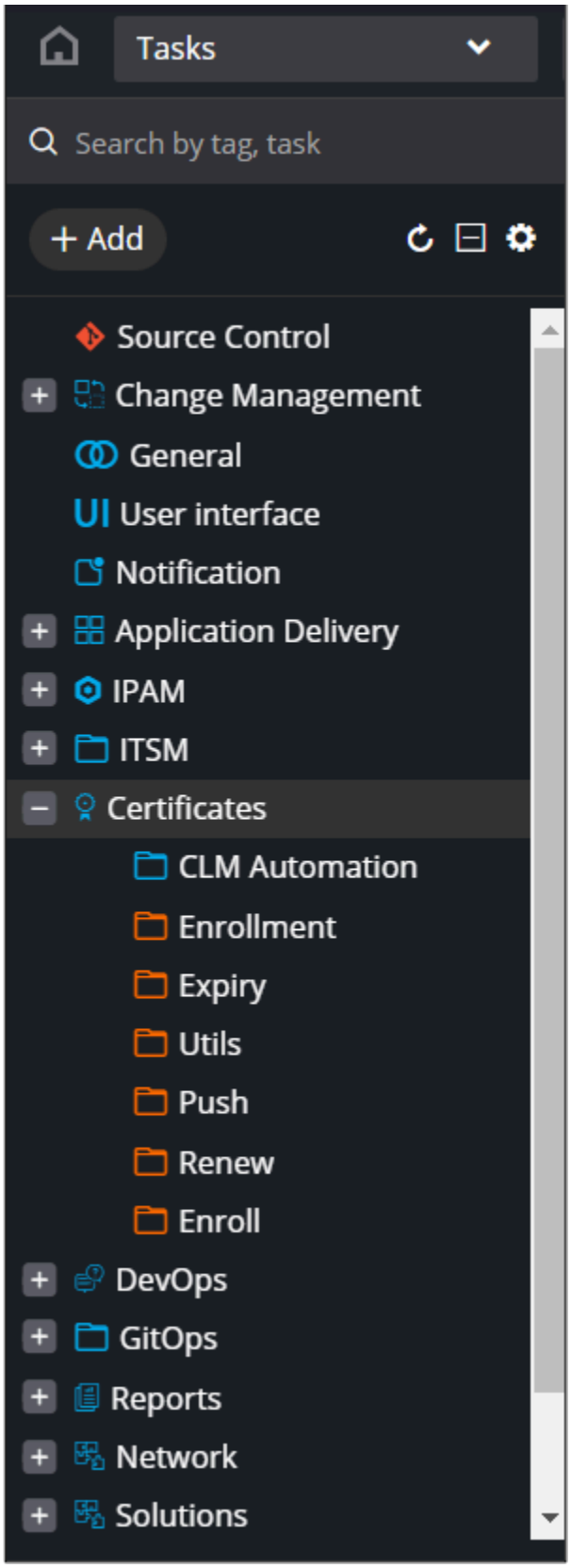
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



The **Workflow** inventory page is displayed.



4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.
7. To access the OOB workflow tasks, from the left menu, click **Certificates**.



The following categories of tasks are available in this folder:

- Enrollment - Lists all the OOB tasks for enrolling certificates from configured CAs.
- Expiry - Lists the Get Expiry Certificates task.
- Renew - Lists the Renew and Regenerate tasks.
- Push - Lists all the OOB taks for pushing certificates to devices and servers.

Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

Chapter 5: Certificate Expiry Workflows

Overview

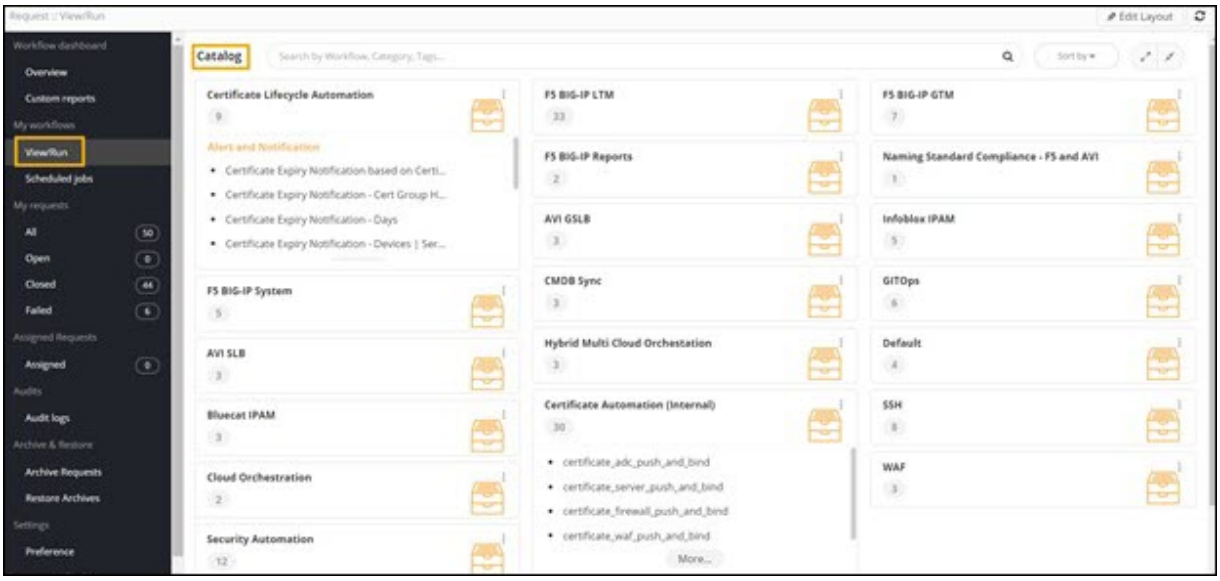
This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. It also enables you to create tickets for expiring certificates on Jira/ServiceNow.

Certificate Expiry Notification based on Certificate Attributes

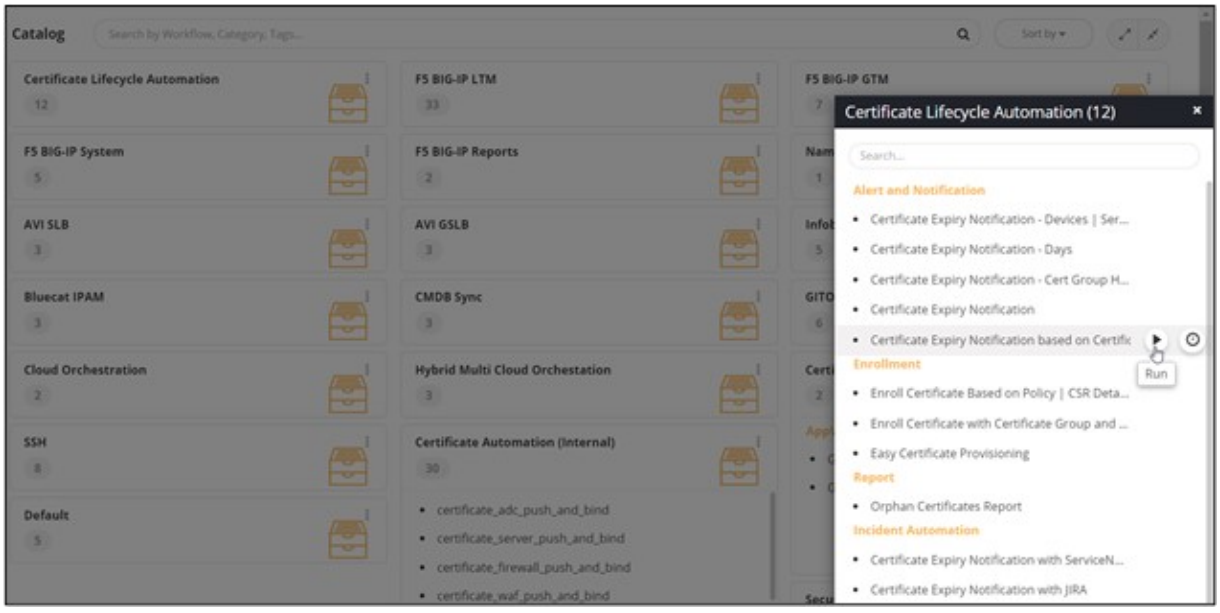
This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run.**
   The workflow **Catalog** page is displayed.

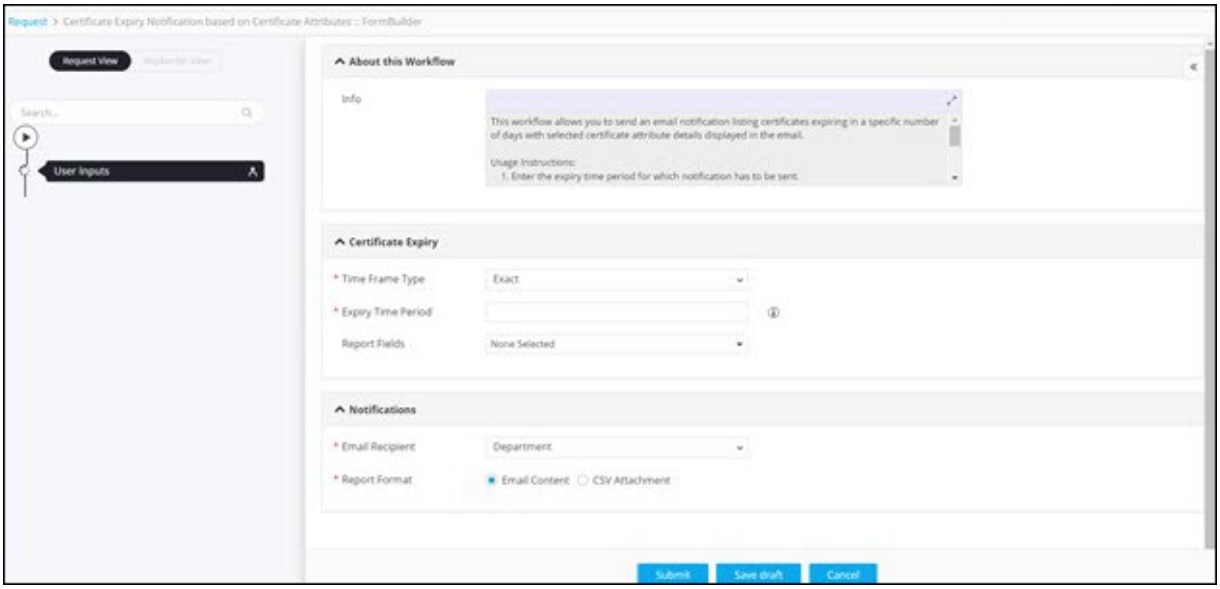


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification based on Certificate Attributes** workflow and click .

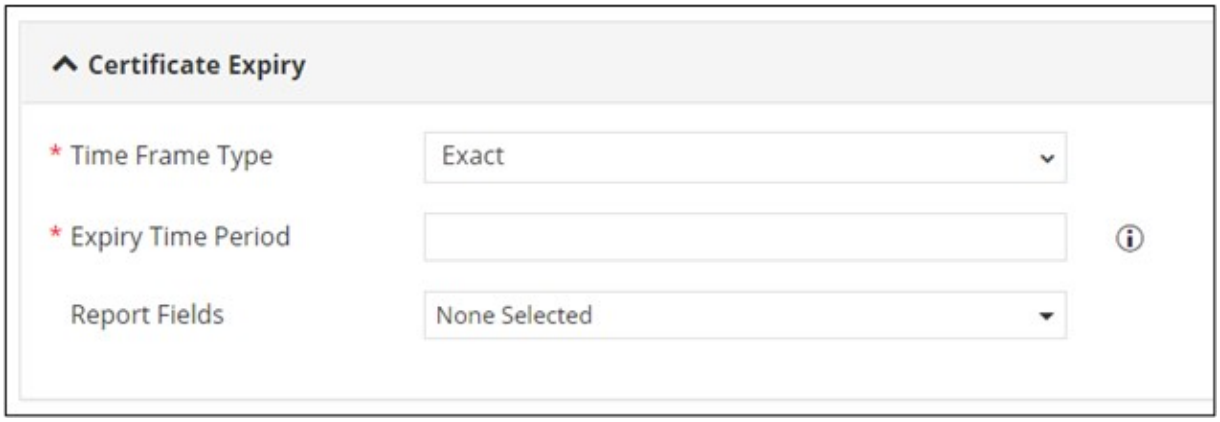


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



5. Under the **Certificate Expiry** section, enter or select the field information as shown.

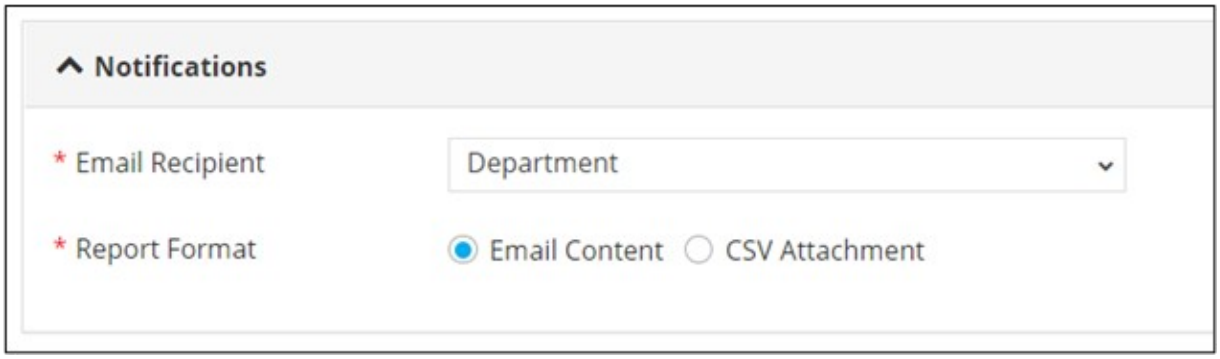


The following table describes the fields under the **Certificate Expiry** section:

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact** - The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month.

Field	Description
	• **Range** - The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter or select the field information as shown.

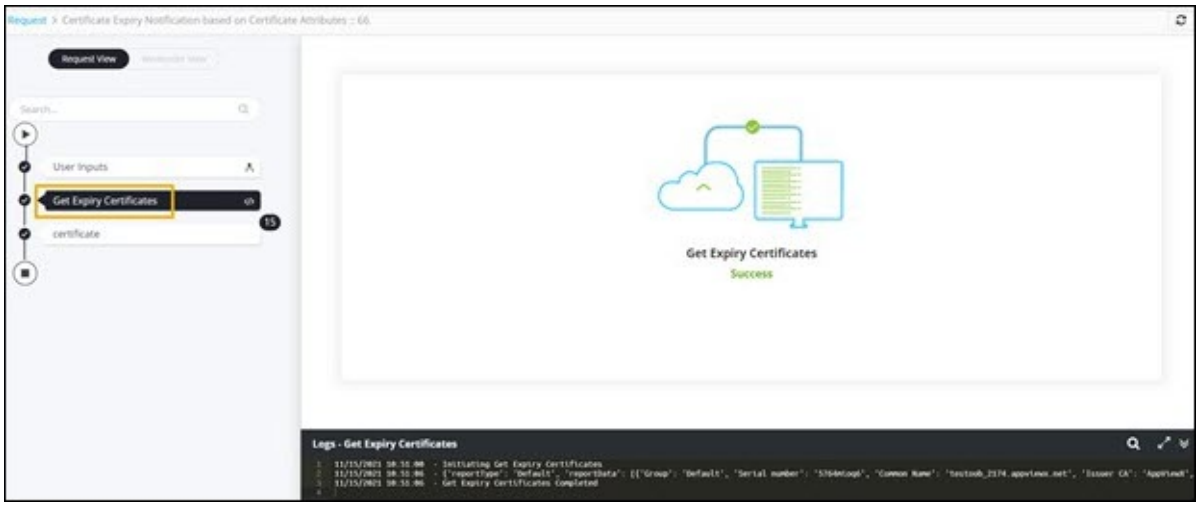


The following table describes the fields under the **Notifications** section:

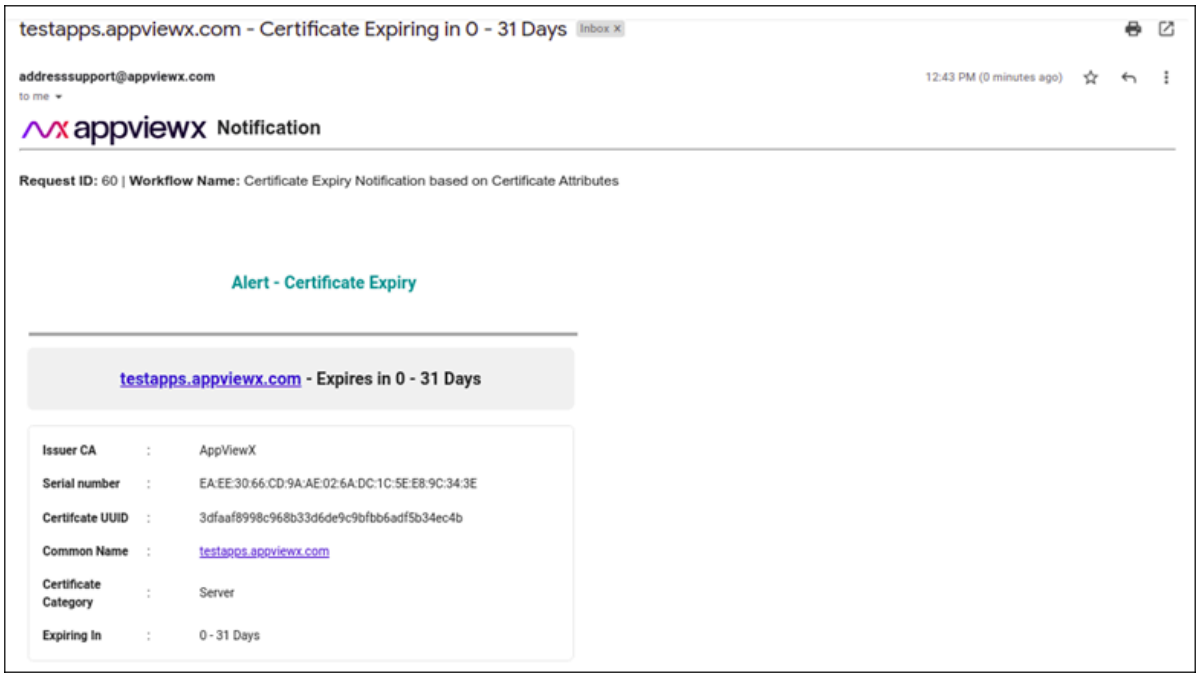
Field	Description
***Email Recipient**	Select the email recipient from the dropdown list.
***Report Format**	Select the required checkbox to send the report as: • **Email content** - The report will be sent as Email content. or

Field	Description
	• **CSV Attachment** - The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.
   - **Get Expiry Certificates** task completed.



   - Email notification received individually for expiring certificates.

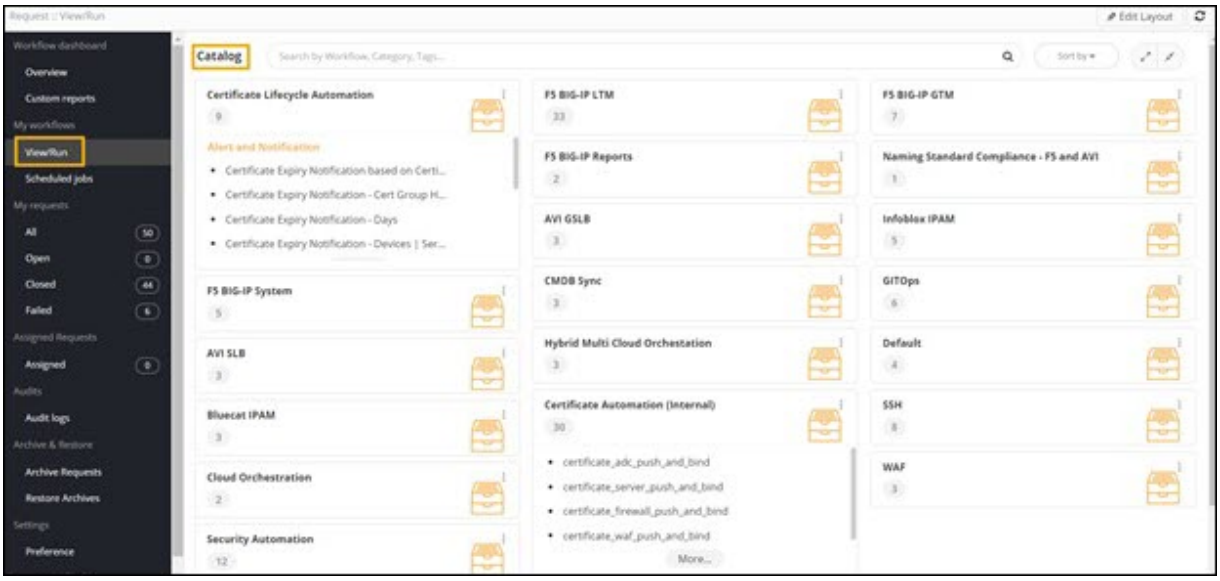


Certificate Expiry Notification - Cert Group Hierarchy

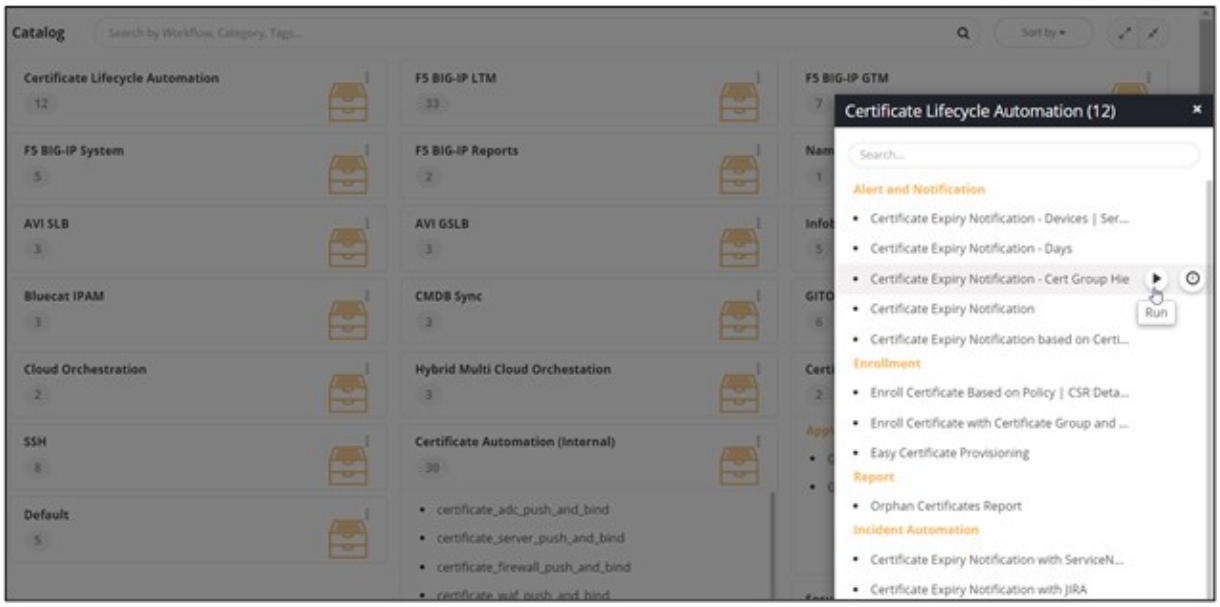
This workflow allows you to send a certificate expiry report notification to the certificate group and its associated hierarchical groups.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

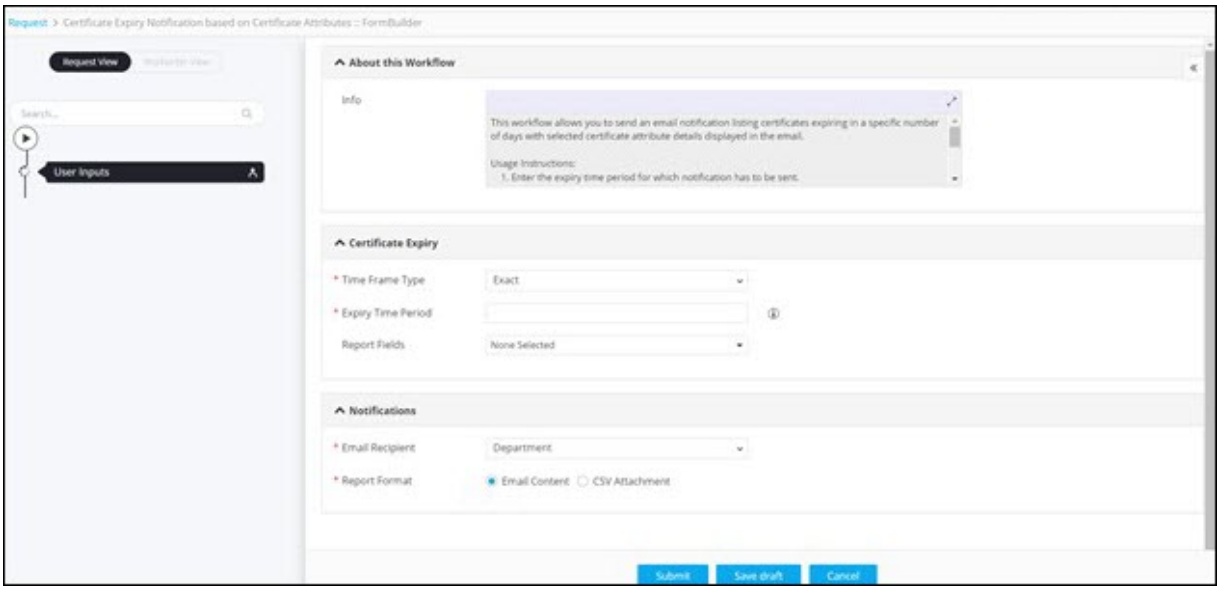


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Cert Group Hierarchy** workflow and click .

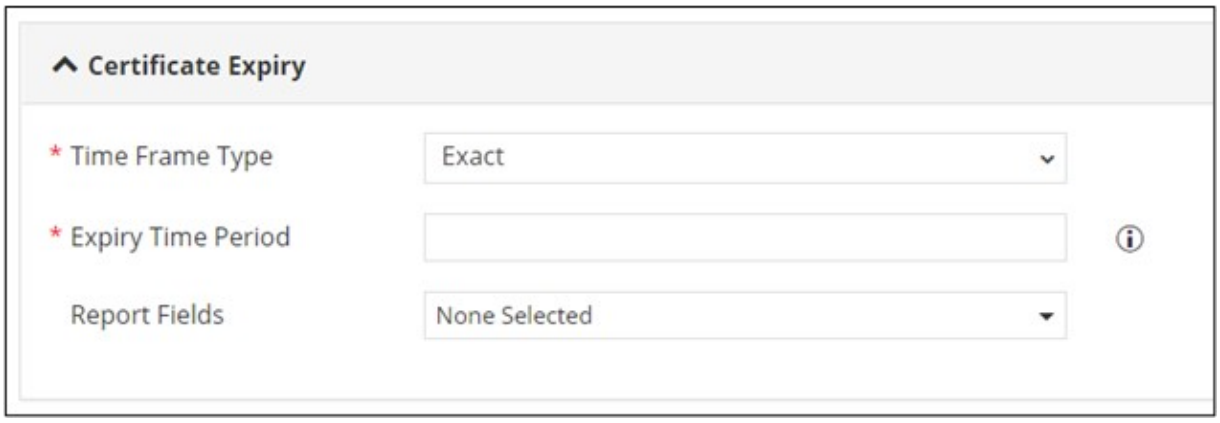


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



5. Under the **Certificate Expiry** section, enter or select the field information as shown.

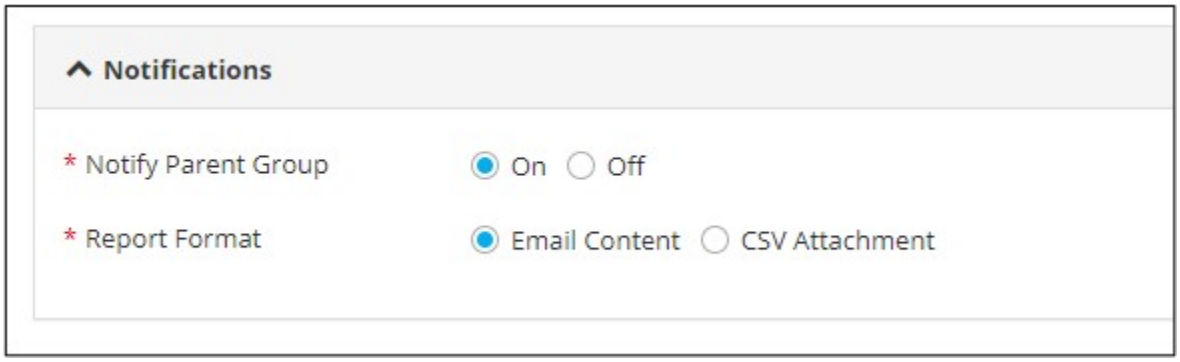


The following table describes the fields under the **Certificate Expiry** section:

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact** - The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range** - The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the

Field	Description
	range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter or select the field information as shown.



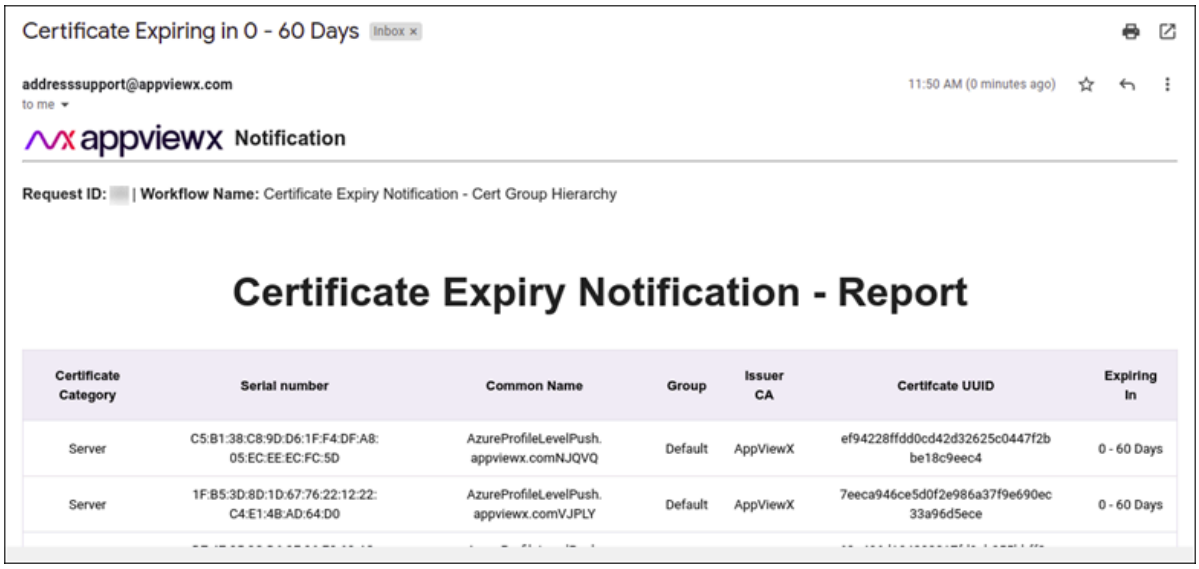
The following table describes the fields under the **Notifications** section:

Field	Description
***Notify Parent Group**	Select **On** if a notification has to be sent to the parent group of the certificate group. Select **Off** if a notification is not required to be sent to the parent group of the certificate group.

Field	Description
	Note: On is the default selection.
***Report Format**	Select the required checkbox to send the report as: • **Email content** - The report will be sent as Email content. or • **CSV Attachment** - The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.
   - **Get Expiry Certificates** task completed.

   - Email notification received.

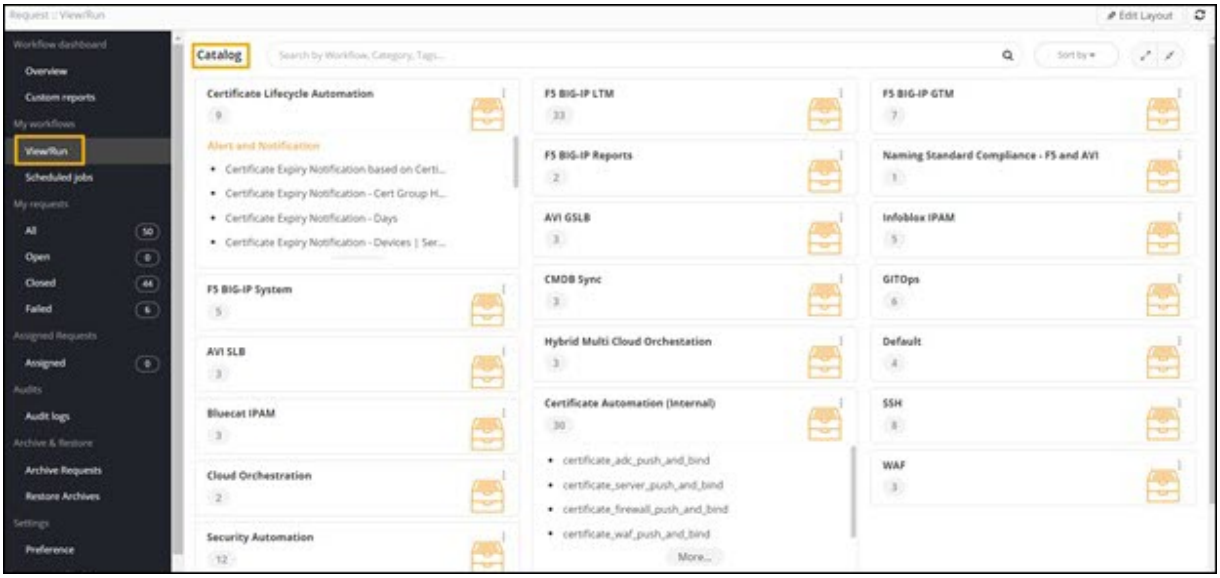


Certificate Expiry Notification - Days

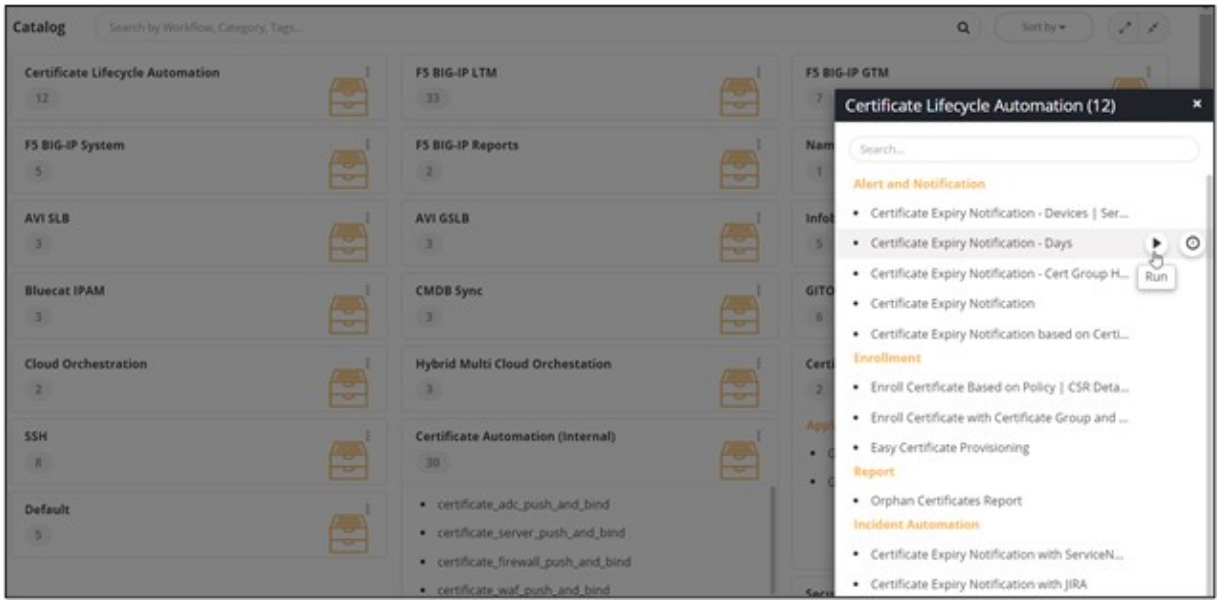
This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run.**
   The workflow **Catalog** page is displayed.

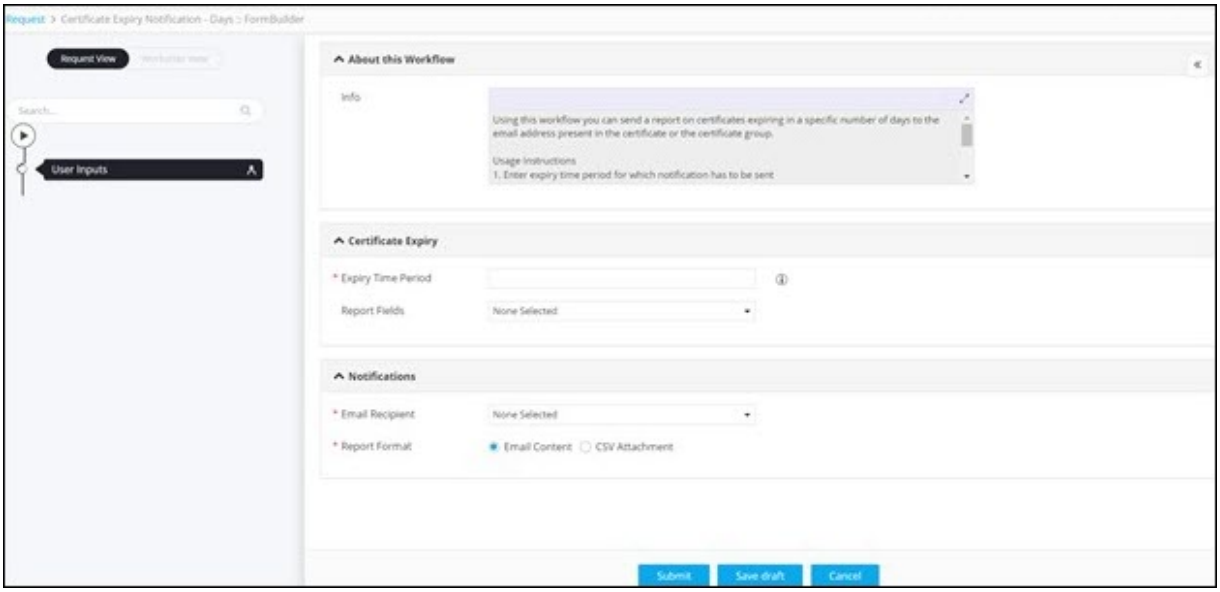


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Days** workflow and click .

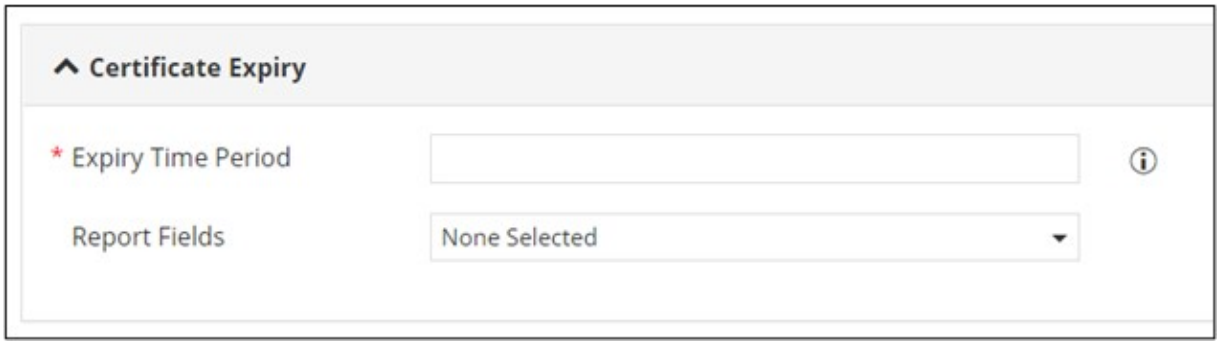


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



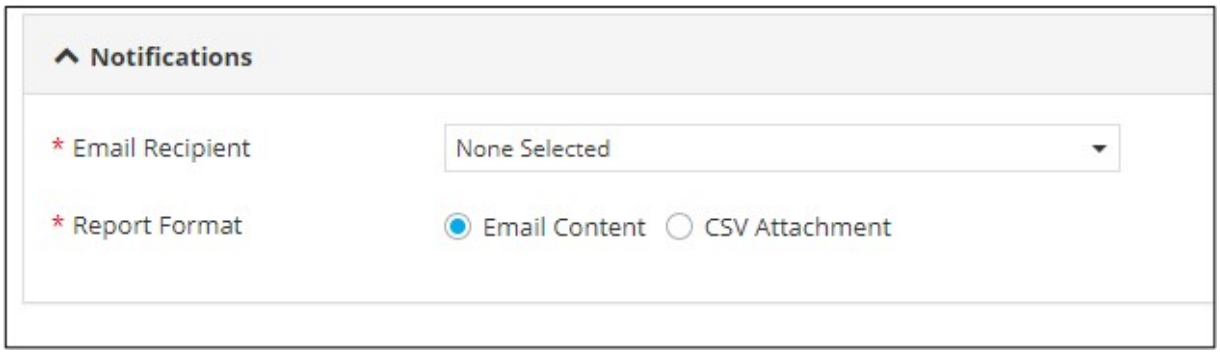
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



The following table describes the fields under the **Certificate Expiry** section:

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter or select the field information as shown.

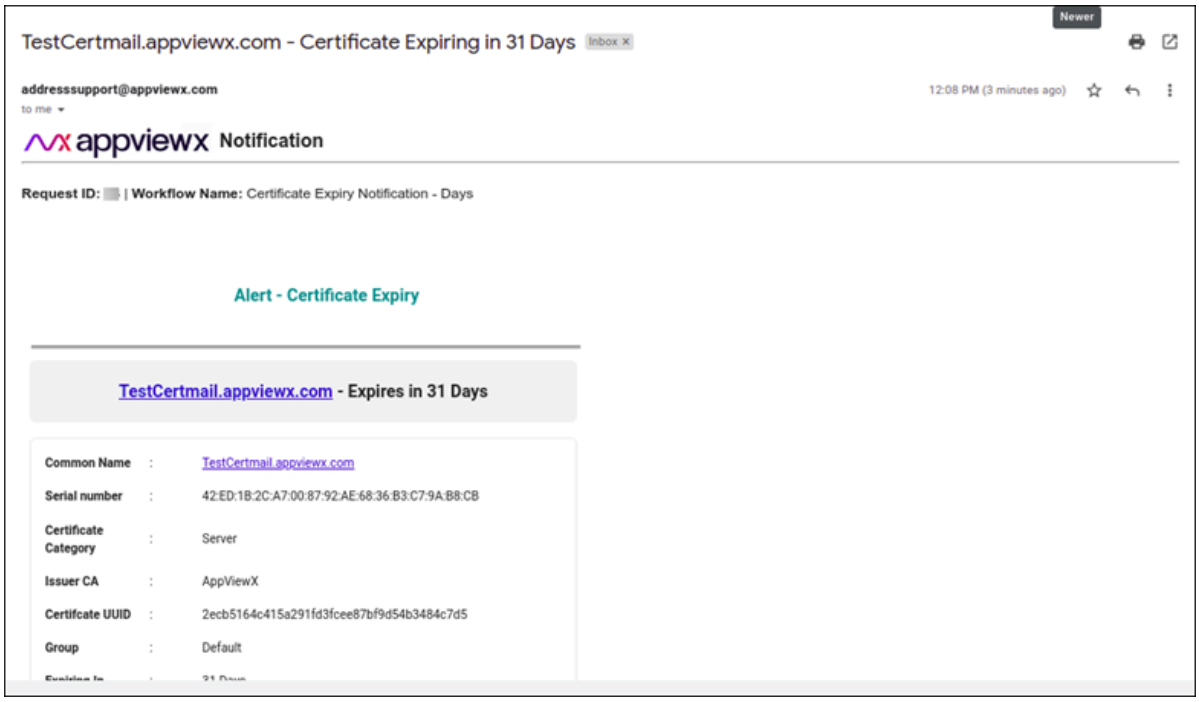


The following table describes the fields under the **Notifications** section:

Field	Description
***Email Recipient**	Select the required recipient of the notification. You can select: • **Select all** • **Certificate Email -** The notification will be sent to the email addresses associated with the certificate. • **Certificate Group Email -** The notification will be sent to the entire certificate group to which the certificate belongs.
***Report Format**	Select the required checkbox to send the report as: • **Email Content -** The report will be sent as Email content. or • **CSV Attachment -** The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.
   - Get Expiry Certificates task completed.

   - Email notification received with Certificate Expiry Alert for each expiring certificate.

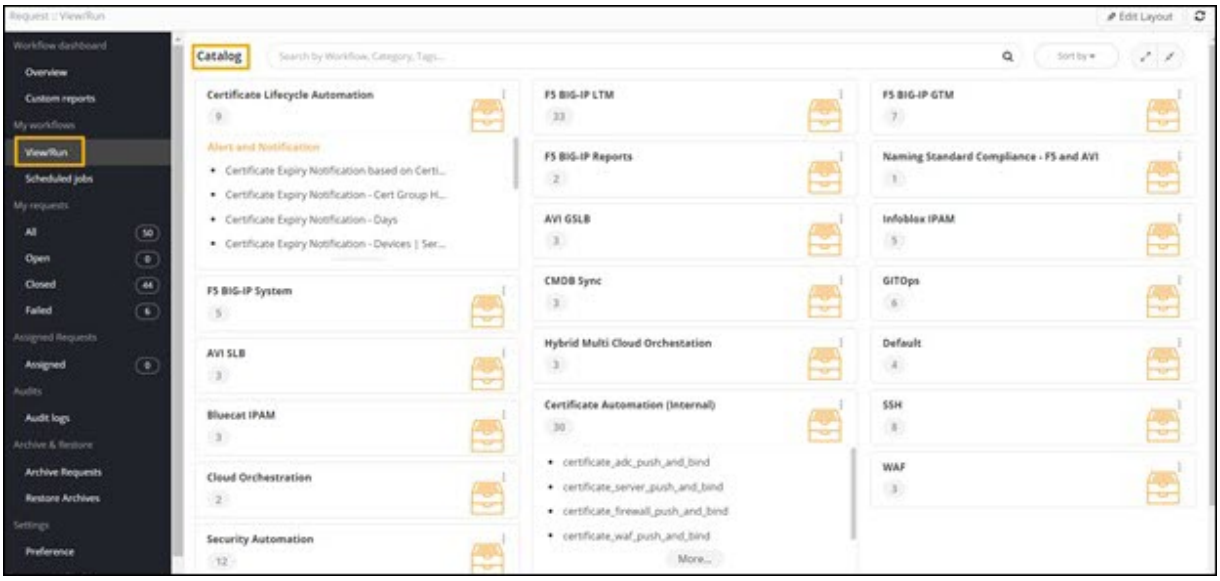


Certificate Expiry Notification - Devices | Servers

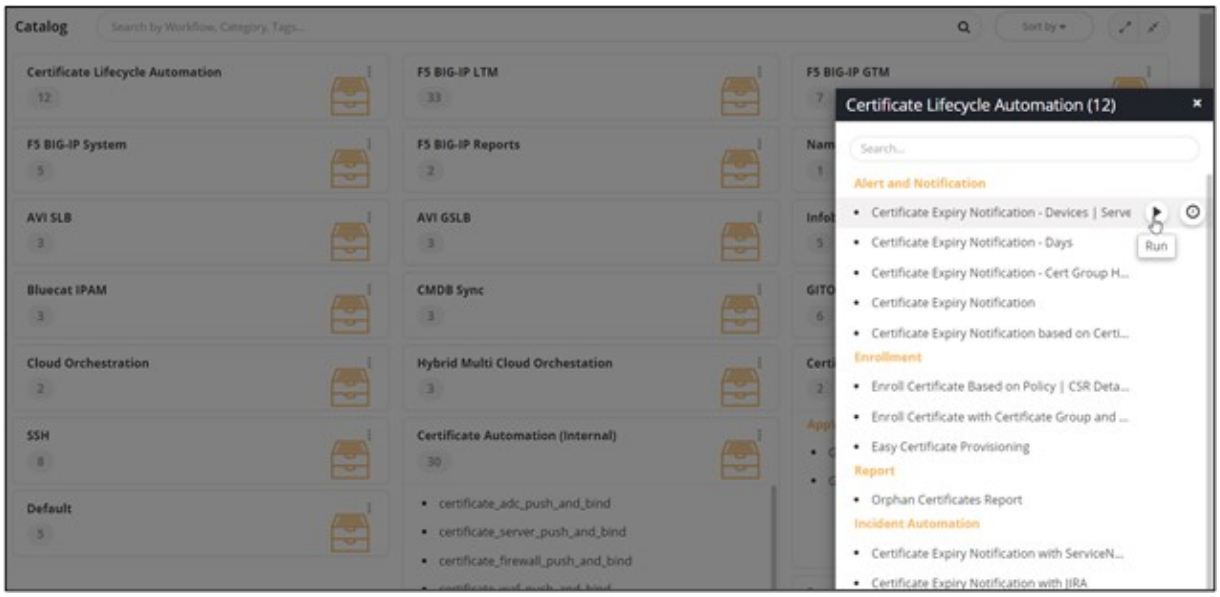
This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

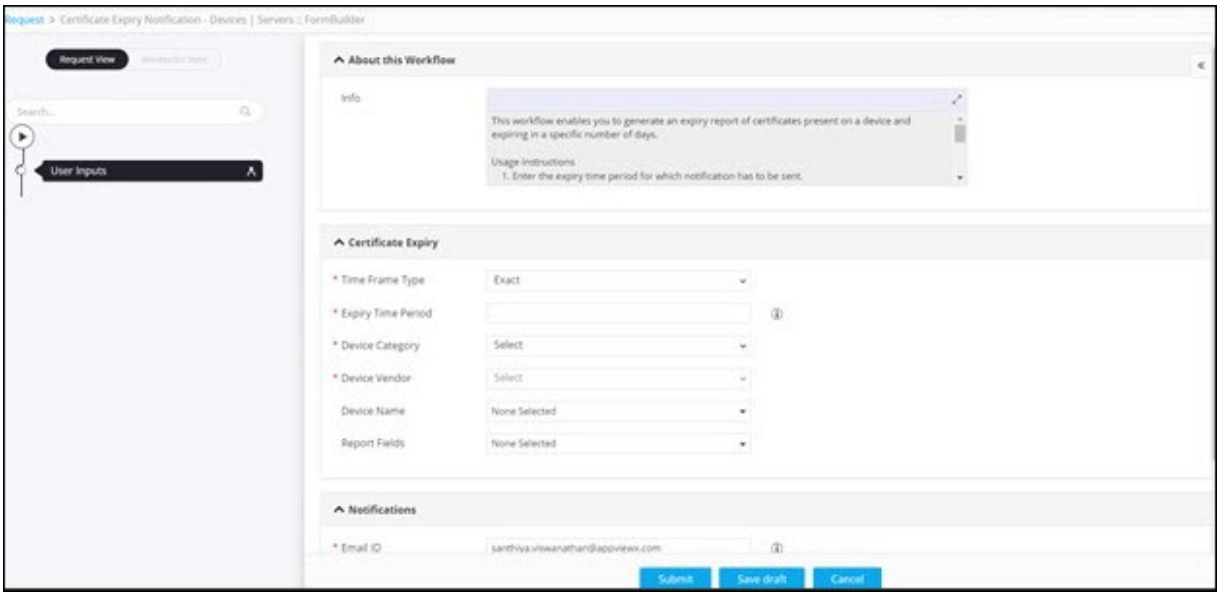


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Devices | Servers** workflow and click .

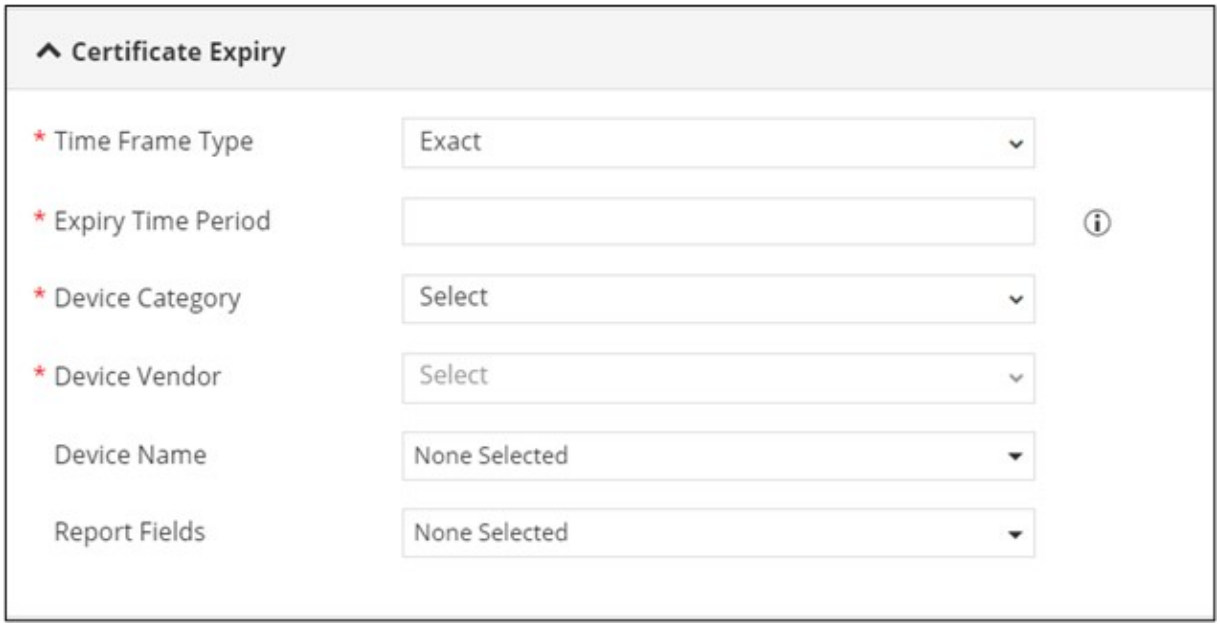


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



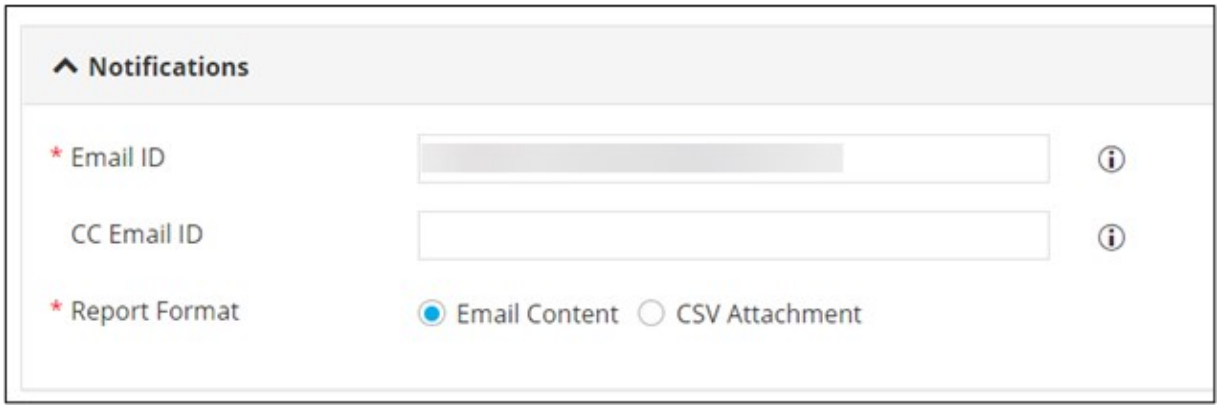
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



The following table describes the fields in the **Certificate Expiry** section:

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact -** The system generates a report of certificates that expire on exactly the number of days as mentioned in the Expiry Time Period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range -** The system generates a report of certificates that expire within a range of days as mentioned in Expiry Time Period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day. **Note: Exact** is the default selection.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
***Device Category**	Select the device category for the report from the dropdown list.
***Device Vendor**	Select the device vendor for the report from the dropdown list.
Device Name	Select the specific device for the report.
Report Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter or select the field information as shown.

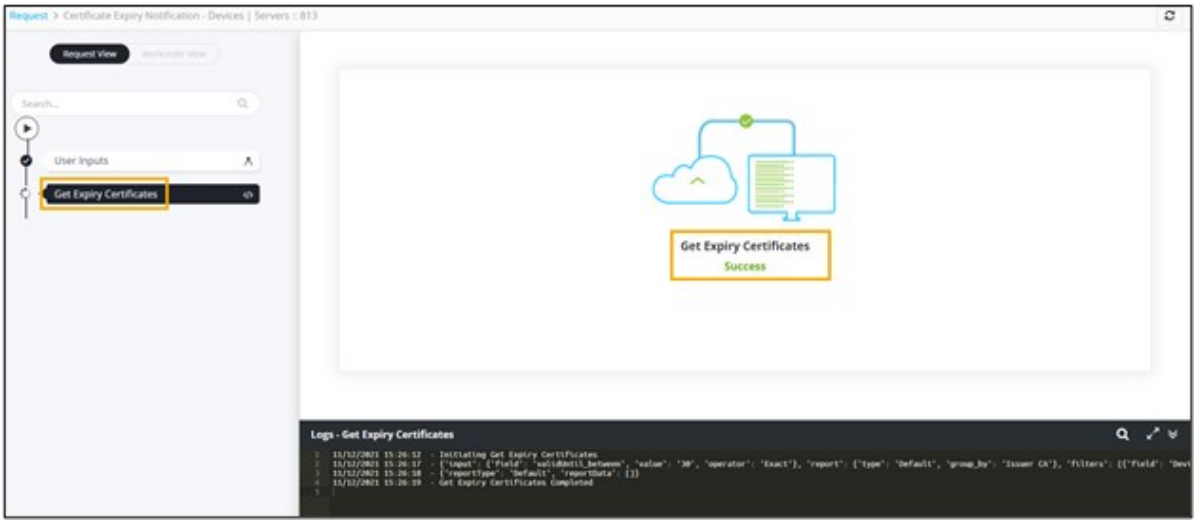


The following table describes the fields in the **Notifications** section:

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content -** The report will be sent as Email content. or • **CSV Attachment -** The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

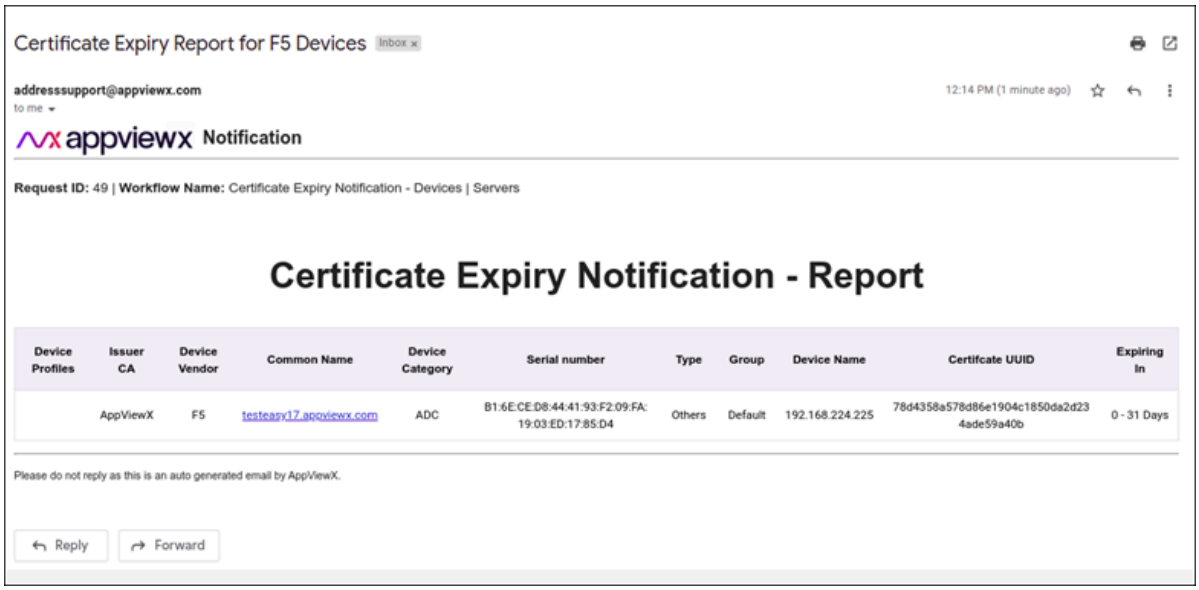
7. Click **Submit**.

- **Get Expiry Certificates** task completed.



- Certificate Device list generated.

- Email report received.



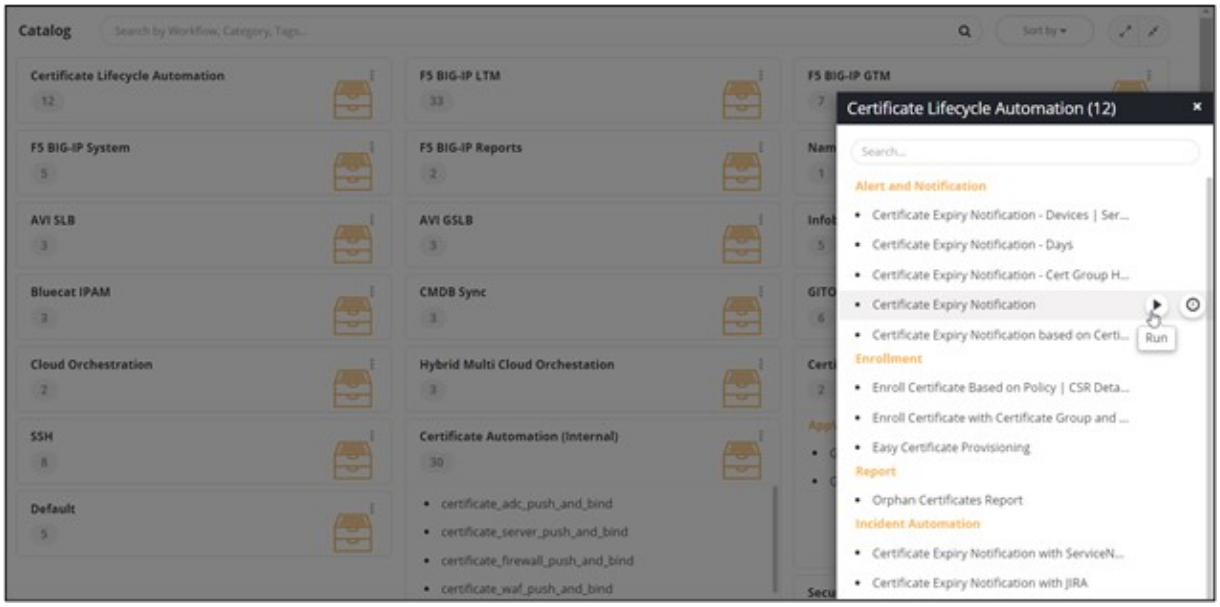
Certificate Expiry Notification

This workflow enables you to generate a report listing certificates expiring in a specific number of days and notify the recipients via email. You can also mention email addresses of the recipients who need to be informed additionally in CC mails.

To trigger this workflow:

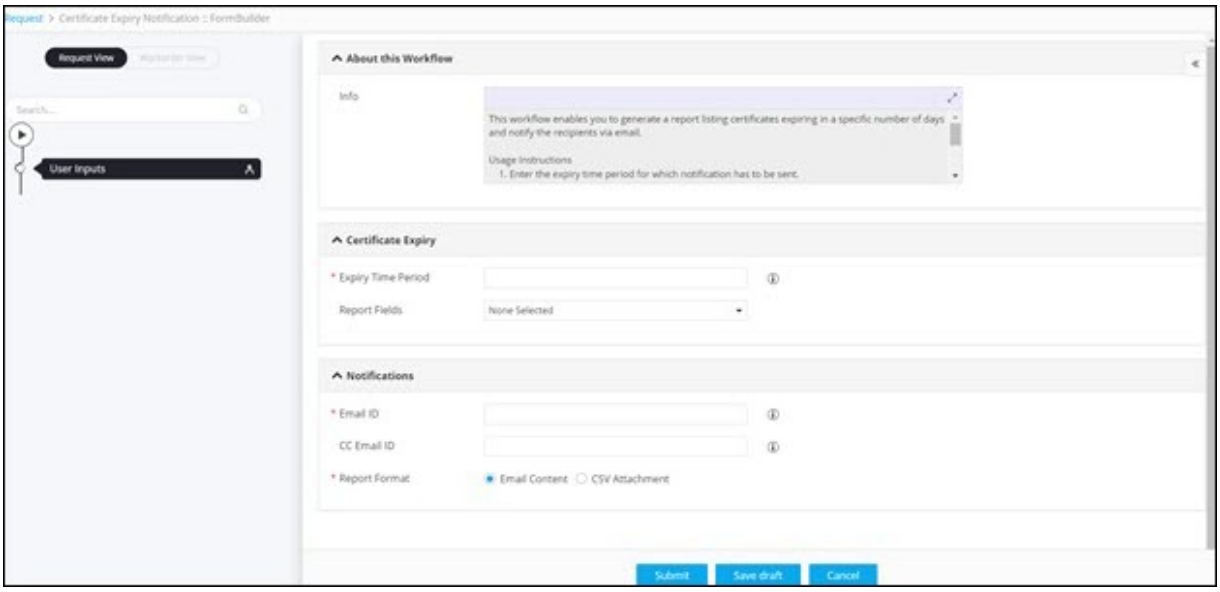
1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification** workflow and click .

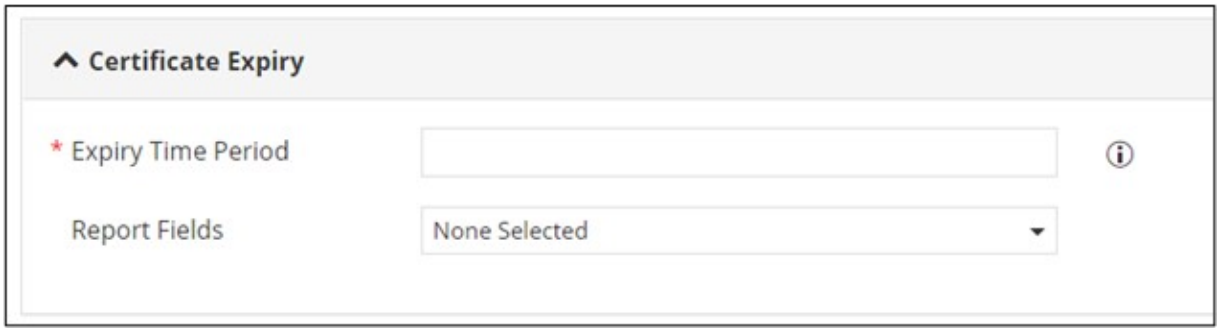


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



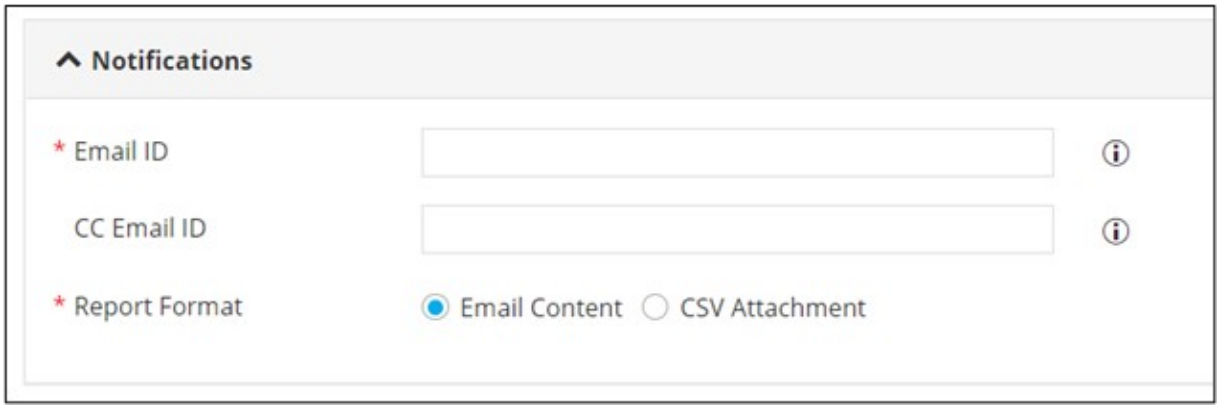
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



The following table describes the fields under the **Certificate Expiry** section:

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

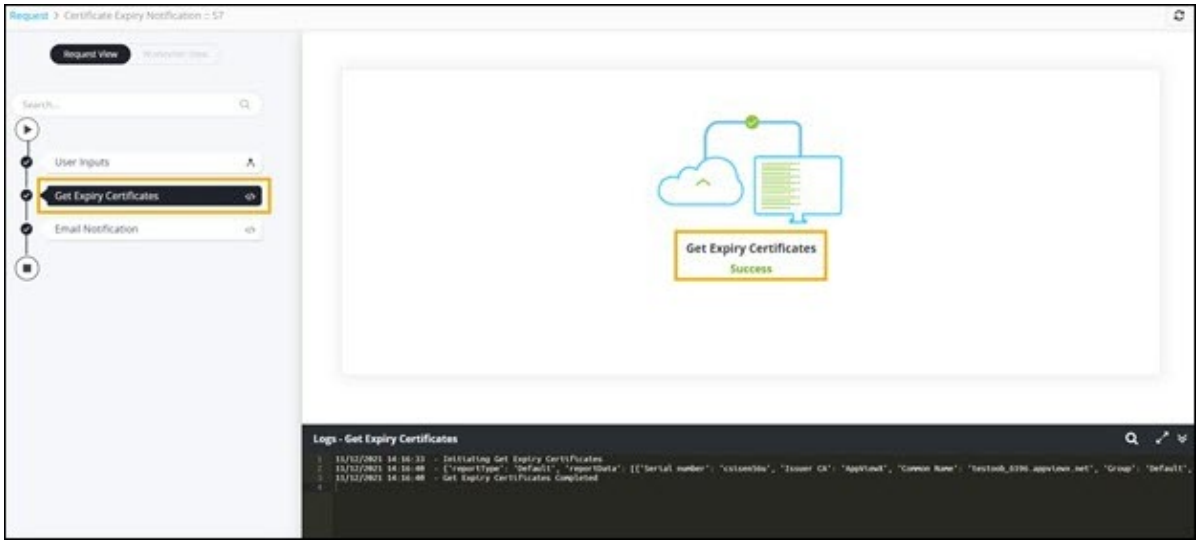
6. Under the **Notifications** section, enter or select the field information as shown.



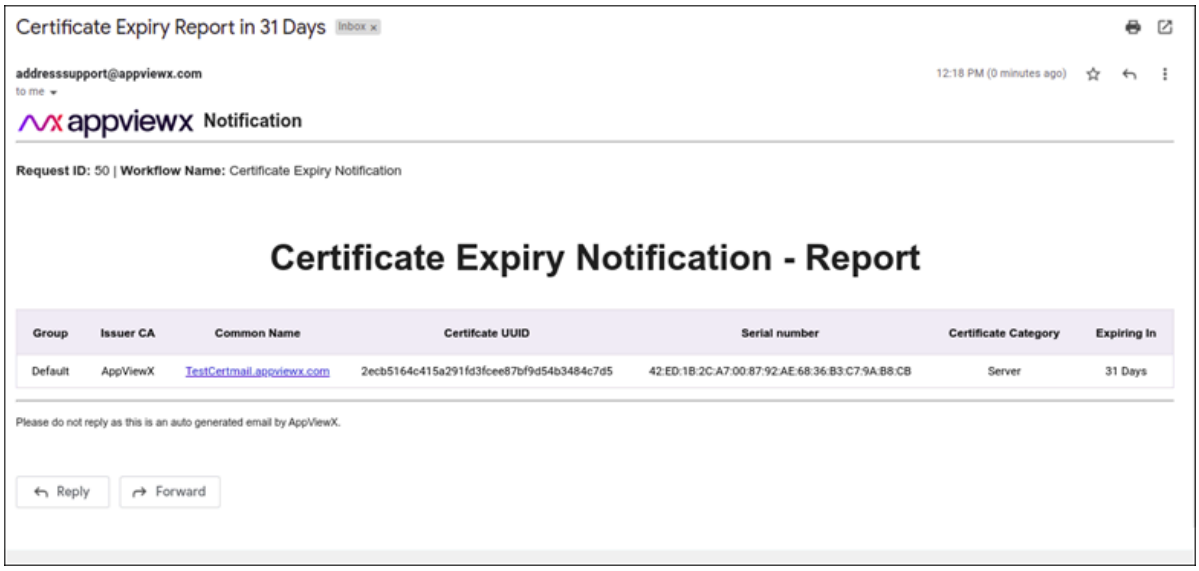
The following table describes the fields under the **Notifications** section:

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma-separated values can be entered for multiple email addresses.
CC Email ID	Enter the email address of the additional recipients in the 'CC' field. Comma-separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content -** The report will be sent as Email content. or • **CSV Attachment -** The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.
   • **Get Expiry Certificates** task is executed.



   • Email notification received with report as email content.

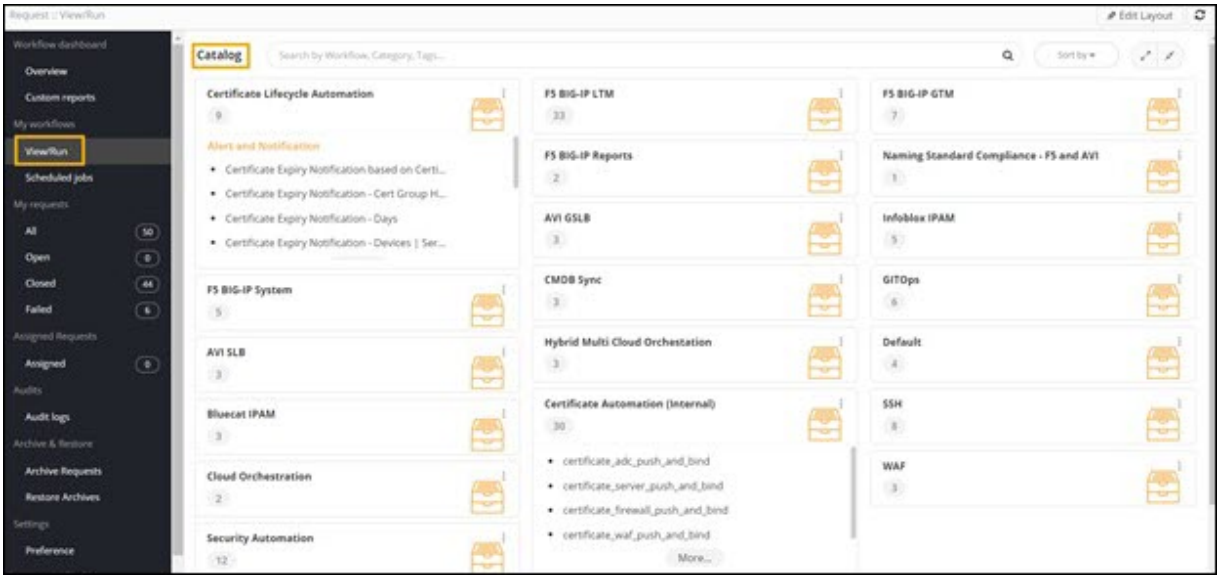


Update Certificate Attributes

This workflow allows you to update the certificate attributes in bulk.

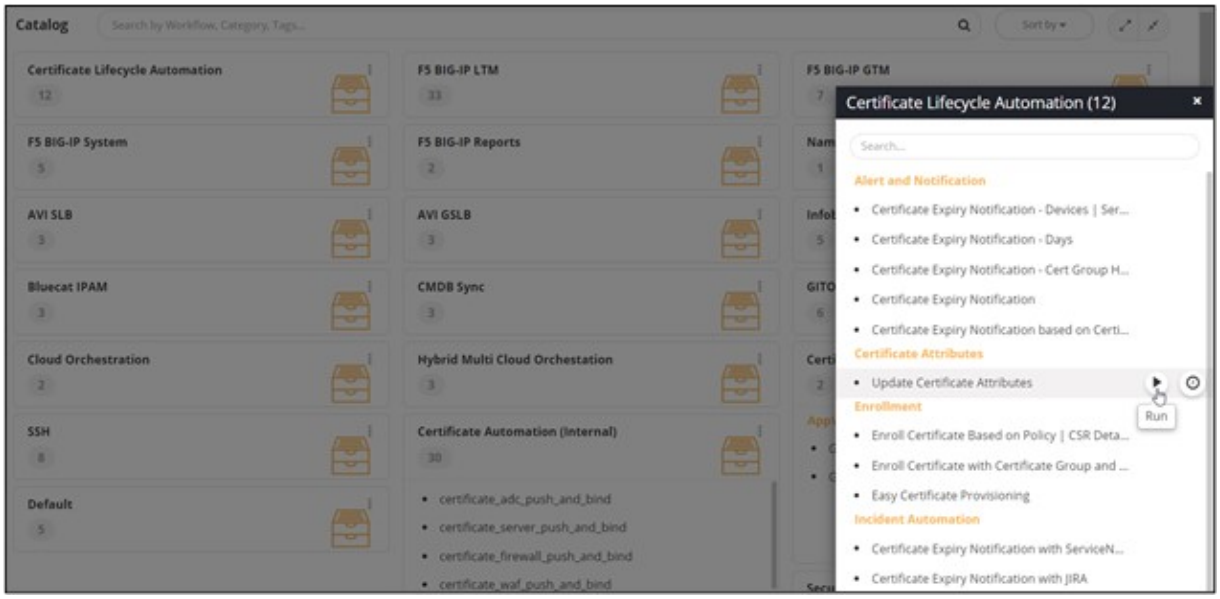
To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.



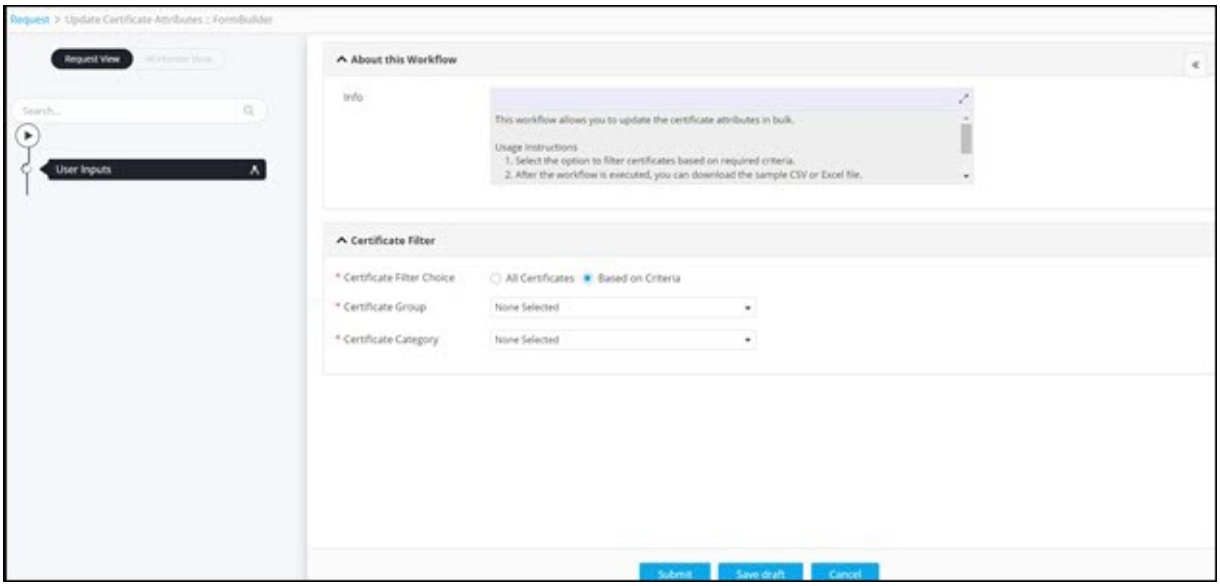
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .

3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Update Certificate Attributes** workflow and click  .



Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



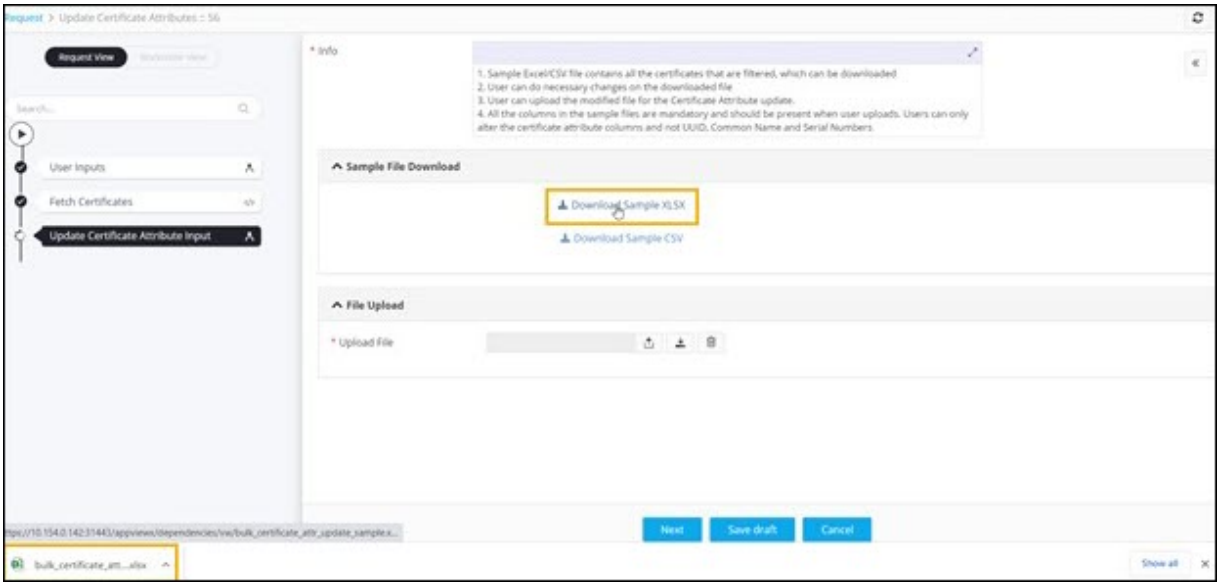
The following table describes the fields in the **Certificate Filter** section:

Field	Description
***Certificate Filter Choice**	Select the required checkbox to fetch • **All certificates** **Note:** This is the default selection. • **Based on Criteria** **Note:** Selecting this option will fetch certificates based on criteria such as certificate group and certificate category.
***Certificate Group**	Select the appropriate certificate group from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
***Certificate Category**	Select the appropriate certificate category from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
All asterisk (*) marked fields are mandatory.	

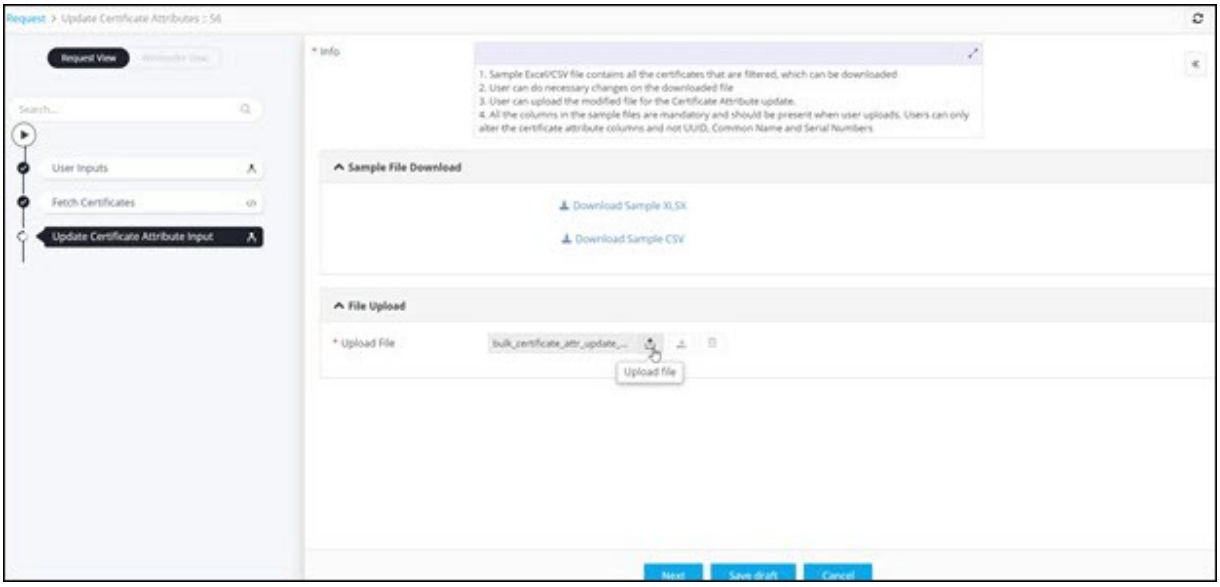
5. Click **Submit**.

   Fetch Certificates task is executed.

6. Select the appropriate option for downloading the file as a CSV or Excel file.
   The file is downloaded to your device.

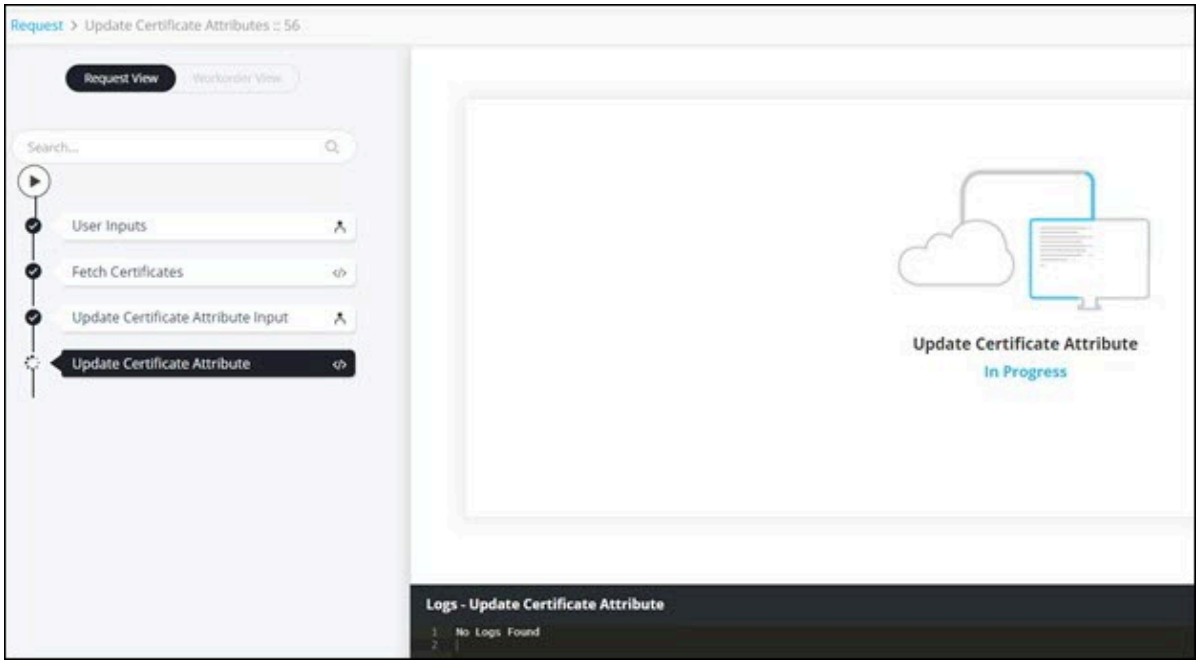


7. Once you have updated the certificate attributes in the downloaded file, under **File Upload**, click  to upload the modified file.

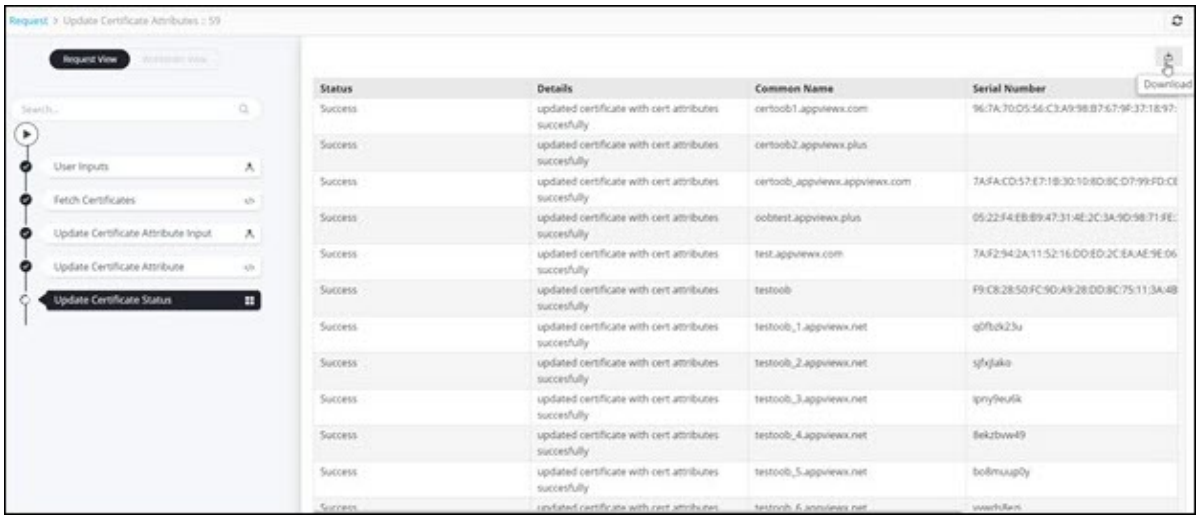


8. Click **Next**
9. In the **Confirmation** pop-up window, click **Ok**.

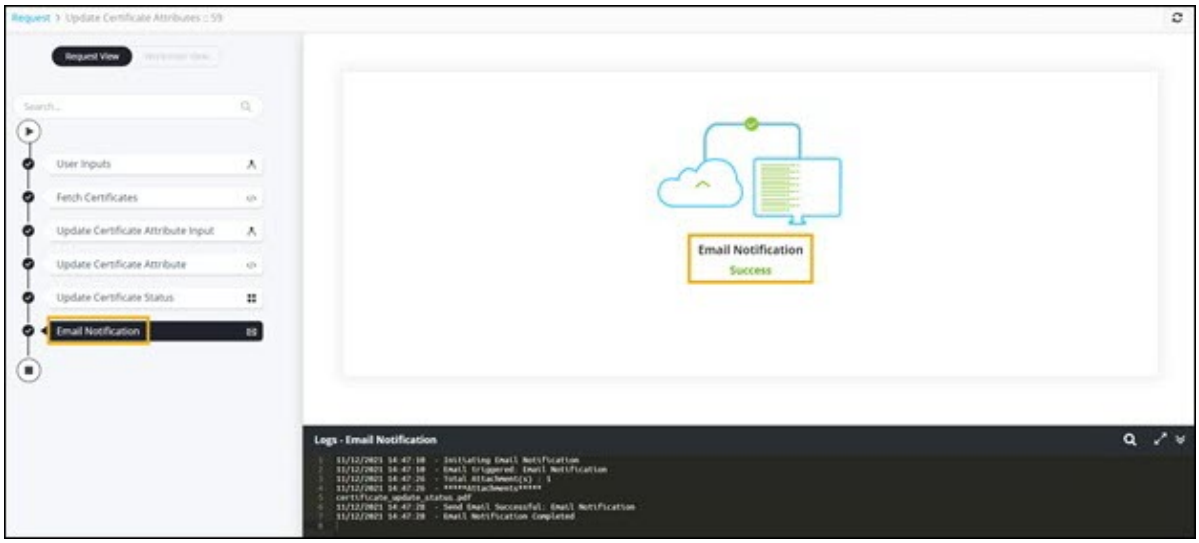
• Update Certificate Attributes task in progress.



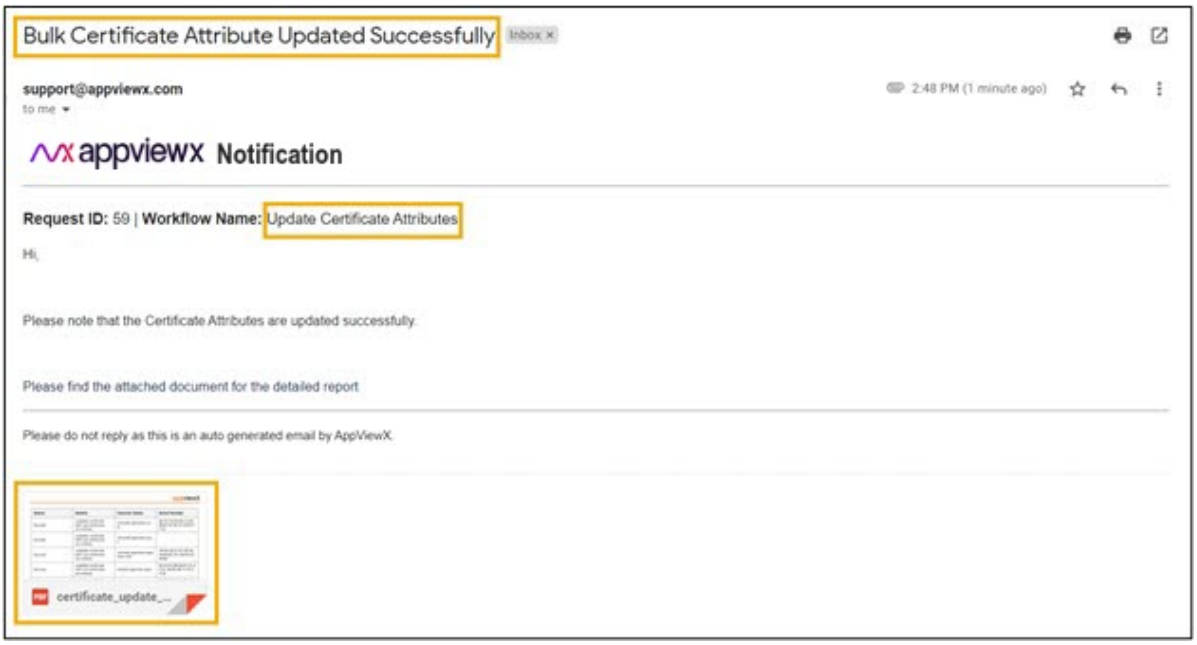
• **Update Certificate Status** is displayed. To download this list, from the top right corner of the screen, click .



• Email notification sent successfully.



- Email with report received.

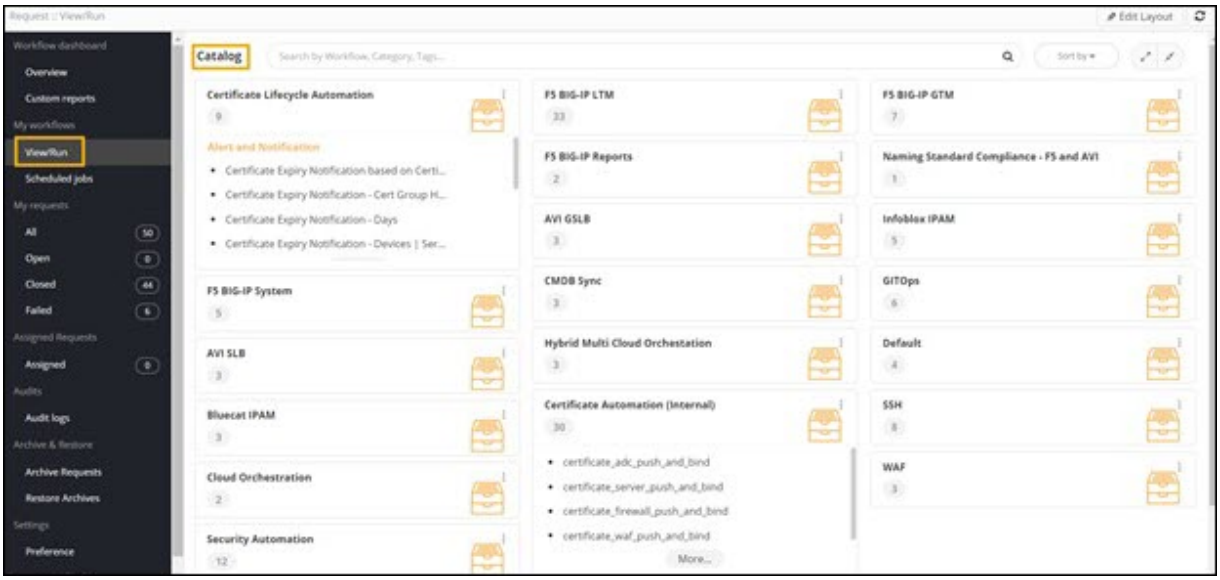


Certificate Expiry Notification with JIRA

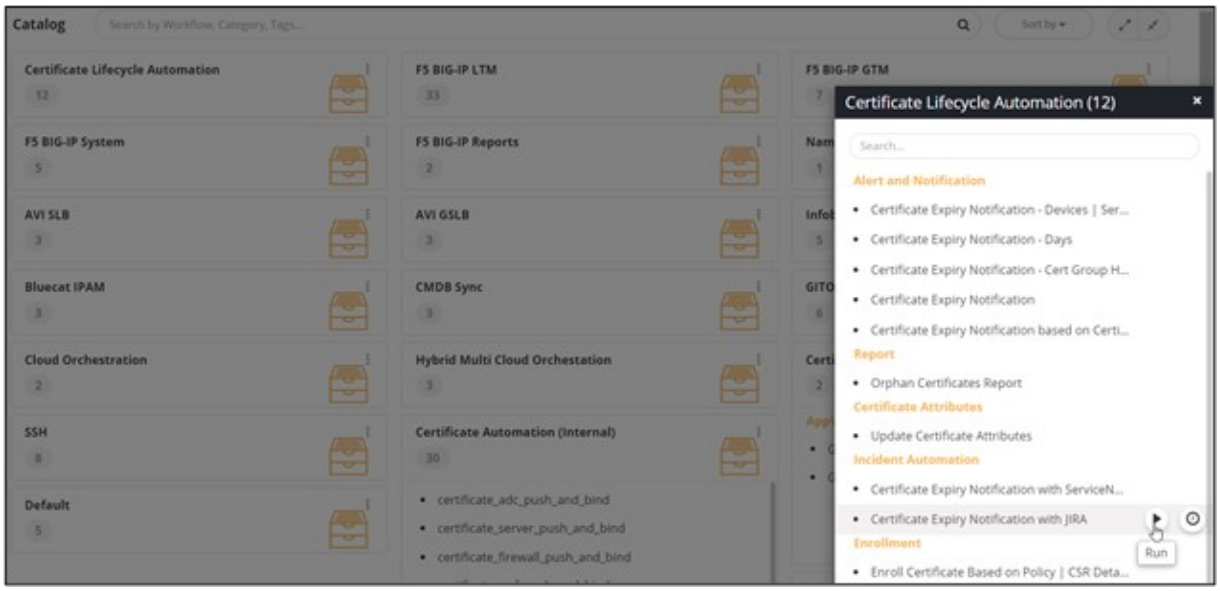
This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

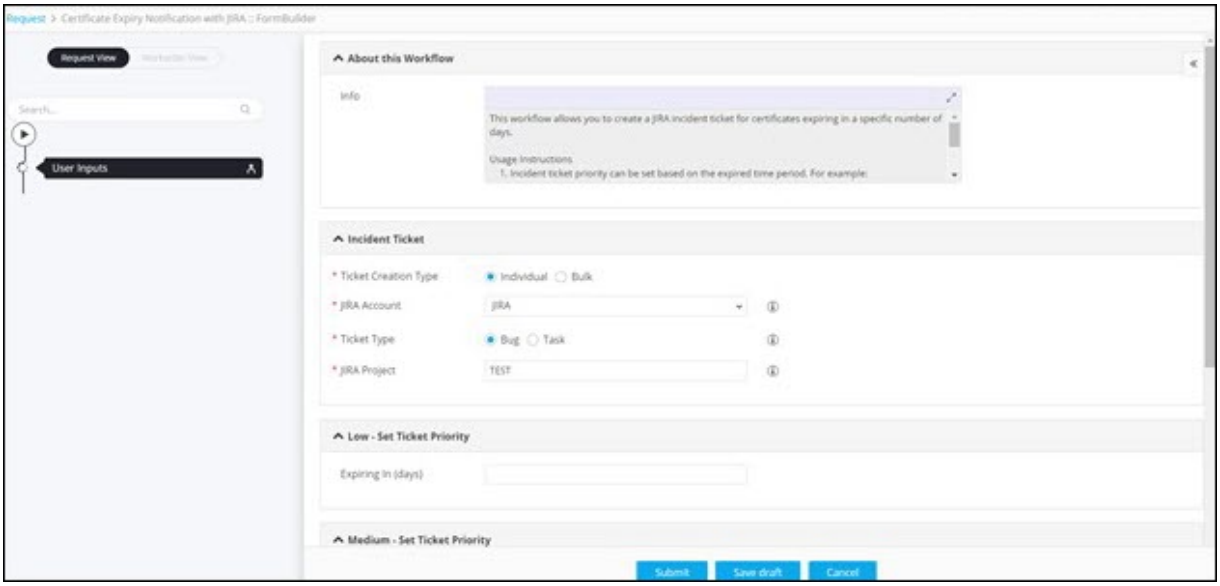


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with JIRA** workflow and click .

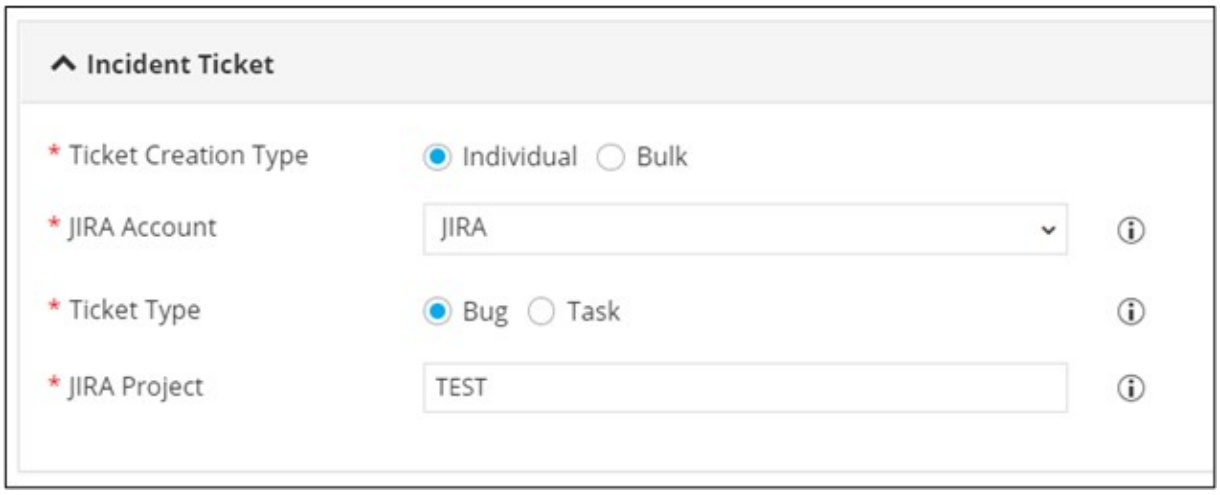


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



5. Under the **Incident Ticket** section, select the field information as shown.



The following table describes the fields in the **Incident Ticket** section:

Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual -** A separate ticket will be created for each certificate. • **Bulk -** A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High.

Field	Description
	Note: Individual is the default selection.
***JIRA Account**	Select the **JIRA Account** as configured in the Integration Hub from the options available in the dropdown. **Note: JIRA** is the default selection.
***Ticket Type**	Select the type of ticket with reference to the project: • **Bug -** This will indicate that the ticket is for a bug in the project. • **Task -** This will indicate that the ticket is for a task in the project. **Note: Bug** is the default selection.
***JIRA Project**	Enter the name of the project for which ticket(s) have to be raised. **Note: Test** is the default selection.
All Asterisk (*) marked fields are mandatory.	

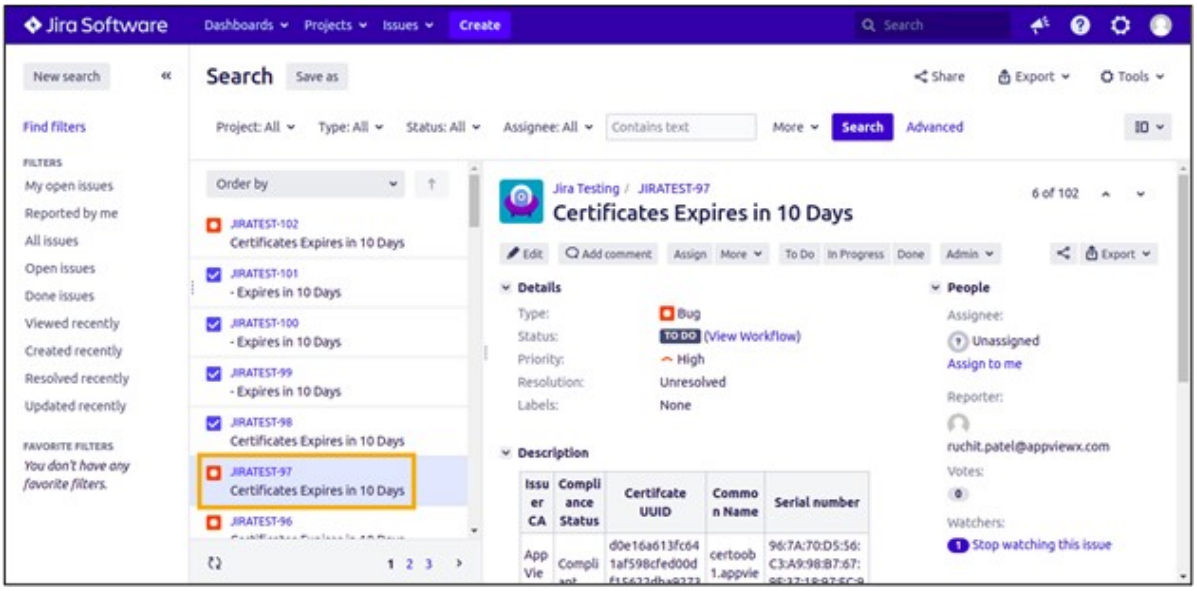
6. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
7. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
8. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
9. Under the **Description Fields** section, select certificate attributes from the dropdown that will be displayed in the JIRA issue description.

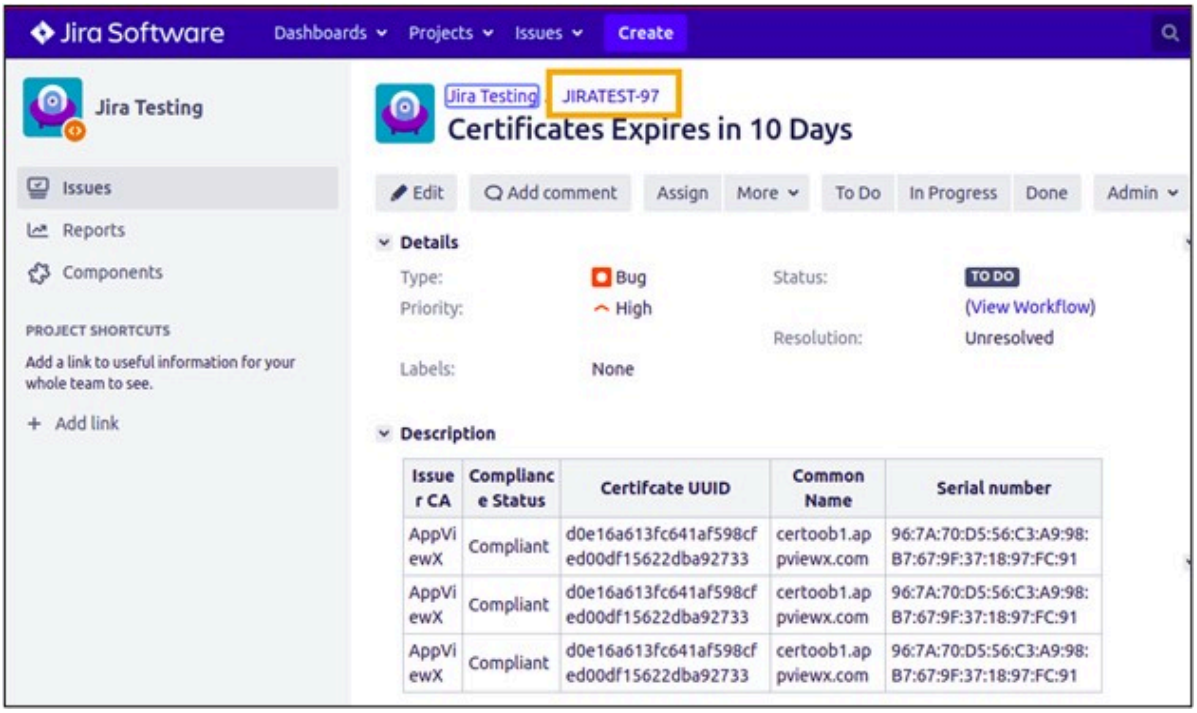
   Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

10. Click **Submit**.

- JIRA ticket creation Summary.

- Ticket created on Jira.



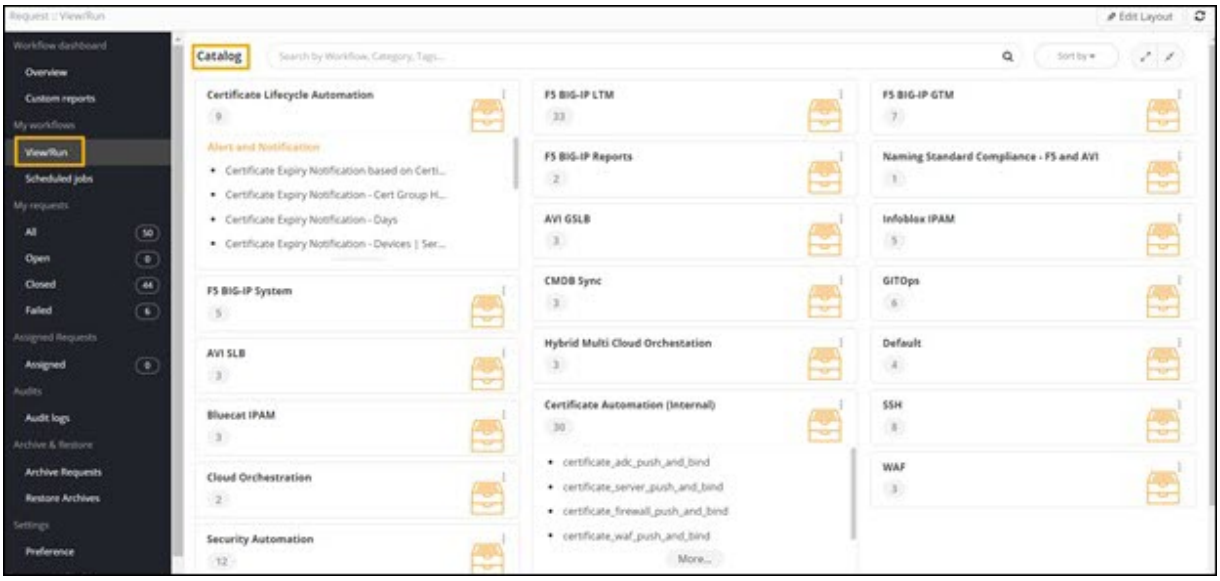


Certificate Expiry Notification with ServiceNow

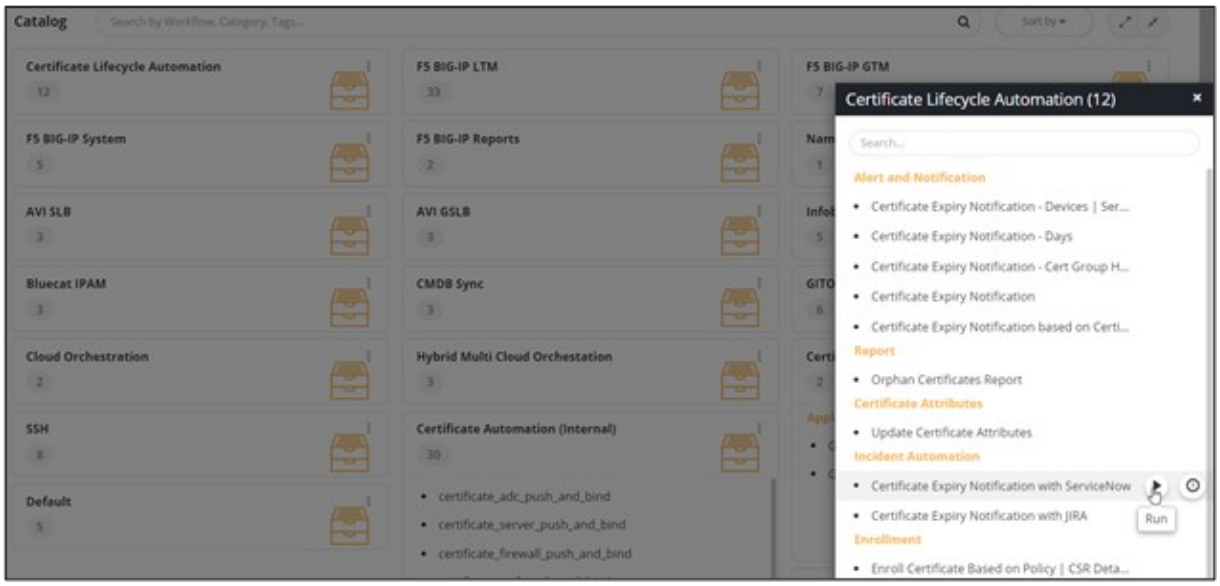
This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

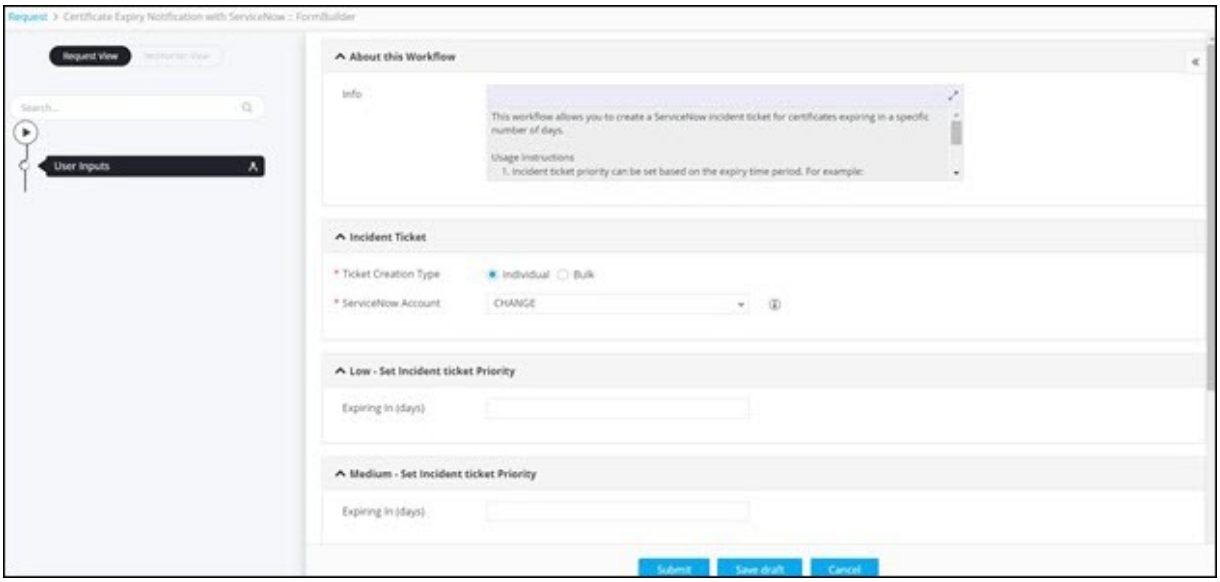


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with ServiceNow** workflow and click .

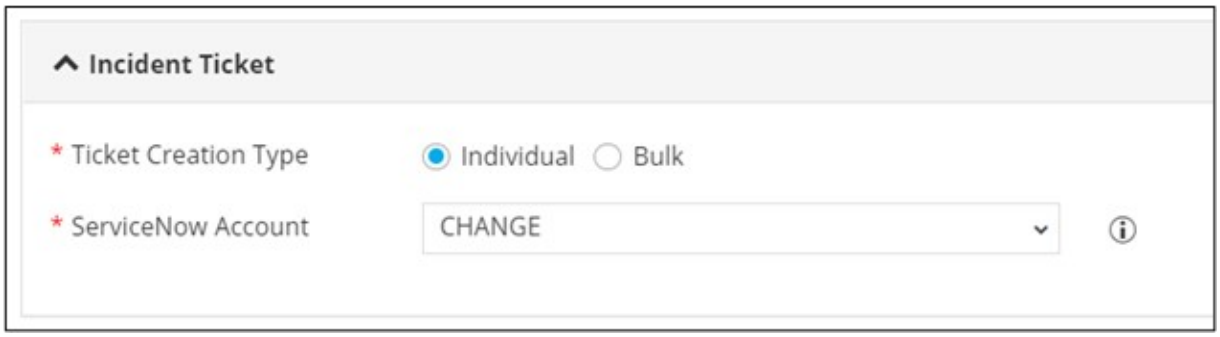


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



5. Under the **Incident Ticket** section, select the field information as shown.



The following table describes the fields in the **Incident Ticket** section:

Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual -** A separate ticket will be created for each certificate. • **Bulk -** A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High. **Note: Individual** is the default selection.
***ServiceNow Account**	Select the **ServiceNow Account** as configured in the Integration Hub from the options available in the dropdown.

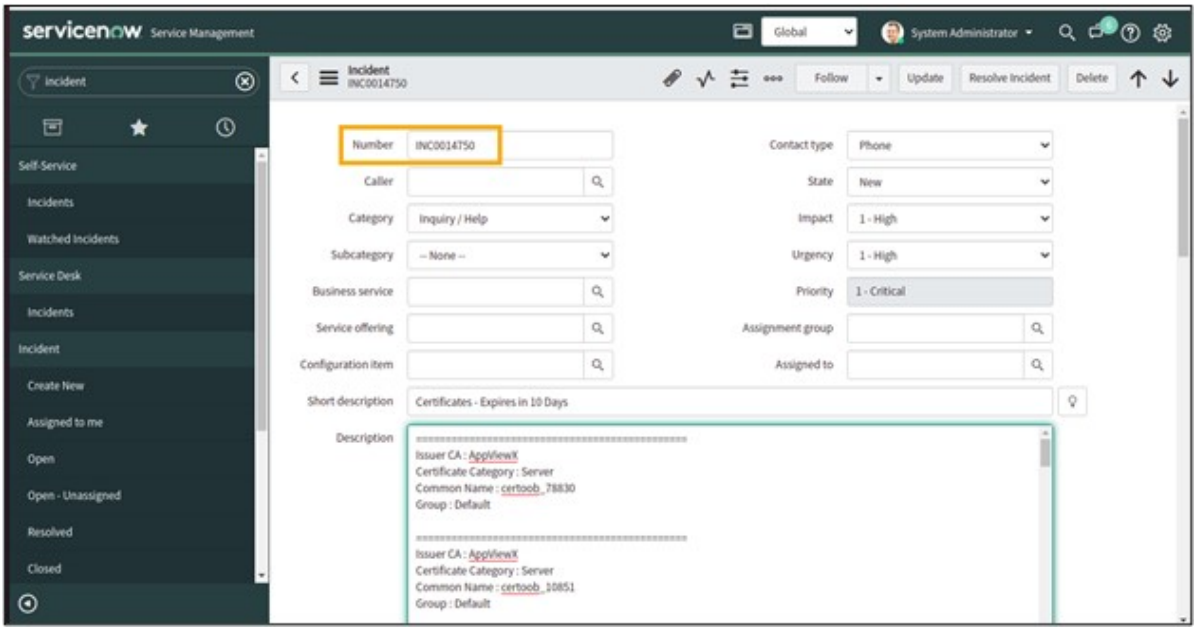
Field	Description
	Note: Change is the default selection.
All Asterisk (*) marked fields are mandatory.	

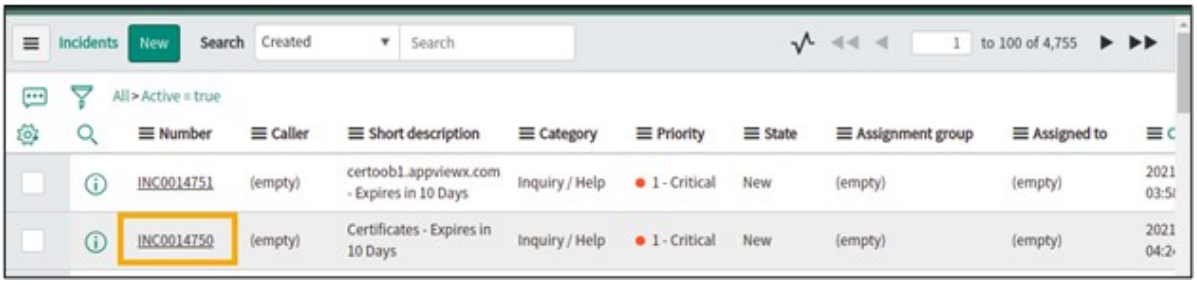
6. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
7. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
8. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
9. Under the **Description Details** section, select multiple certificate attributes from the dropdown that will be displayed in the ServiceNow description.

Note: This is a mandatory field.

10. Click **Submit**.
    - Incident Creation Summary

    - Incident ticket created on ServiceNow.



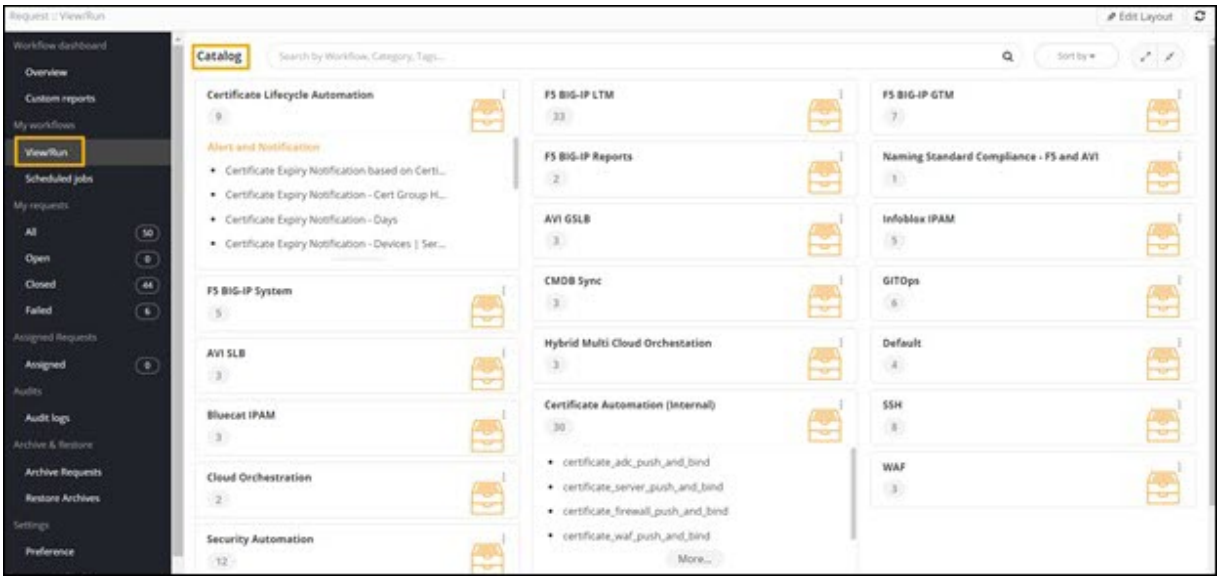


Orphan Certificates Report

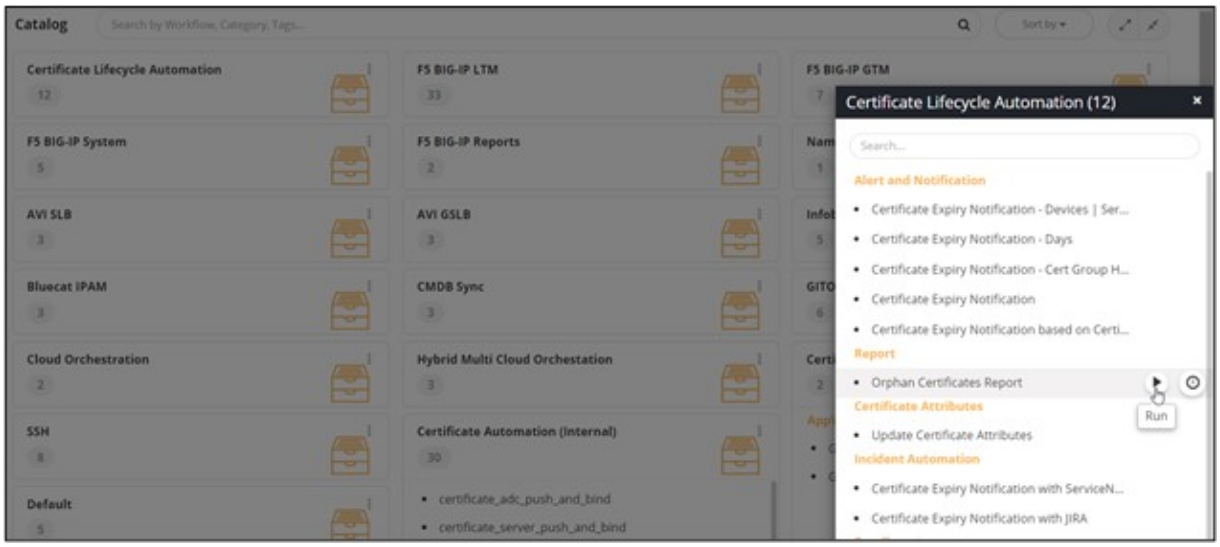
This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

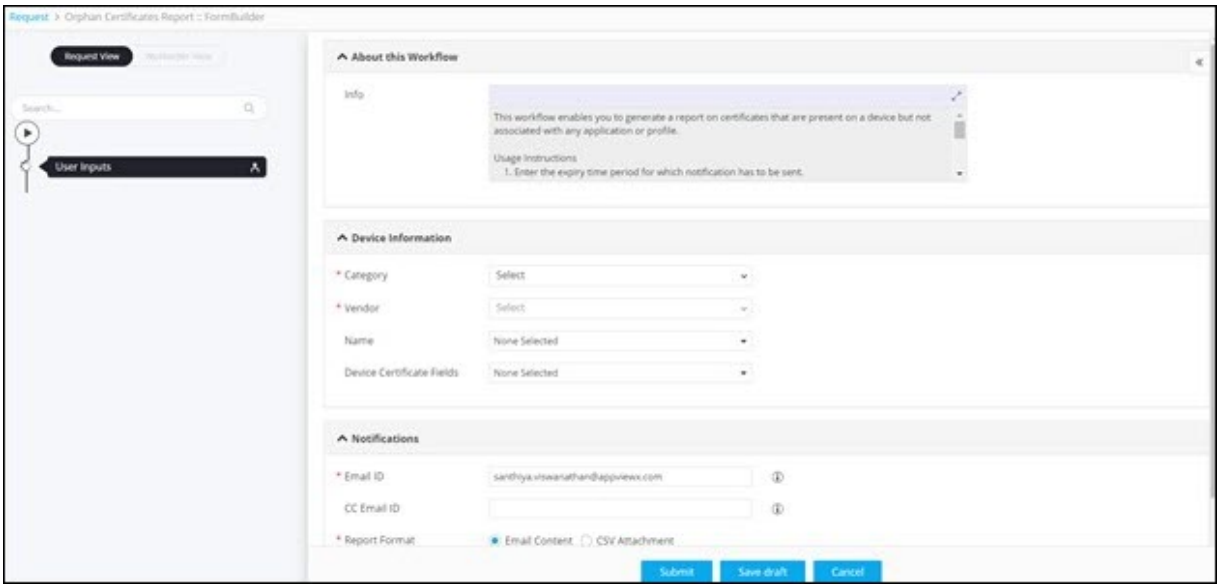


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Report** category, hover your mouse over the **Orphan Certificates Report** workflow and click .

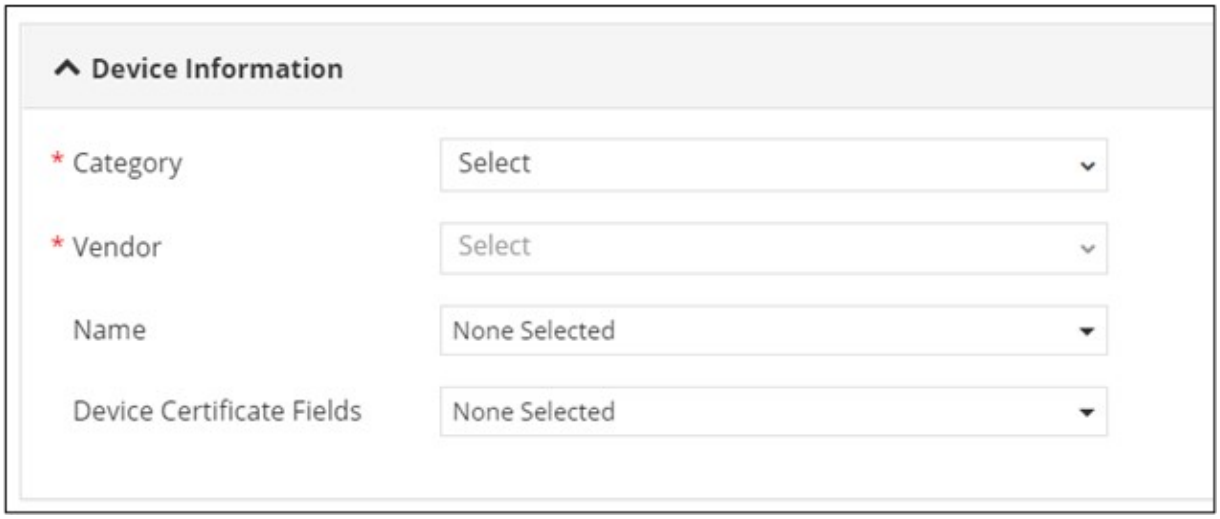


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow is executed with the workflow inputs requested at the first stage.



5. Under the **Device Information** section, enter or select the field information as shown.

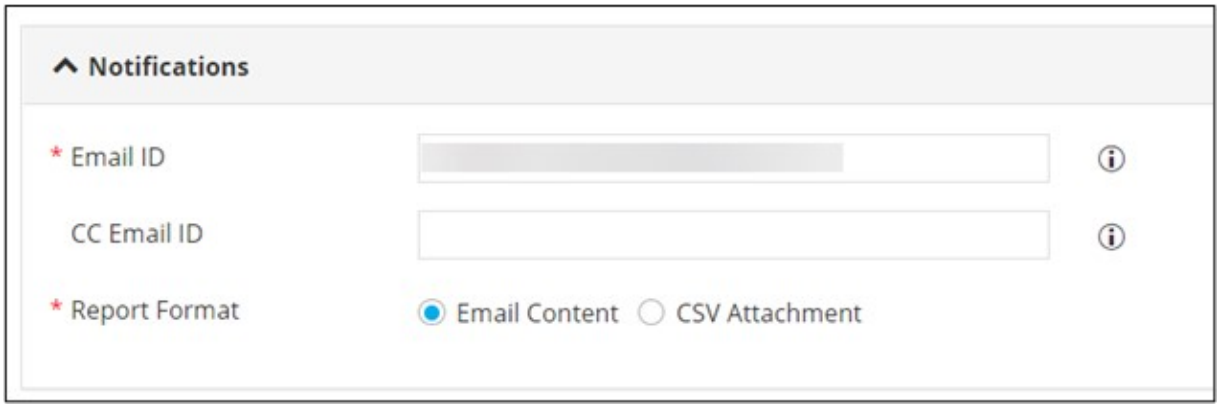


The following table describes the fields in the **Device Information** section:

Field	Description
***Category**	Select the device category for the report from the options available in the dropdown.
***Vendor**	Select the device vendor for the report from the options available in the dropdown.
Name	Select the specific device for the report.

Field	Description
Device Certificate Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

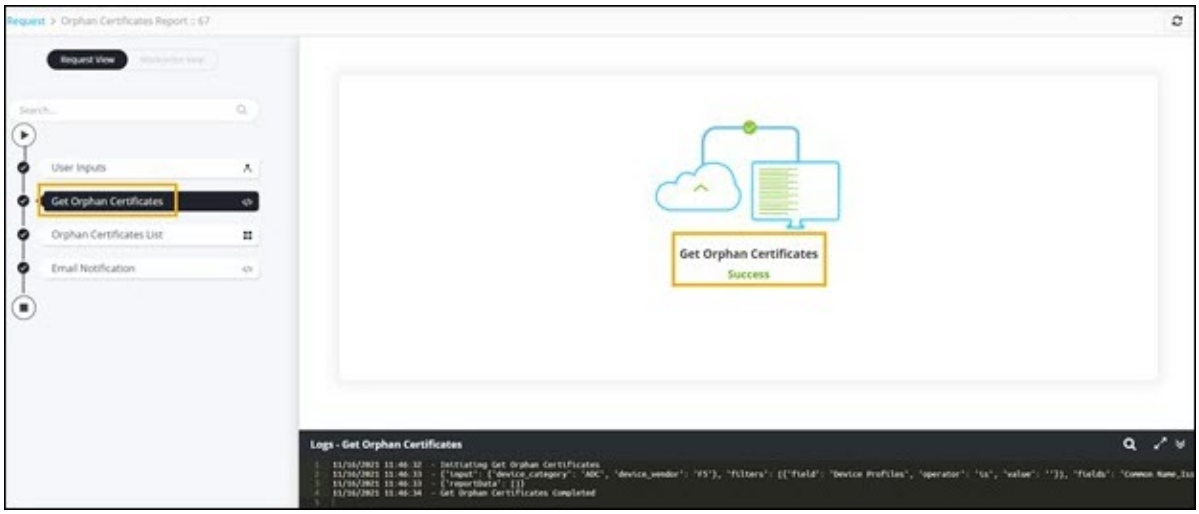
6. Under the **Notifications** section, enter or select the field information as shown.



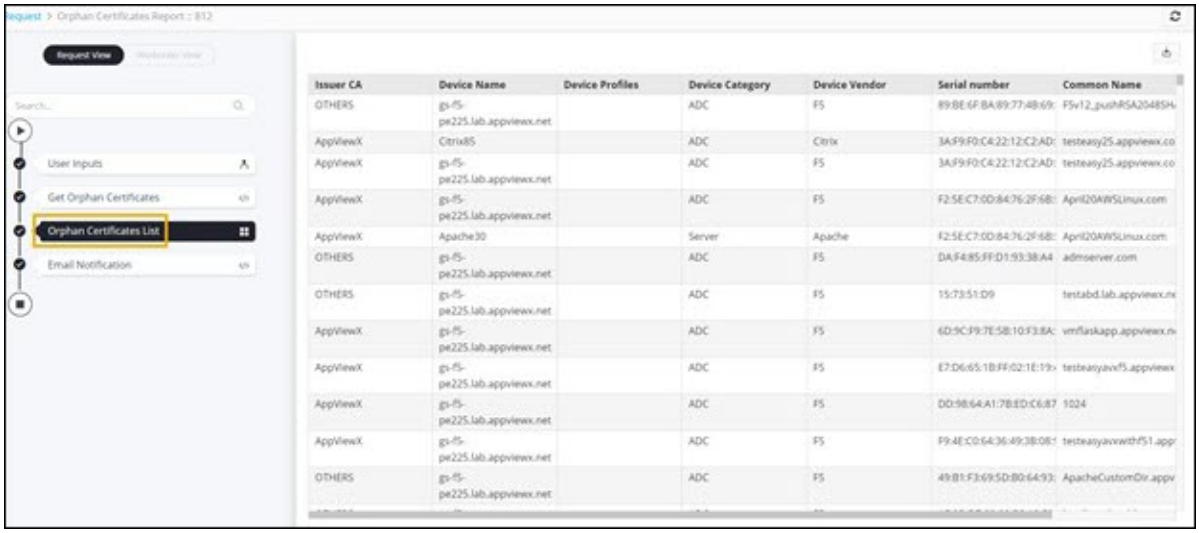
The following table describes the fields in the **Notifications** section:

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content -** The report will be sent as Email content. or • **CSV Attachment -** The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.
   - Get Orphan Certificates task executed.



   - Orphan Certificates List generated.



   - Email notification received with report as email content.

Chapter 6: Create Certificate Workflows

Overview

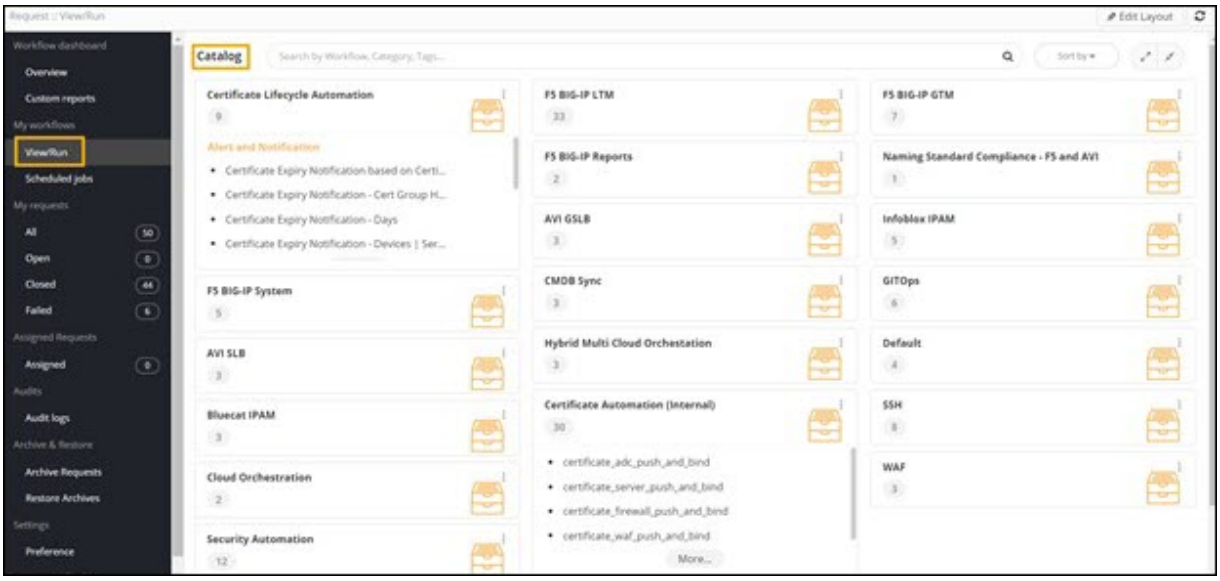
This section lists and describes the workflows that can be used to enroll certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Enrollment with Incident Automation.

Enroll Certificate and Download

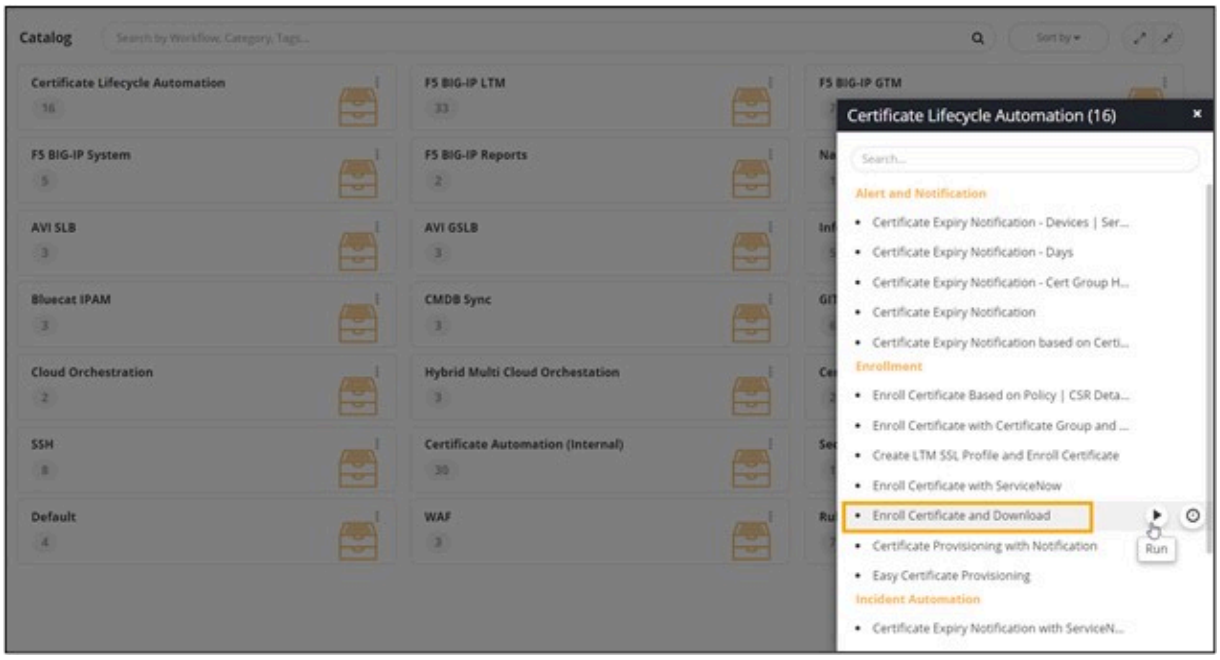
This workflow enables you to create and download certificates based on the certificate group.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

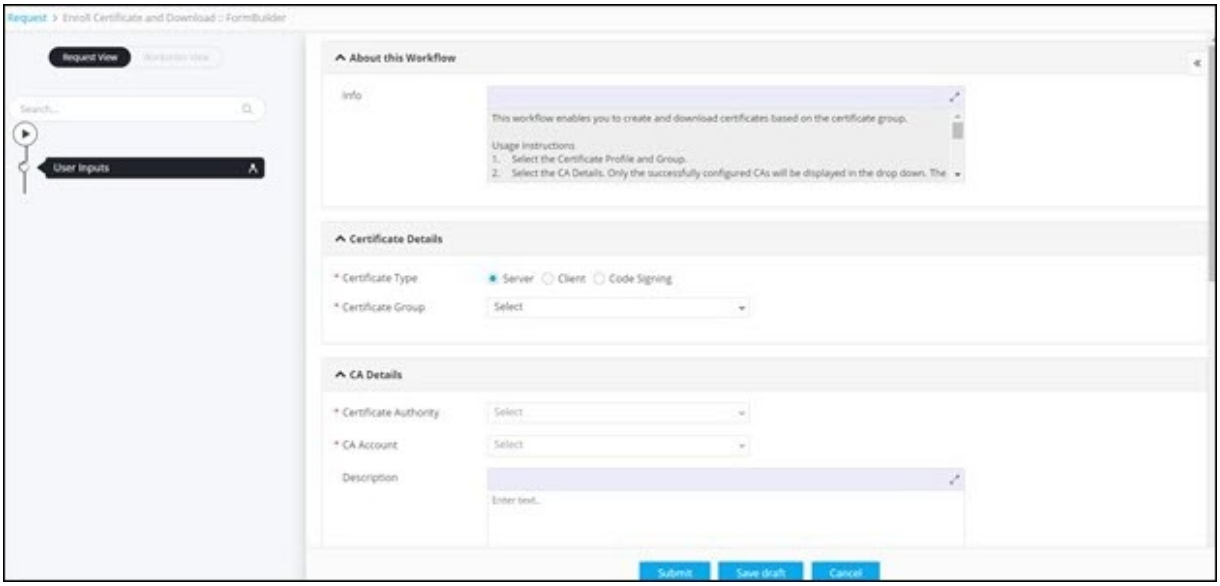


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Download** workflow and click .

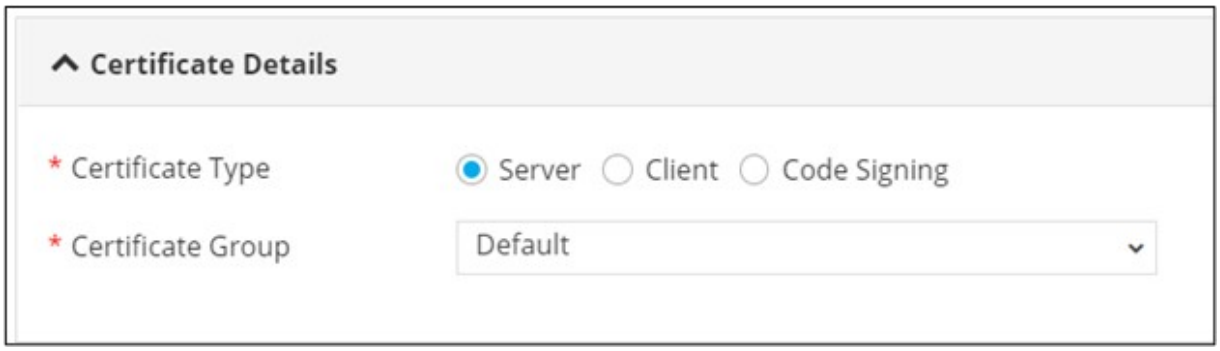


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **Certificate Details** section, select the field information as shown.

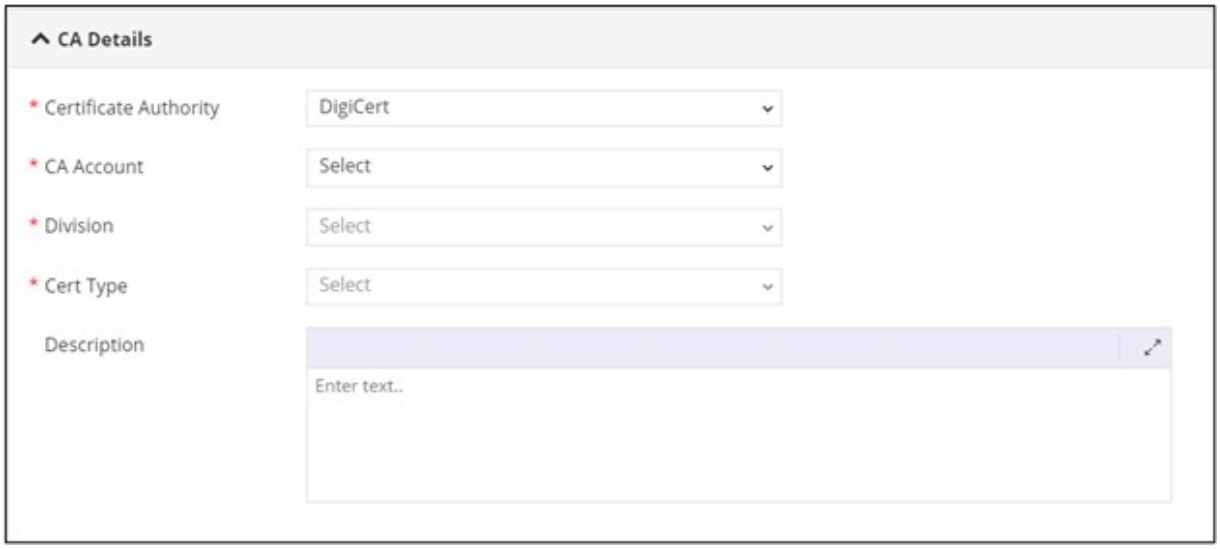


The following table describes the field information under the **Certificate Details** section:

Field	Description
***Certificate Type**	Select the required **Certificate Type** from the available options: • **Server** • **Client** • **Code Signing** **Note**: **Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.

Field	Description
All asterisk (*) marked fields are mandatory.	

6. Under the **CA Details** section, enter or select the field information as shown.

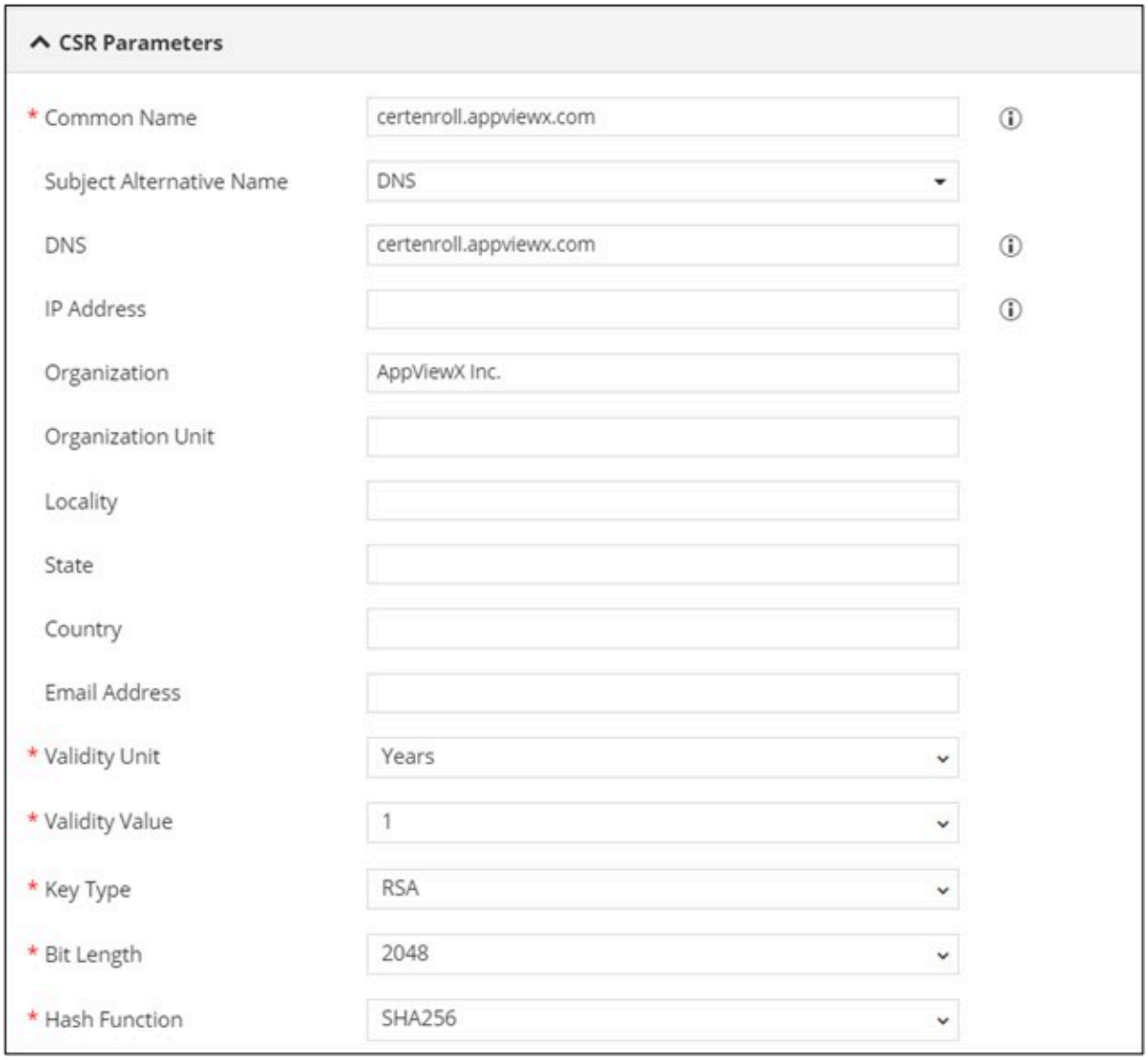


The following table describes the field information under the **CA Details** section:

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note**: This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown.

Field	Description
	Note: This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Provide a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

7. Under the **CSR Parameters** section, enter or select the field information as shown.

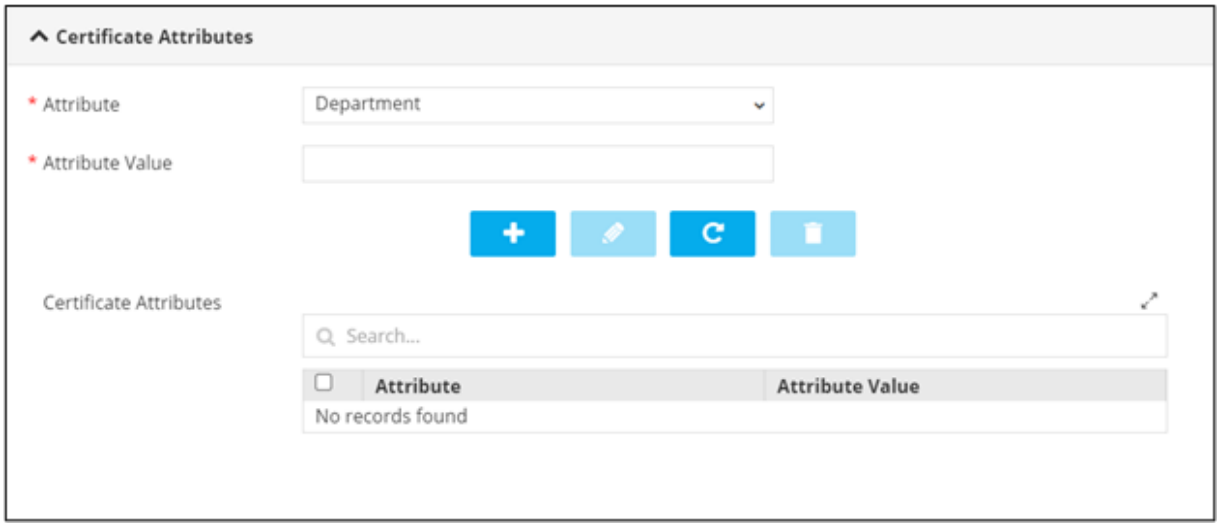


The following table describes the fields under the **CSR Parameters** section:

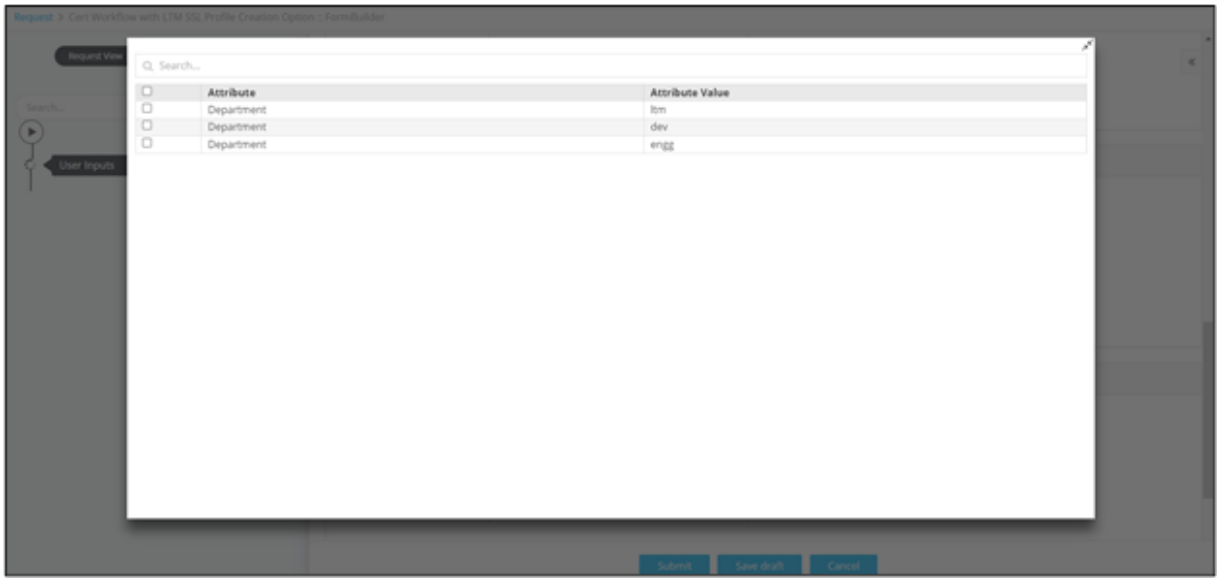
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS, if you select the **DNS** option in the **SAN** field.

Field	Description
IP Address	Enter a valid IP address, if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.  **Note:** This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.



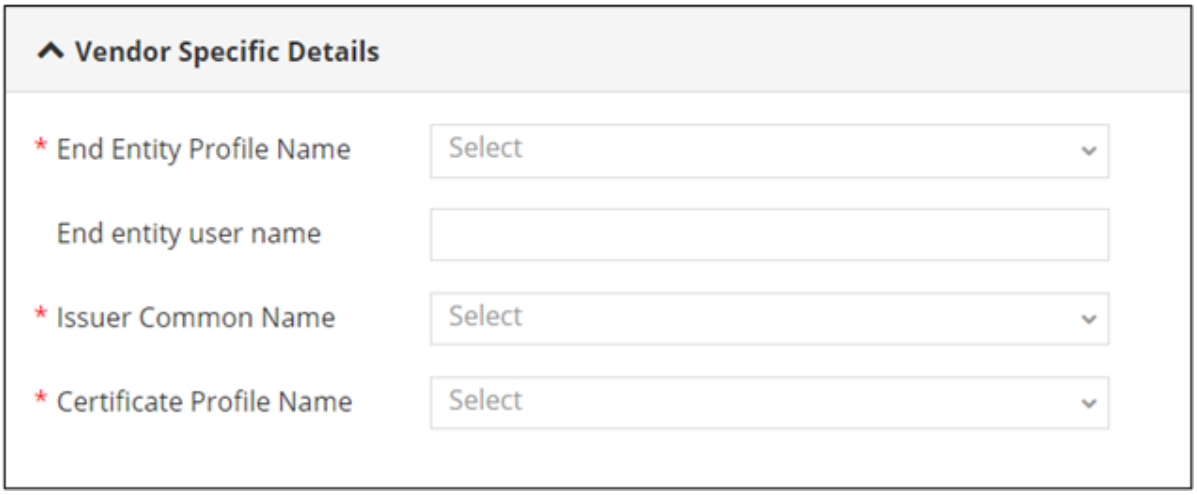
10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



15. To search for a particular attribute in the grid, type the keyword(s) in the search field.

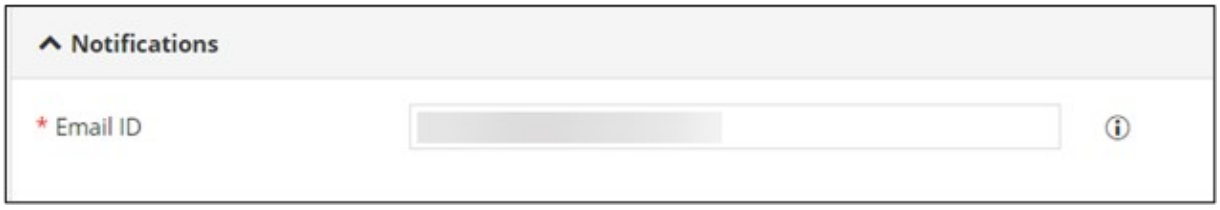
16. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



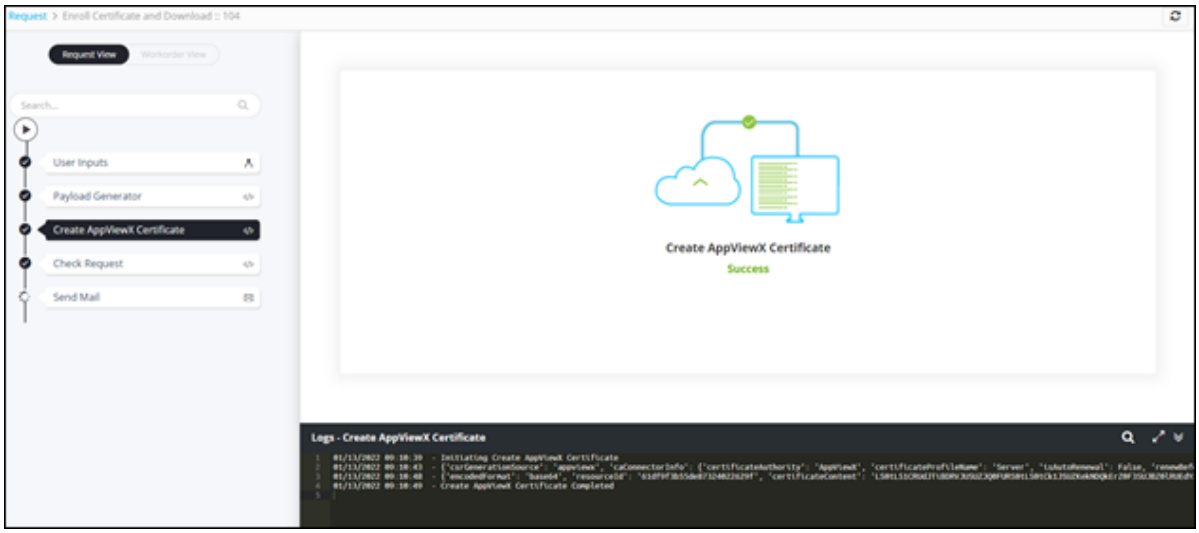
> **Note:** The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

17. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



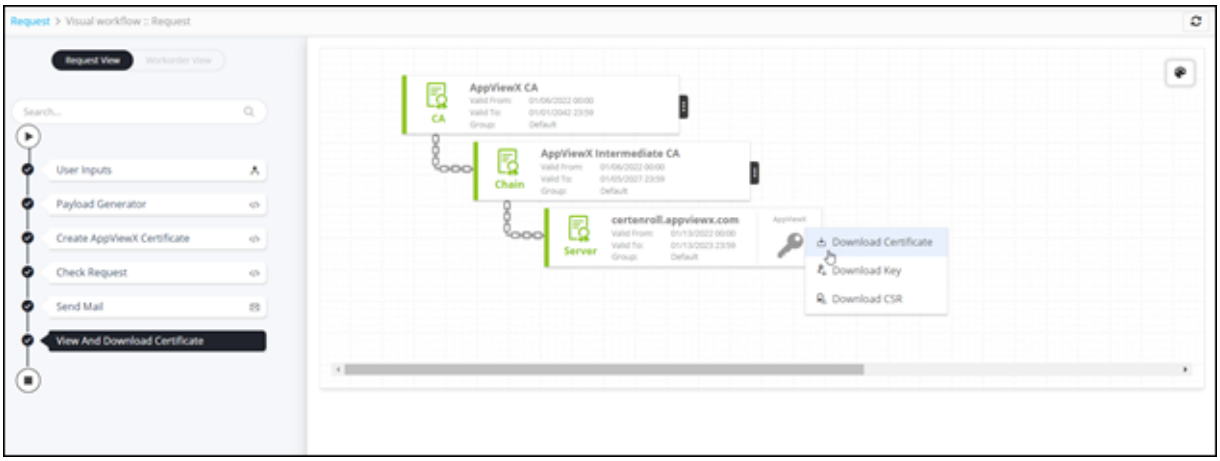
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

18. Click **Submit**.
    - Certificate created successfully.

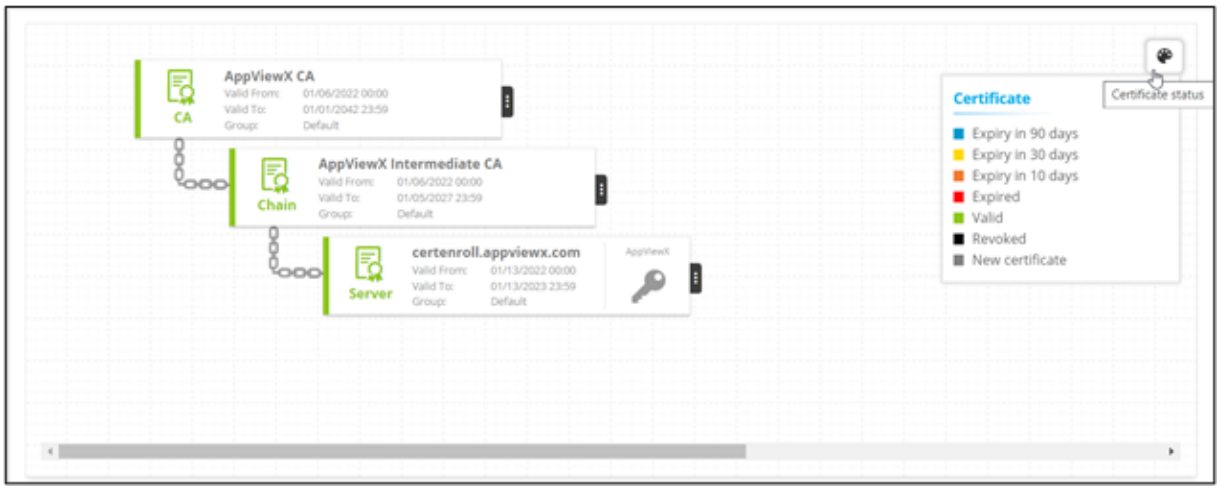


    - Email notification received.

19. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.



20. Hover your mouse over  to view the Certificate status.

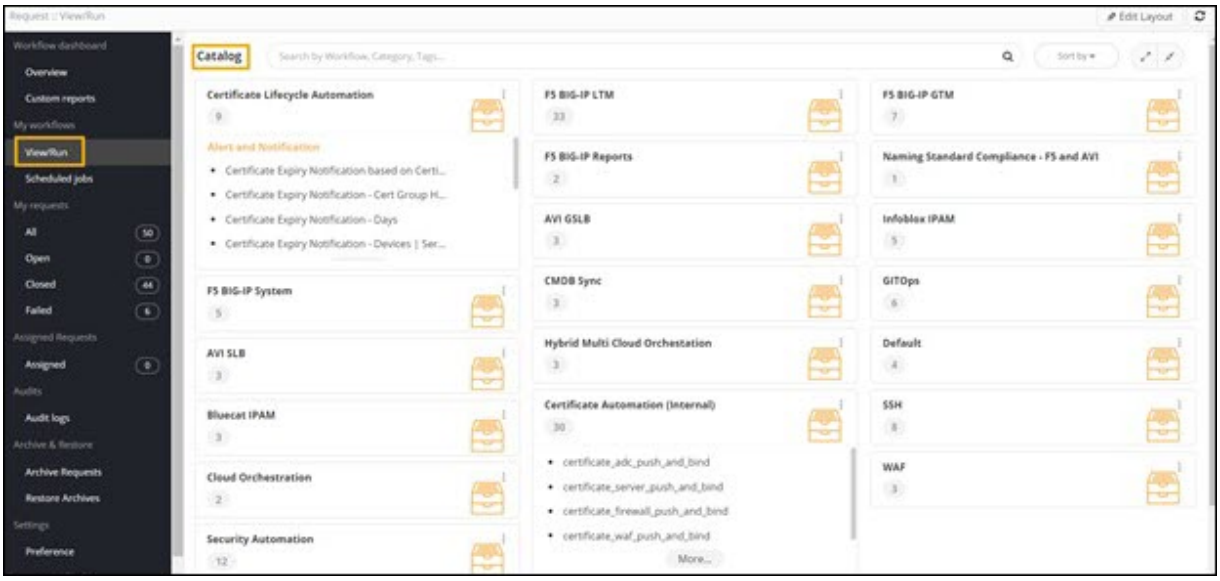


Certificate Provisioning with Notification

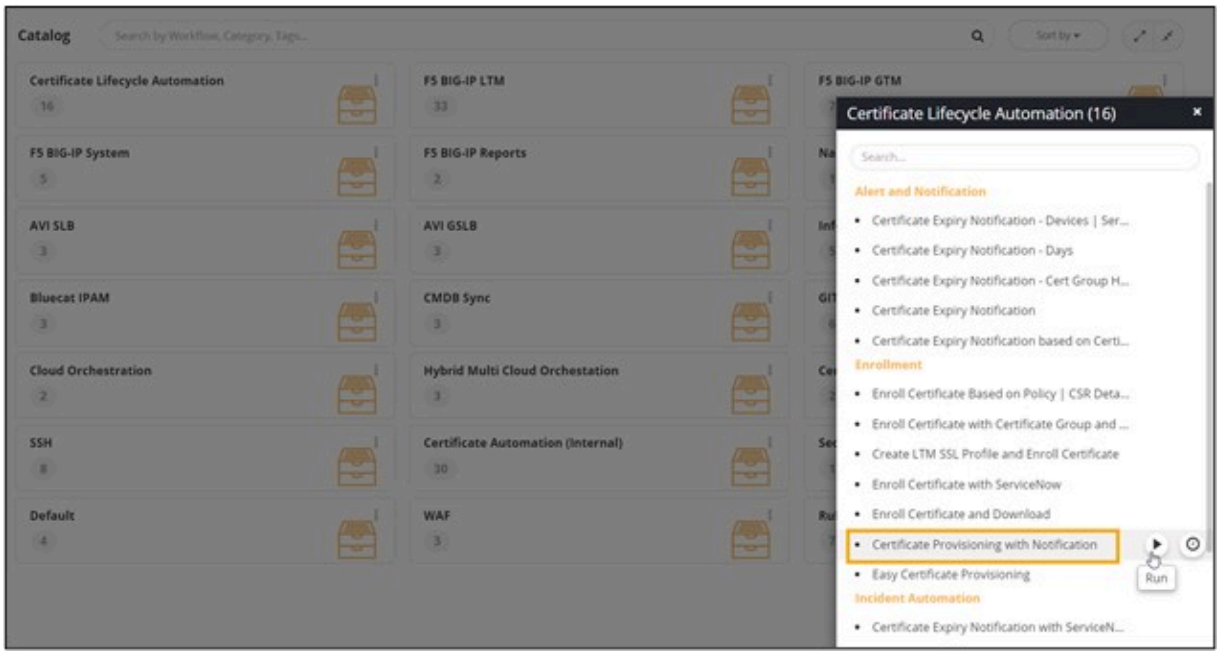
This workflow allows you to create a certificate based on the certificate group and the policy associated with it, and push to a device available in the instance. Email approval is required for certificate creation as well as pushing it to the device. Once approved, the logged in user will receive an email informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

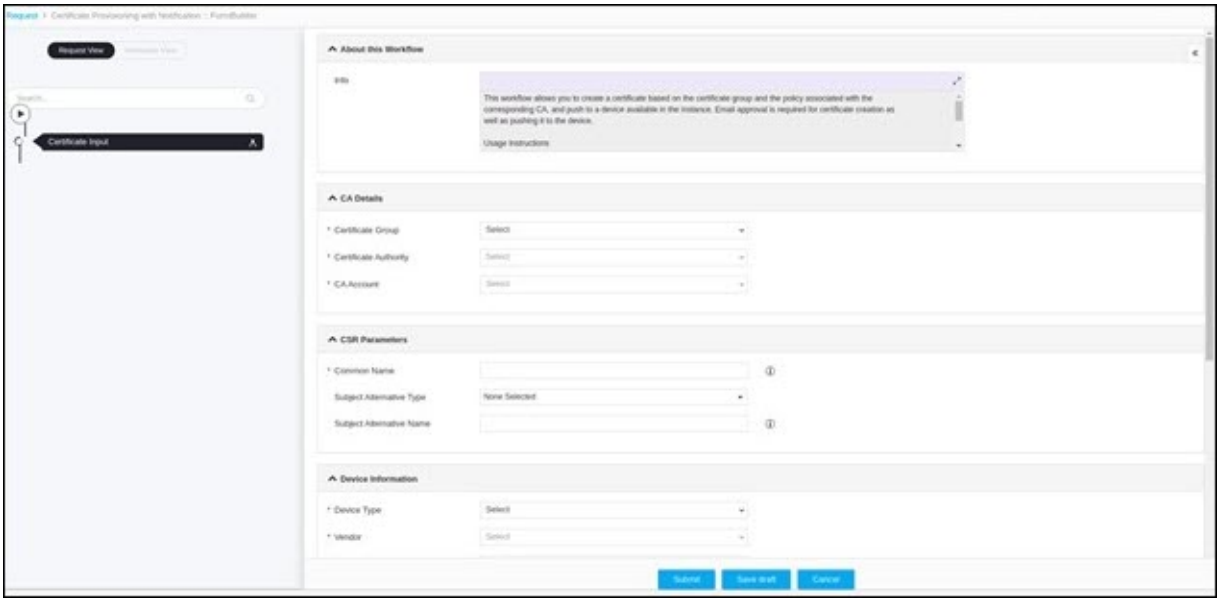


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Certificate Provisioning with Notification** workflow and click .

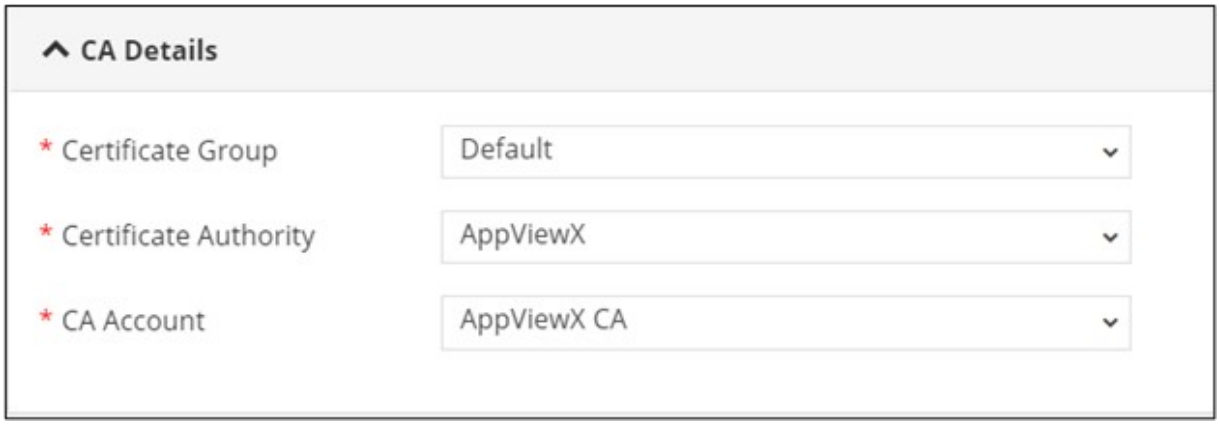


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **CA Details** section, select the field information as shown.



The following table describes the field information under the **CA Details** section:

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Ebtrust • EJBCA

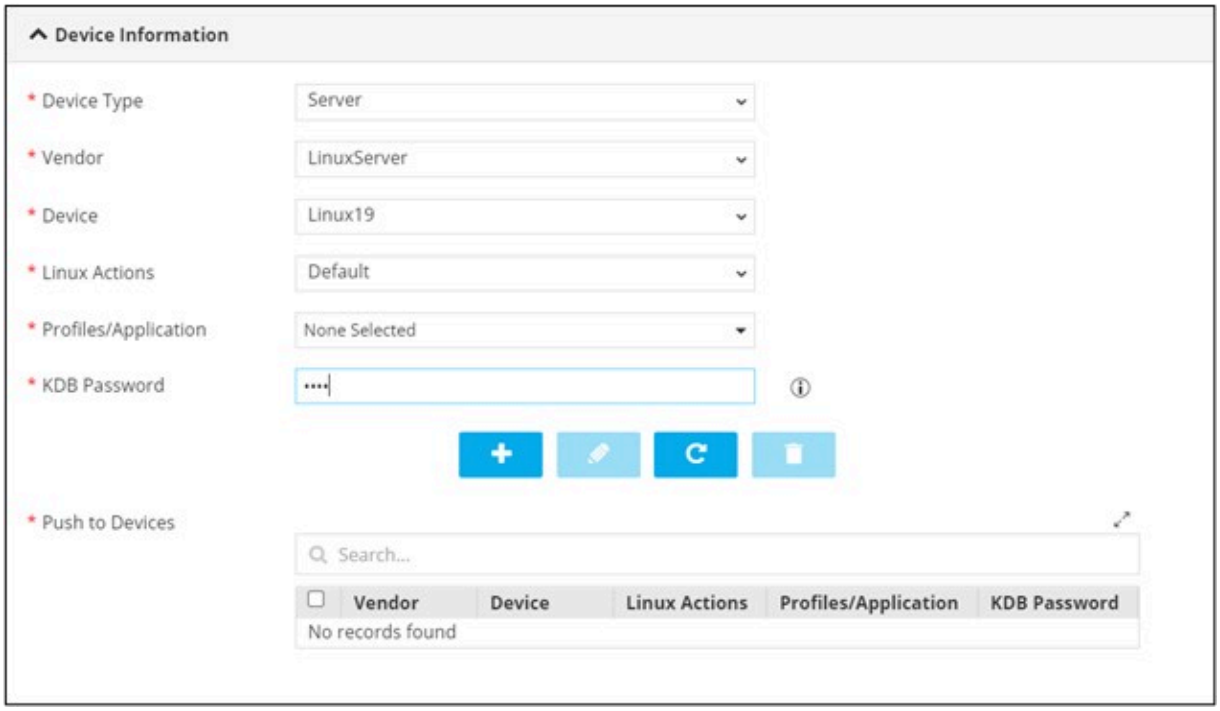
Field	Description
	• Microsoft Enterprise • AppViewX **Note:** This field is populated based on the selected **Certificate Group**.
CA Account	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **CA**selected .
All asterisk (*) marked fields are mandatory.	

6. Under the **CSR Parameters** section, enter or select the field information as shown.

The following table describes the fields under the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Type	Select the Subject Alternative Type from the available options: • DNS • IP Address
Subject Alternative Name	Enter a valid Subject Alternative Name.
All Asterisk (*) marked fields are mandatory.	

7. Under the **Device Information** section, select the field information as shown.



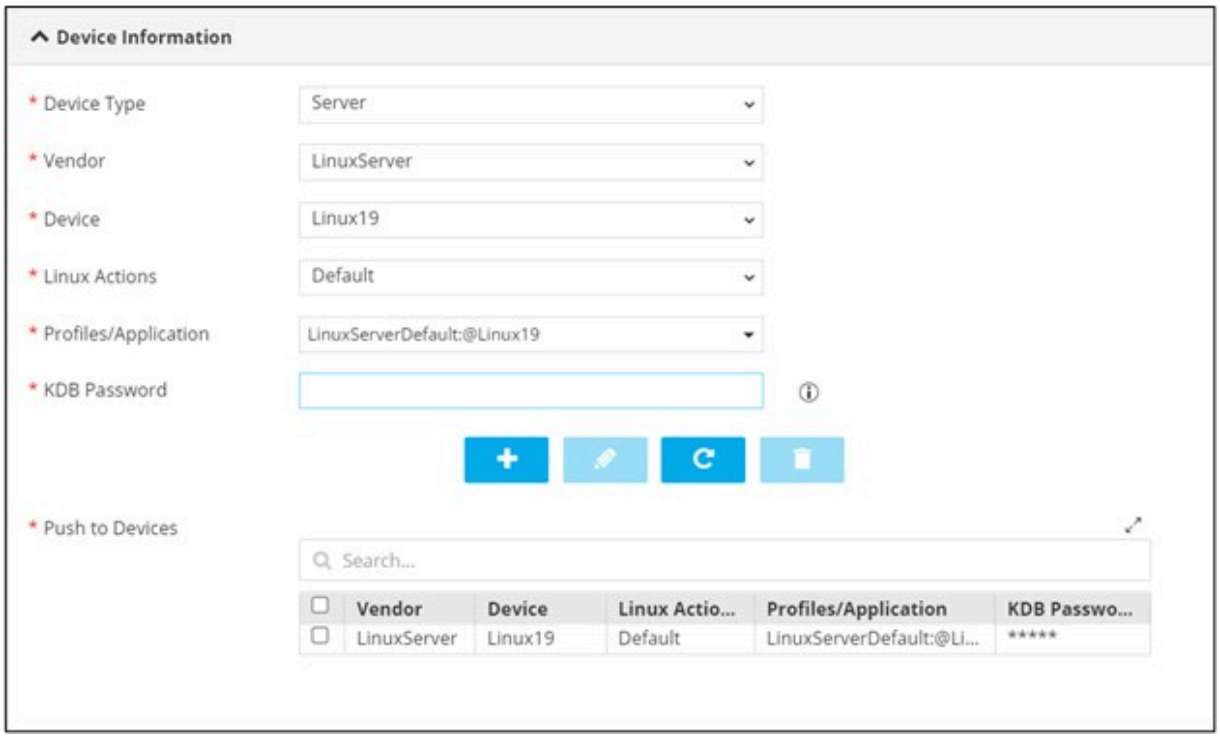
The following table describes the field information in the **Device Information** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown.

Field	Description
	Note: The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

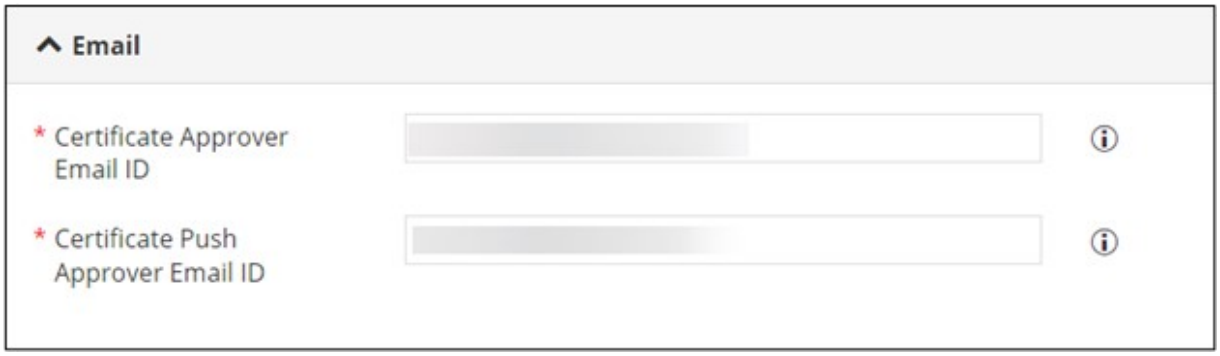
8. To add the selected profile/application to the grid, click +.

   The **Profile/Application** is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

9. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
10. Select a new device and click again to update the value.
11. To delete a profile/application, select the row to be deleted in the grid and click .
12. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
13. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
14. Under the **Email** section, enter the field information as shown.



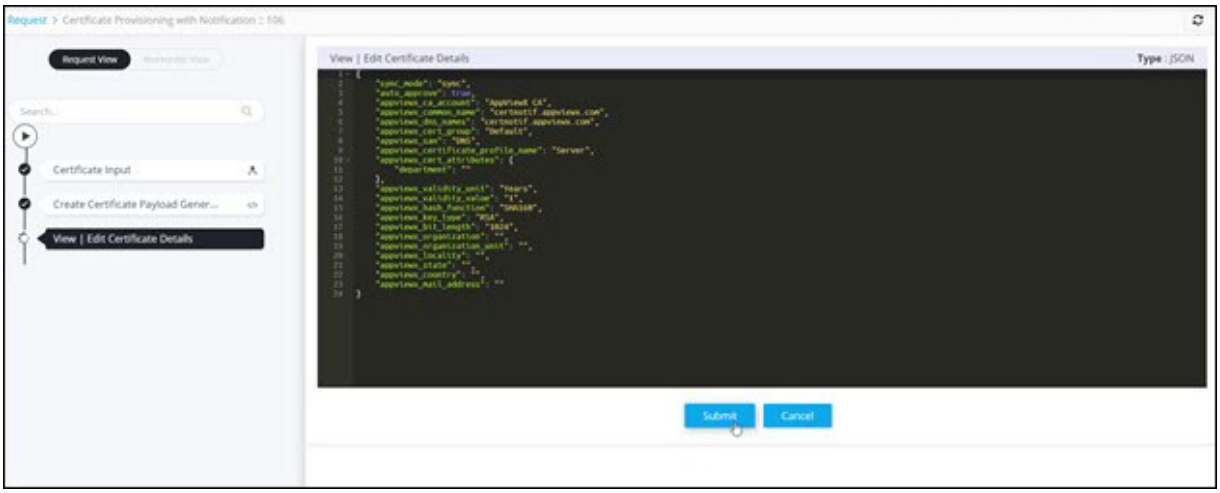
The following table describes the field information under the **Email**section:

Field	Description
***Certificate Approver Email ID**	Enter the email address or multiple addresses, separated by comma, of the user(s) approving the certificate creation request.
***Certificate Push Approver Email ID**	Enter the email address of the user who will approve the certificate push request.
All Asterisk (*) marked fields are mandatory.	

15. Click **Submit**.

The workflow is executed.

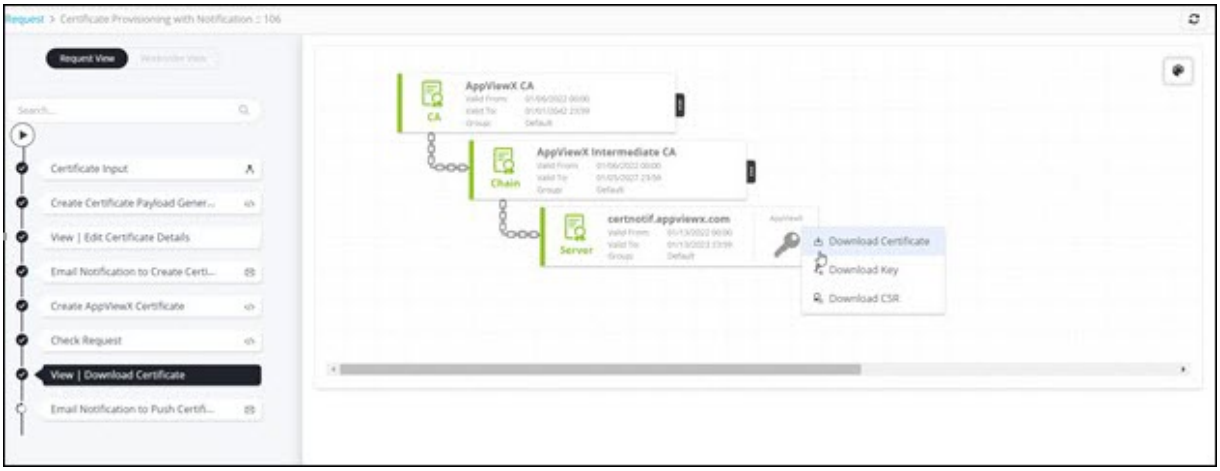
16. At the **View | Edit Certificate Details** stage, click **Submit**.



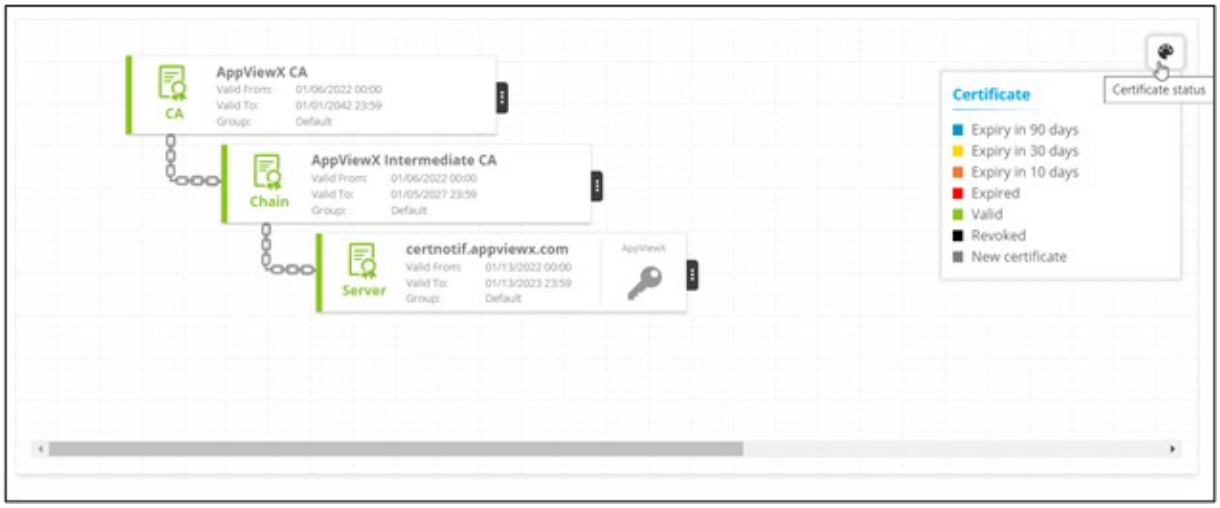
Email notification for Create Certificate approval received.

17. Click **Approve** or **Reject** in the **Approval for Creating Certificate** email.
    Certificate is created after the approver clicks **Approve**.

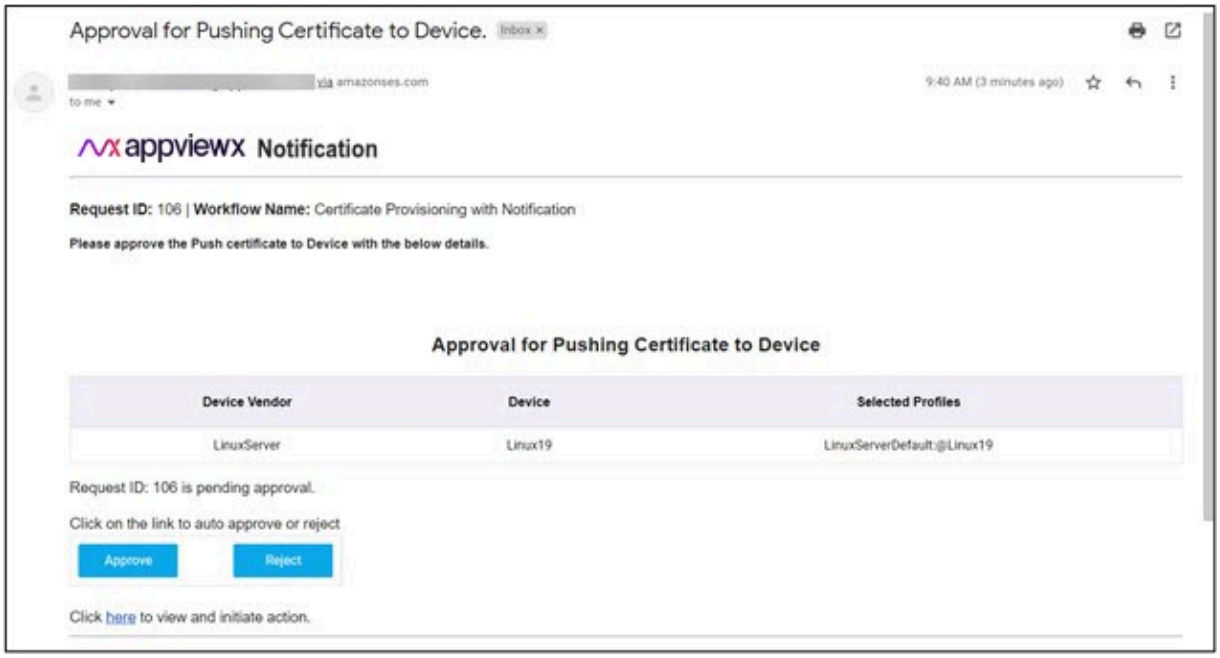
18. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.



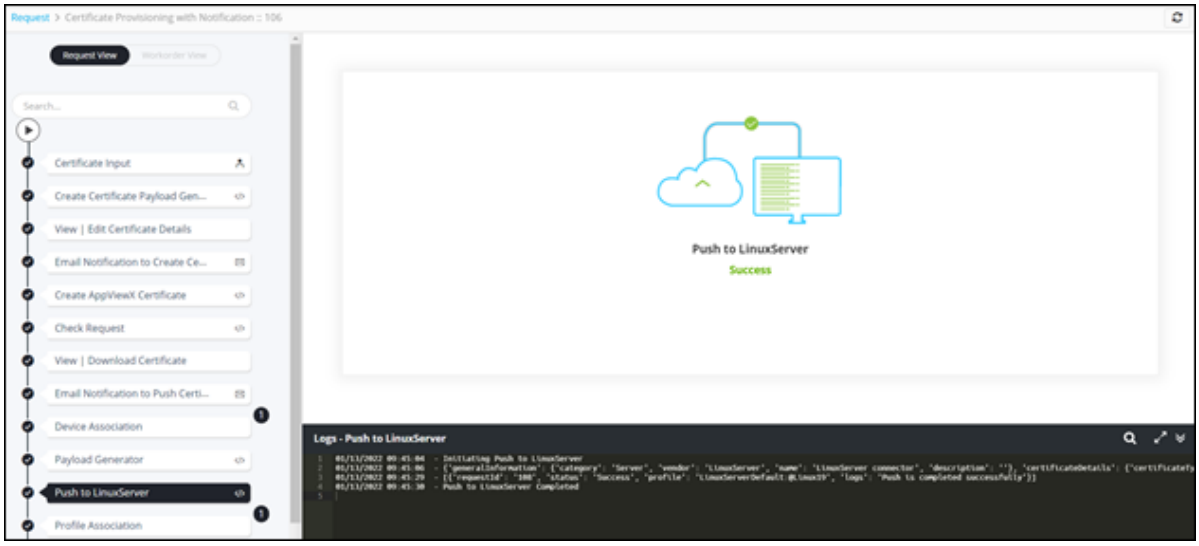
19. Hover your mouse over to view the Certificate status.



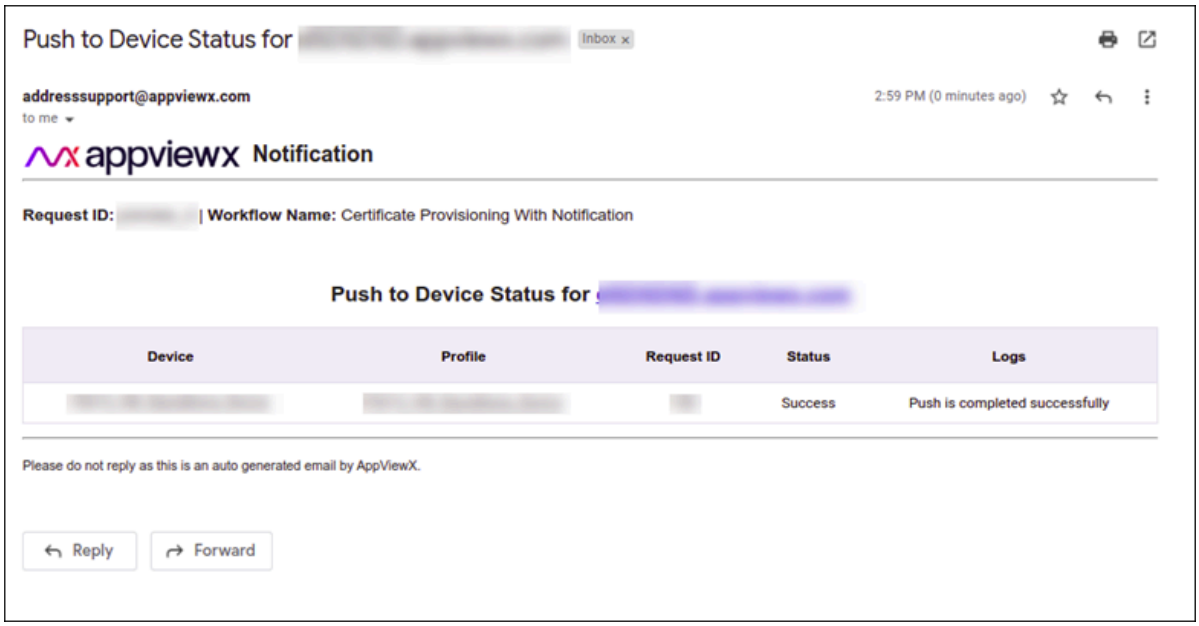
20. Click **Approve** or **Reject** in the **Approval for Pushing Certificate to Device** email.



• Once the approver approves the request, the certificate is pushed to the selected device.



• Email notification received.

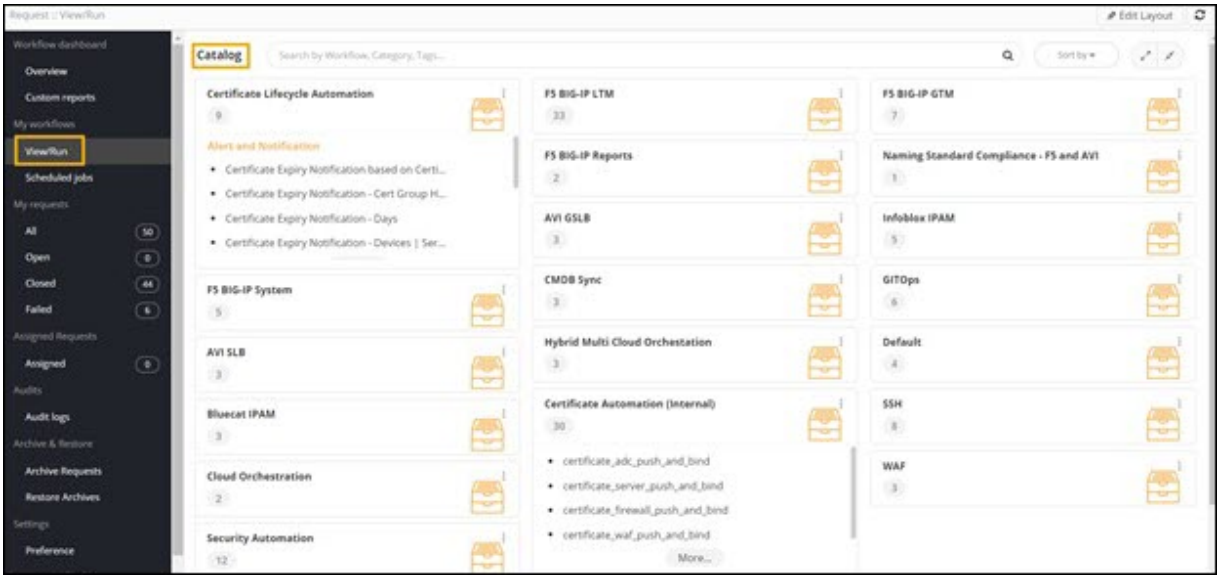


Enroll Certificate Based on Policy | CSR Details | CSR Upload

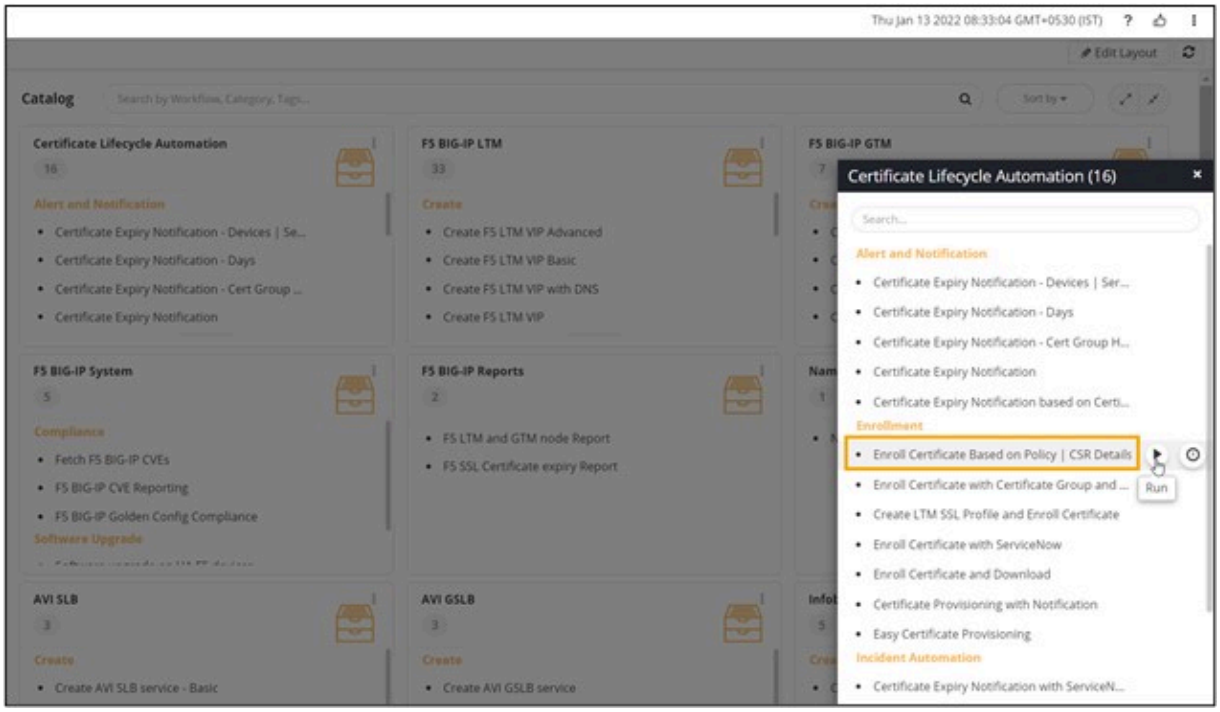
This workflow allows you to create a certificate using three input methods - Manual, Policy Based, and Upload CSR.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

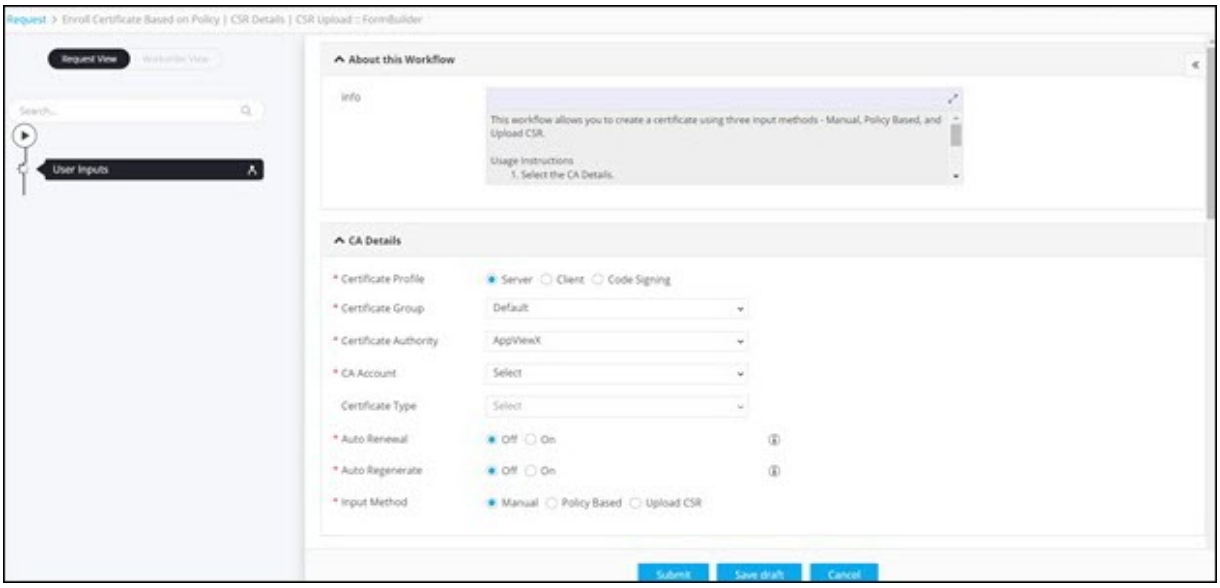


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate Based on Policy | CSR Details | CSR Upload** workflow and click .

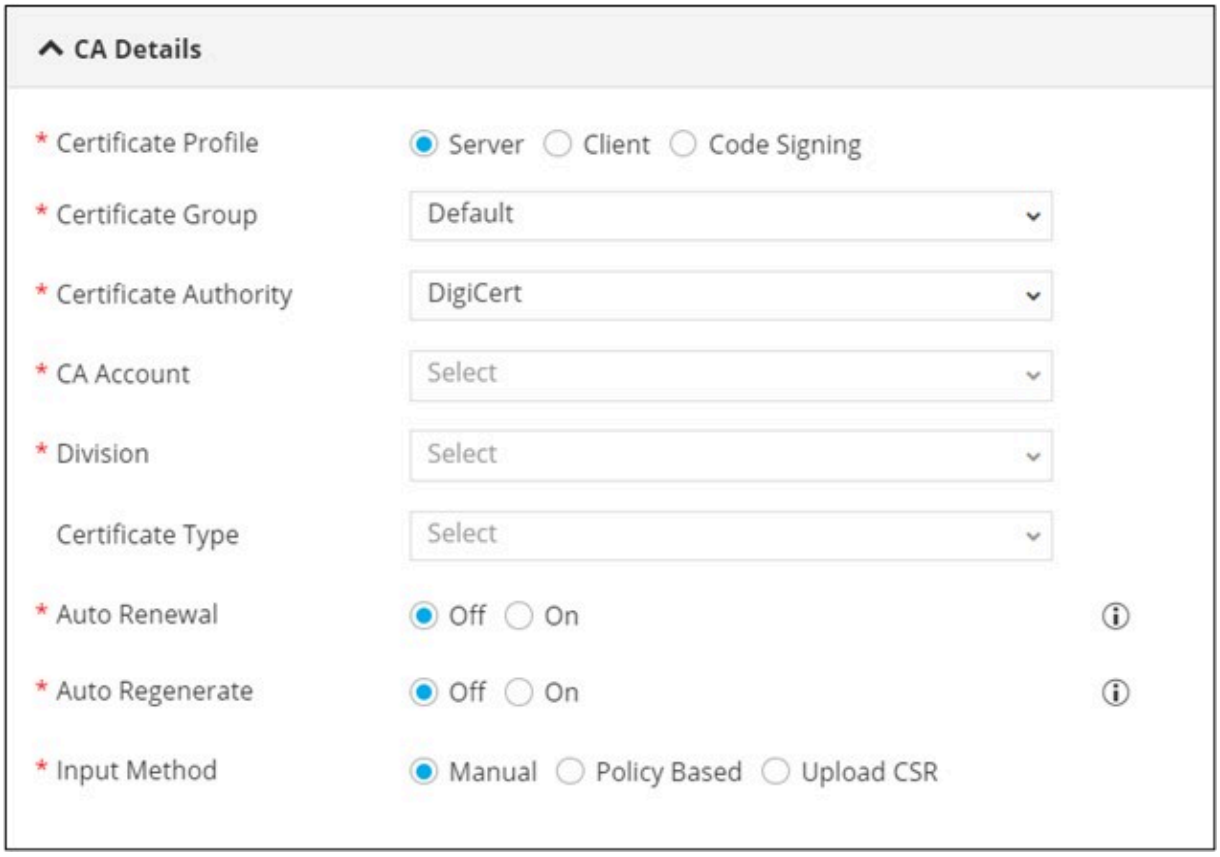


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **CA Details** section, select the following field information:



The following table describes the fields in the **CA Details** section:

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.

Field	Description
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field. **Note:** This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual:** If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. • **Policy Based:** If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR:** If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters. **Note: Manual** is the default selection.
All Asterisk (*) marked fields are mandatory.	

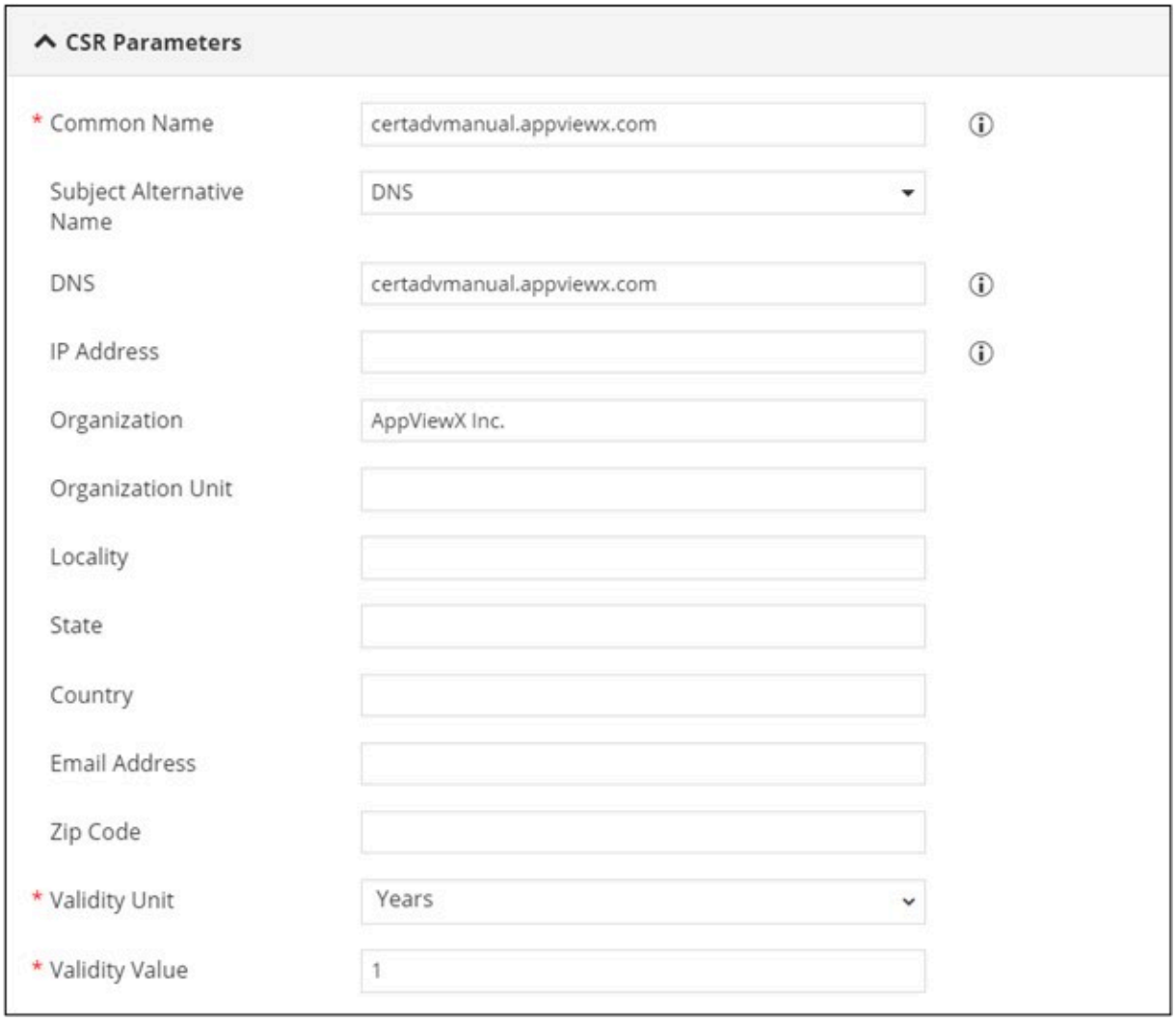
- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

- Manual
- Policy Based
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter the field information as shown.

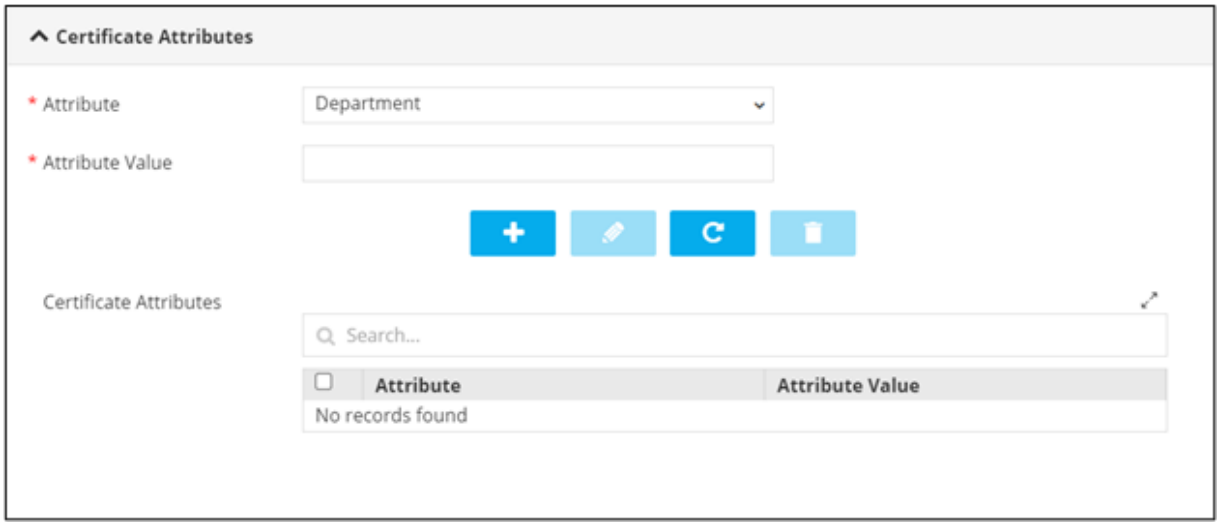


The following table describes the field information in the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either:

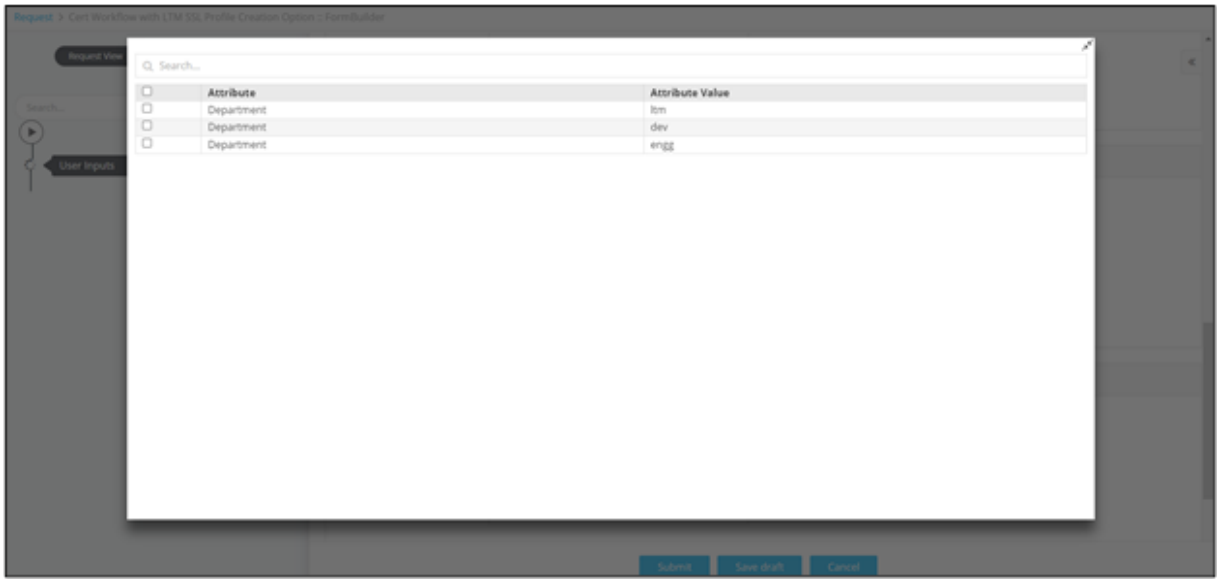
Field	Description
	• **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in 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. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



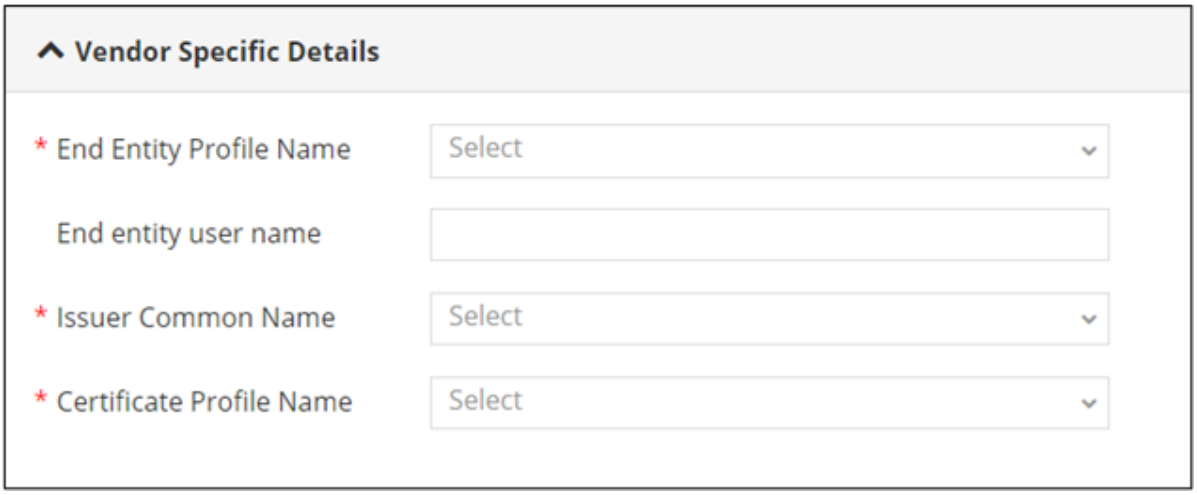
4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .
6. Enter the new value for the attribute in the **Value** field and click again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click .

8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



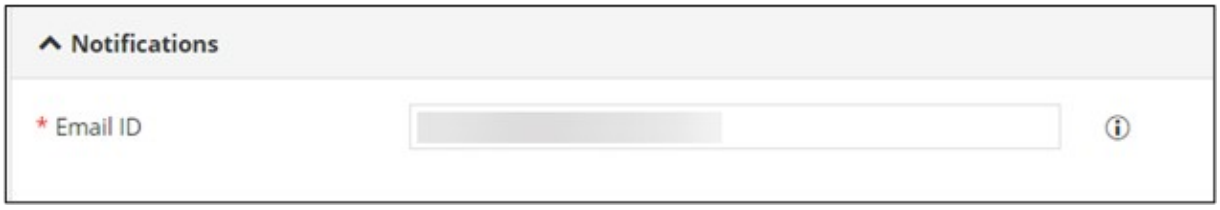
9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

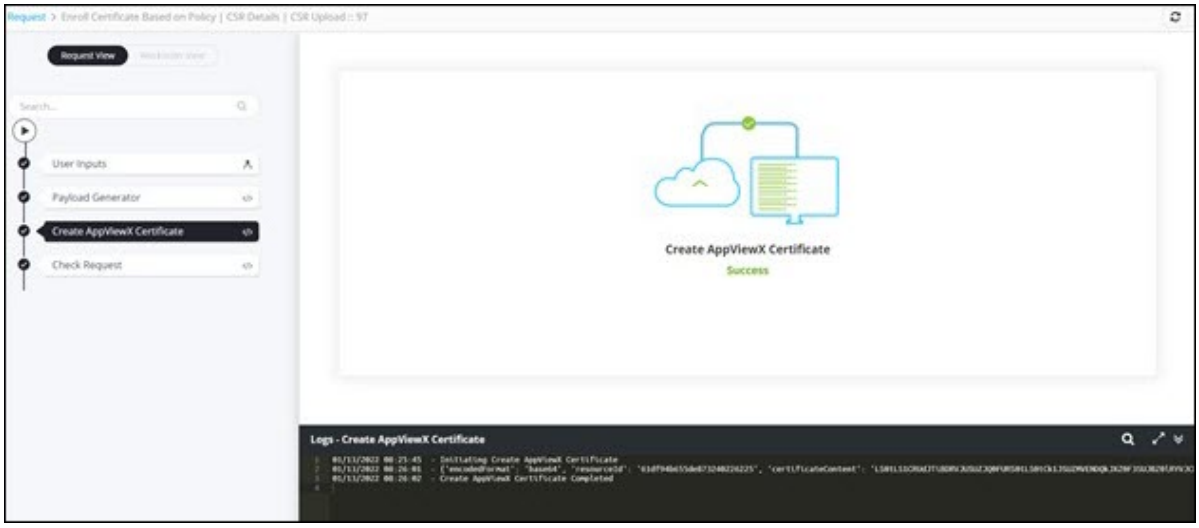
11. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



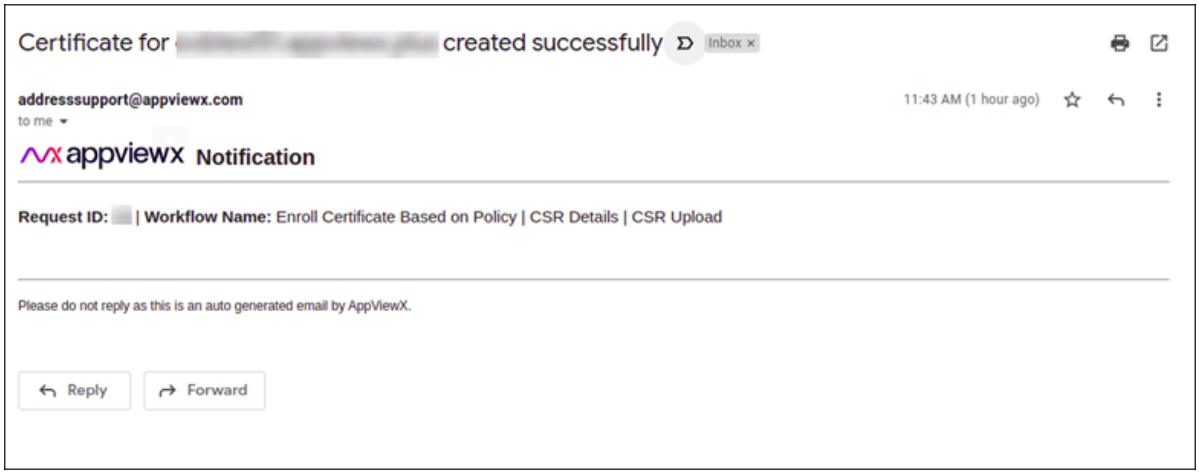
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

12. Click **Submit**.

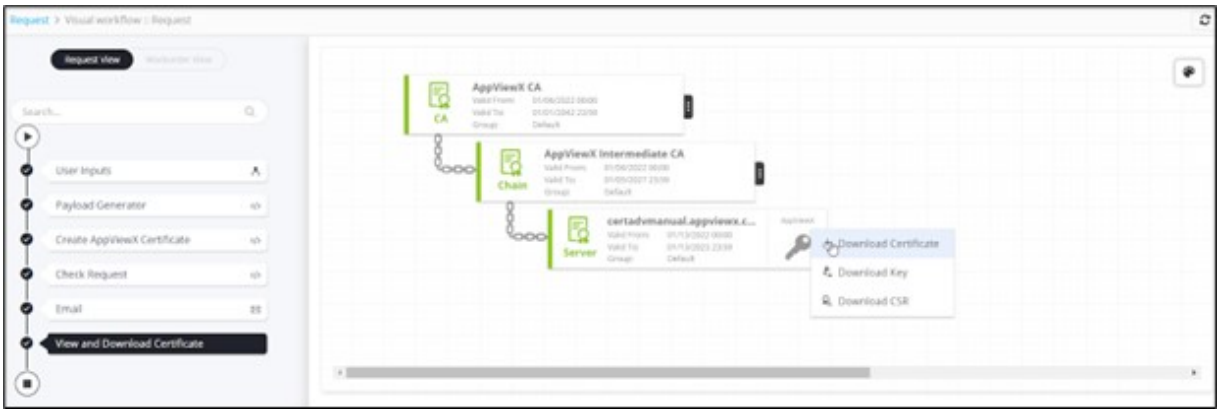
• AppViewX certificate created.



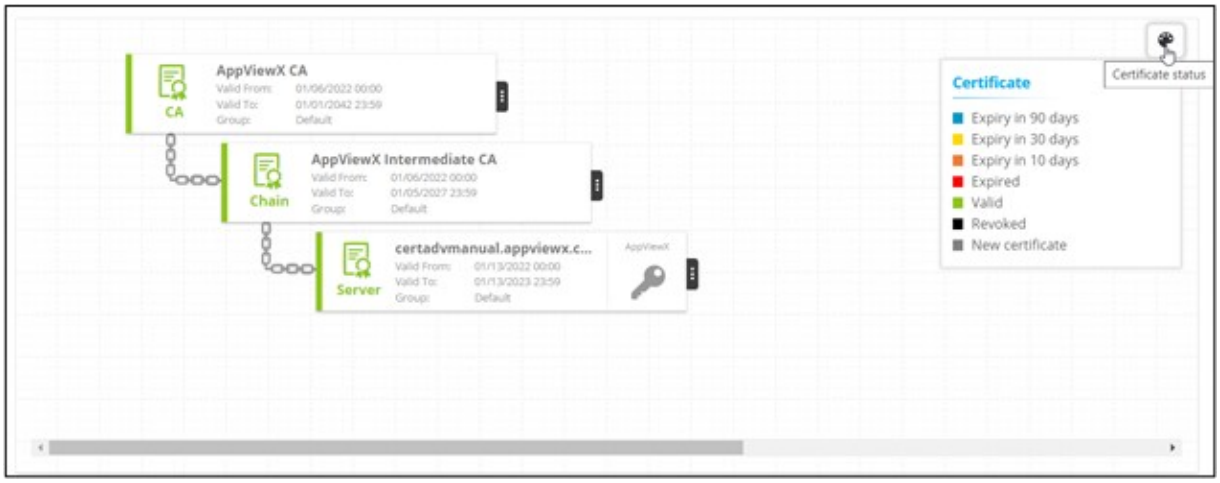
• Email notification received.



13. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



14. Hover your mouse over  to view the **Certificate status**.

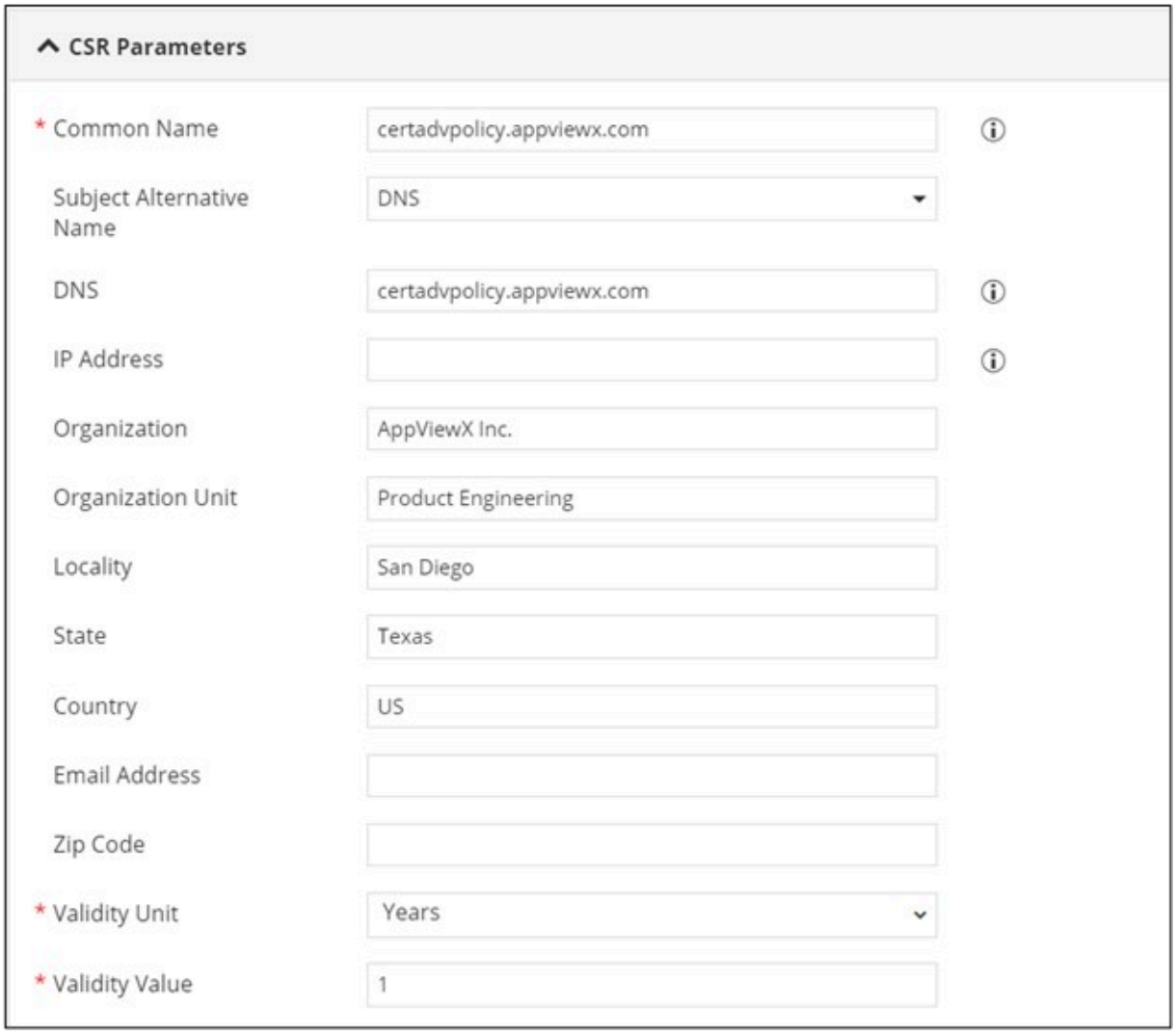


Policy Based

After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

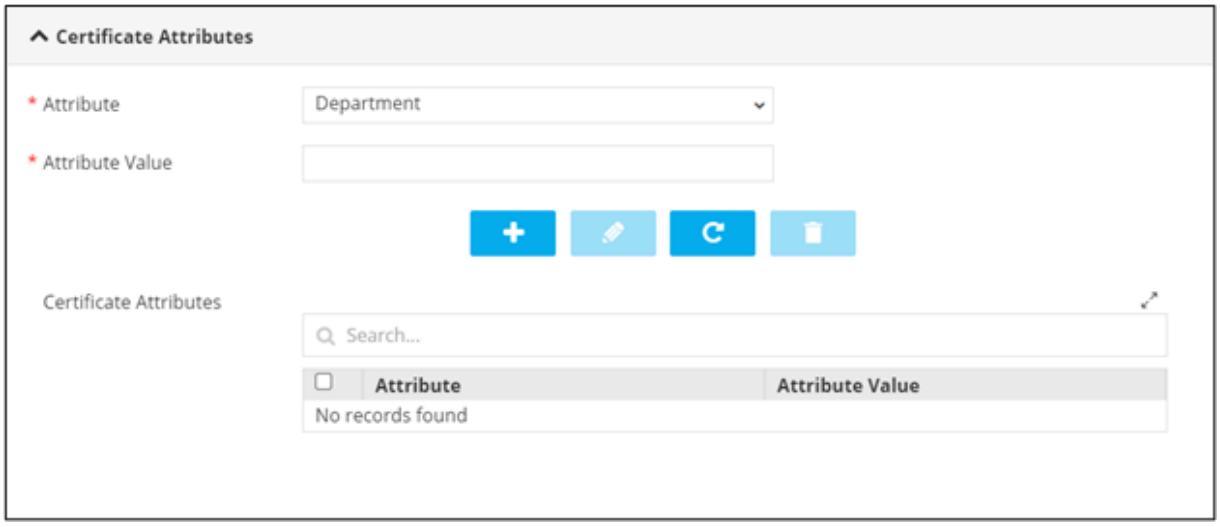
1. Under the **CSR Parameters** section, enter the field information as shown.

> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.



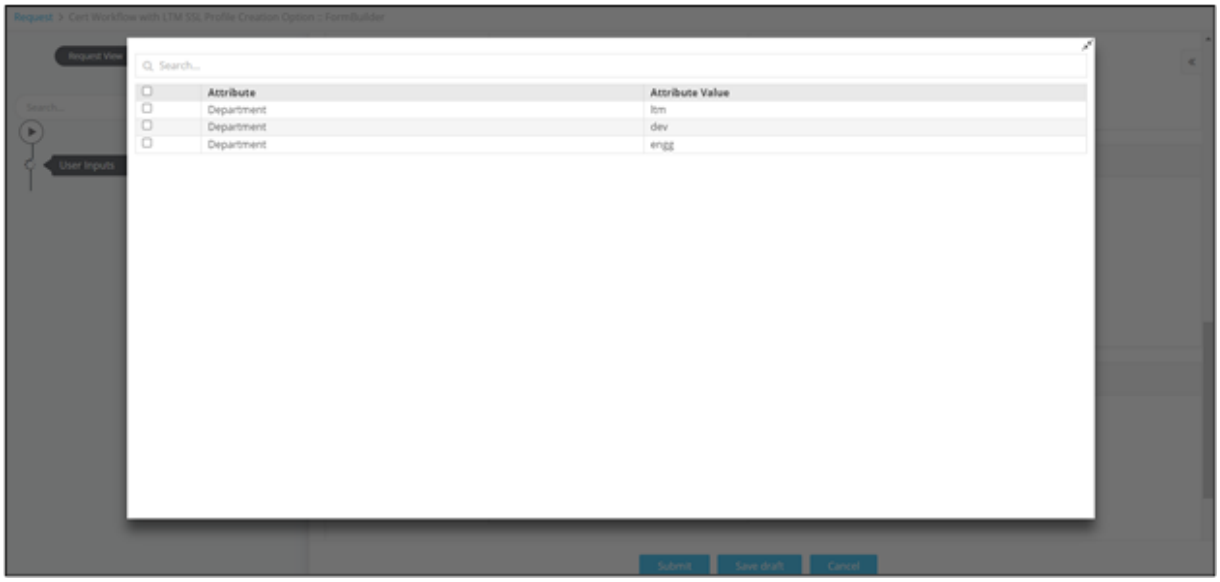
Note: For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



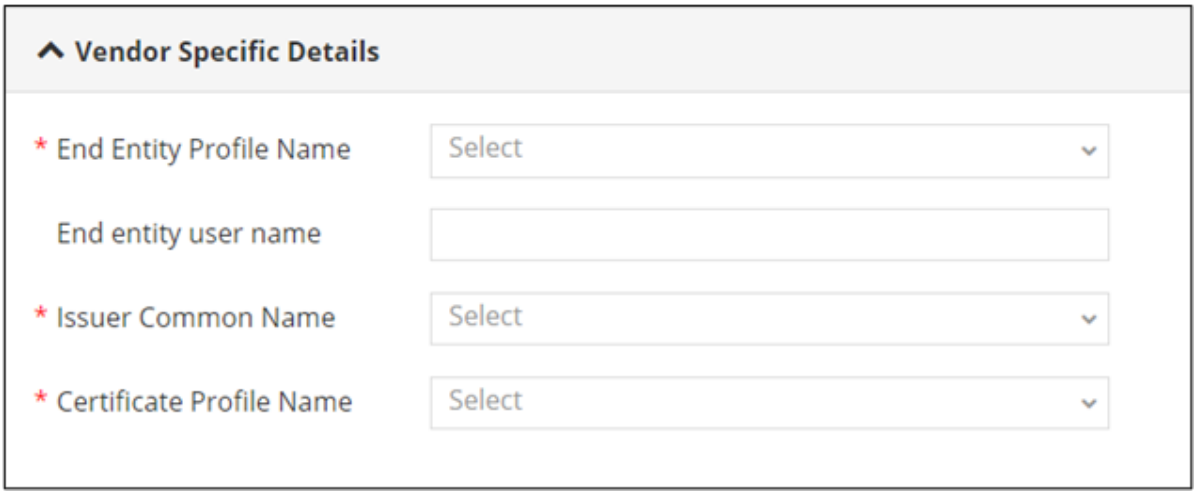
4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .

6. Enter the new value for the attribute in the **Value** field and click  again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click  .
8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



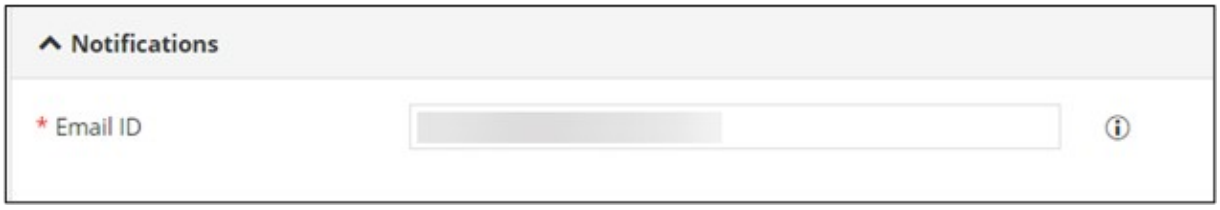
9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

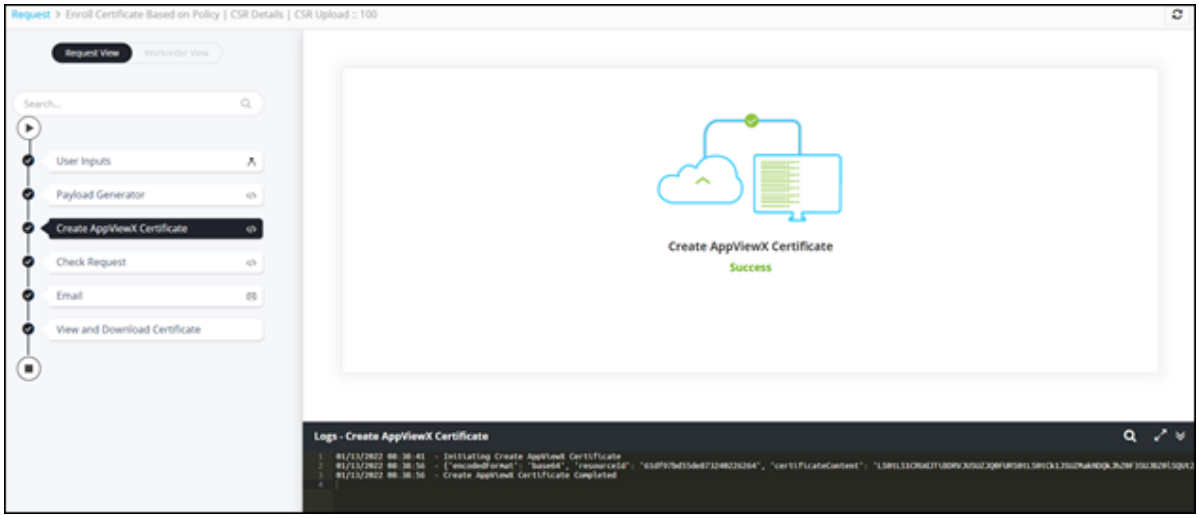
11. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



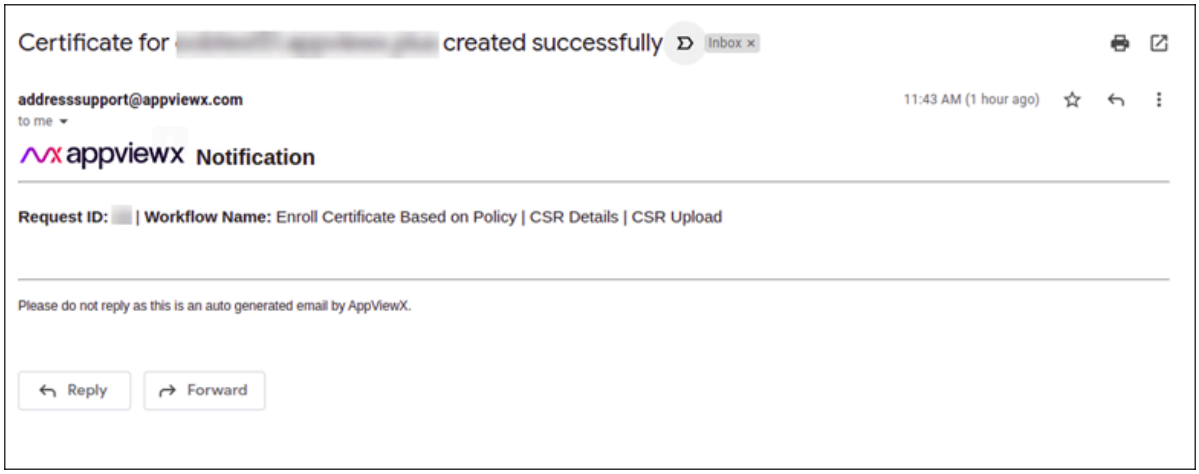
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

12. Click **Submit**.

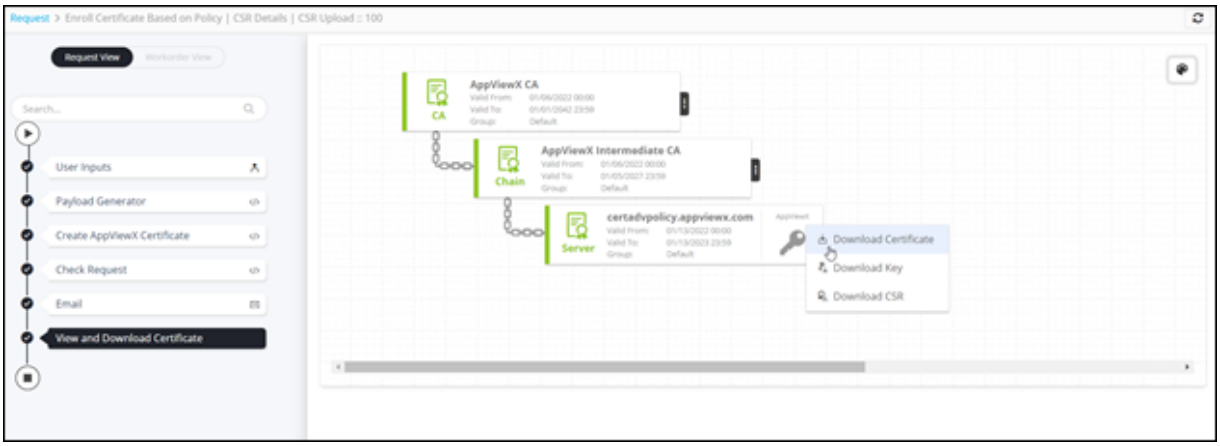
• AppViewX certificate created.



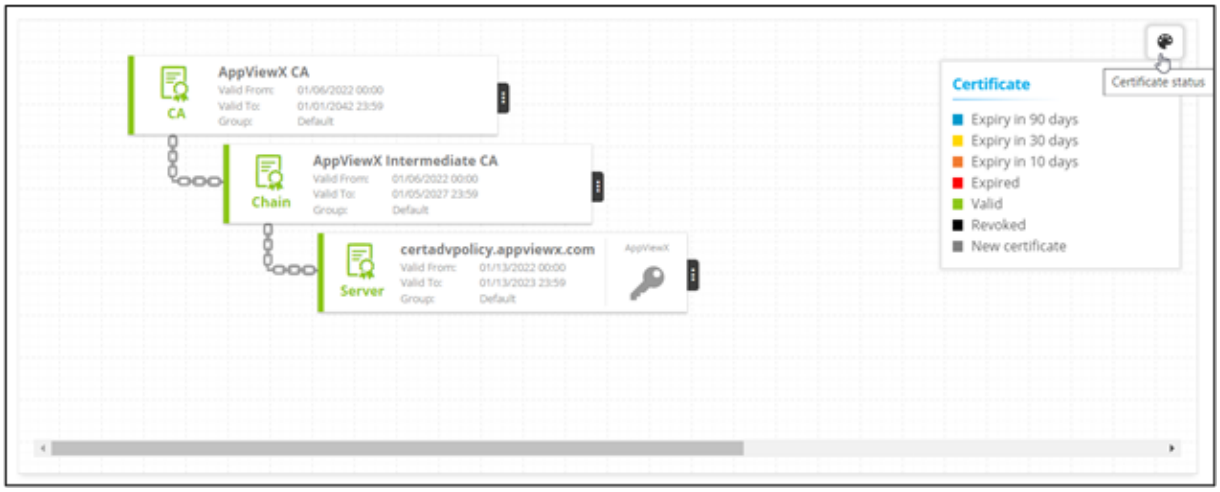
• Email notification received.



13. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



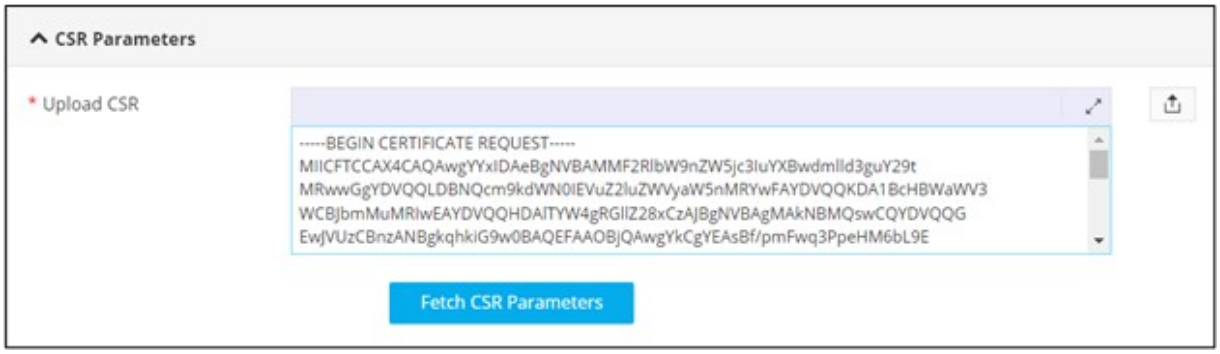
14. Hover your mouse over  to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

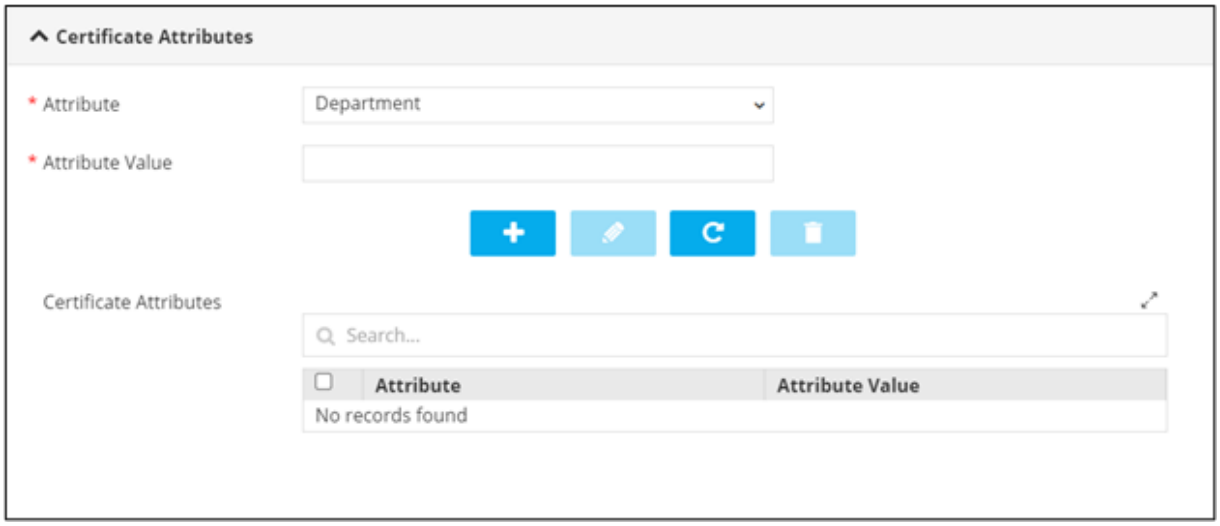
1. Under the **CSR Parameters** section, to **Upload CSR**, click .



2. Click **Fetch CSR Parameters**.

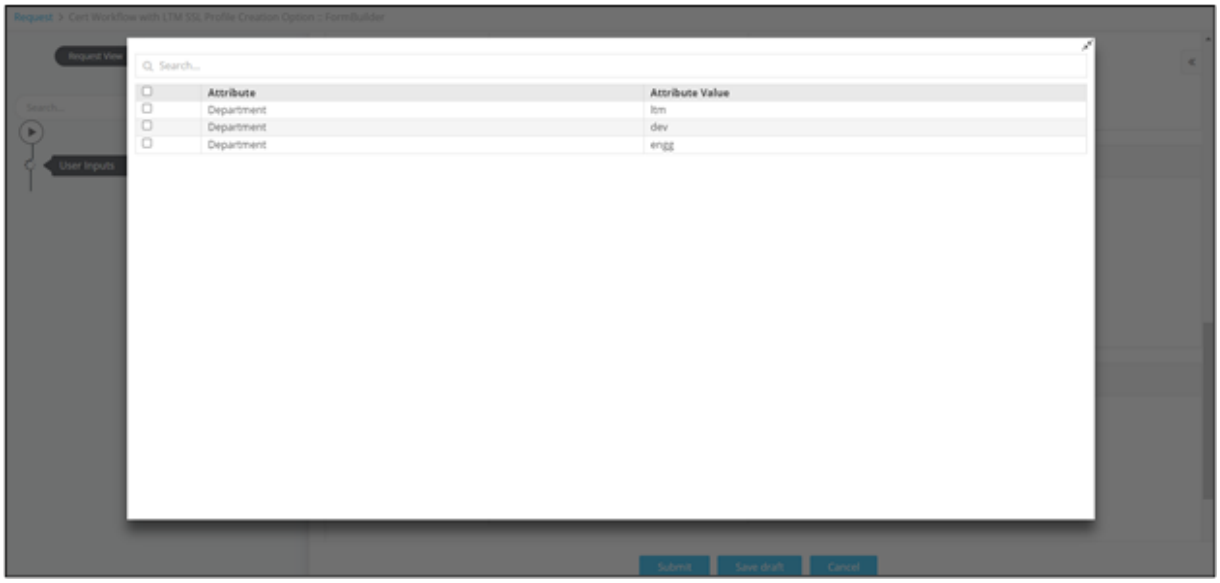
> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



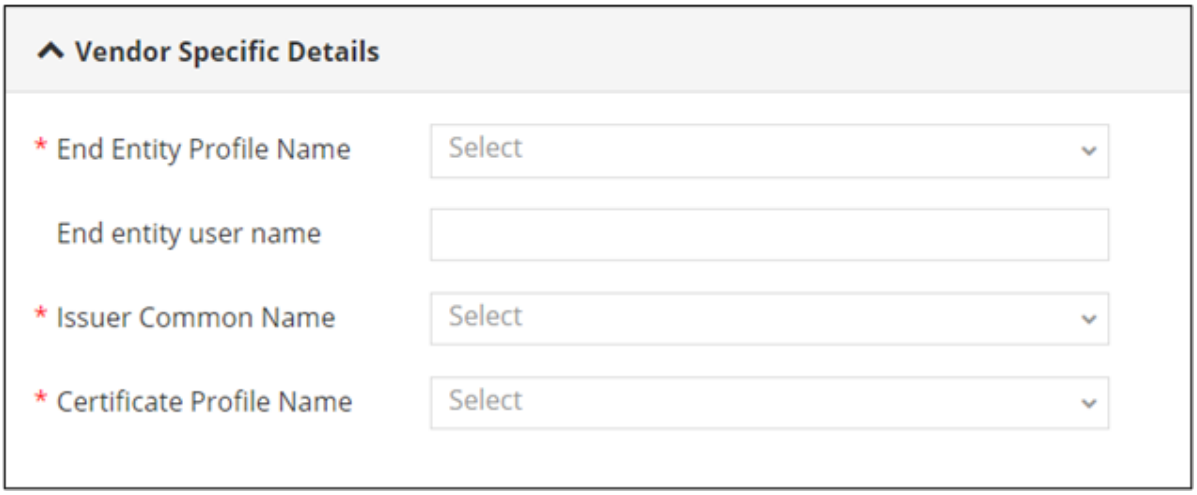
5. To add this attribute to the **Certificate Attributes** grid, click .
6. To edit the value of a particular attribute, select the attribute in the grid and click .
7. Enter the new value for the attribute in the **Value** field and click again to update the value.
8. To delete a certificate attribute, select the attribute in the grid and click .

9. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



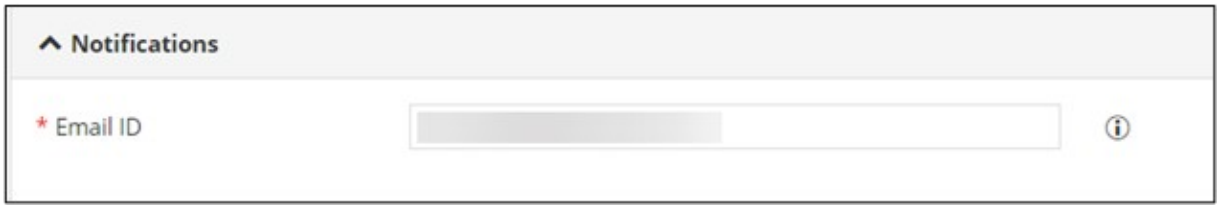
10. To search for a particular attribute in the grid, type the keyword(s) in the search field.
11. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

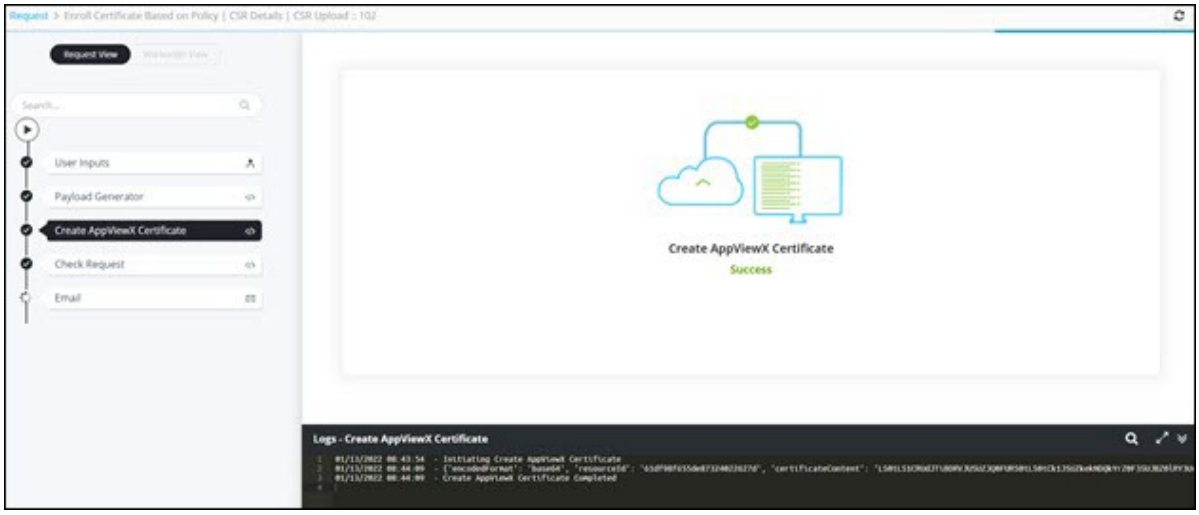
12. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



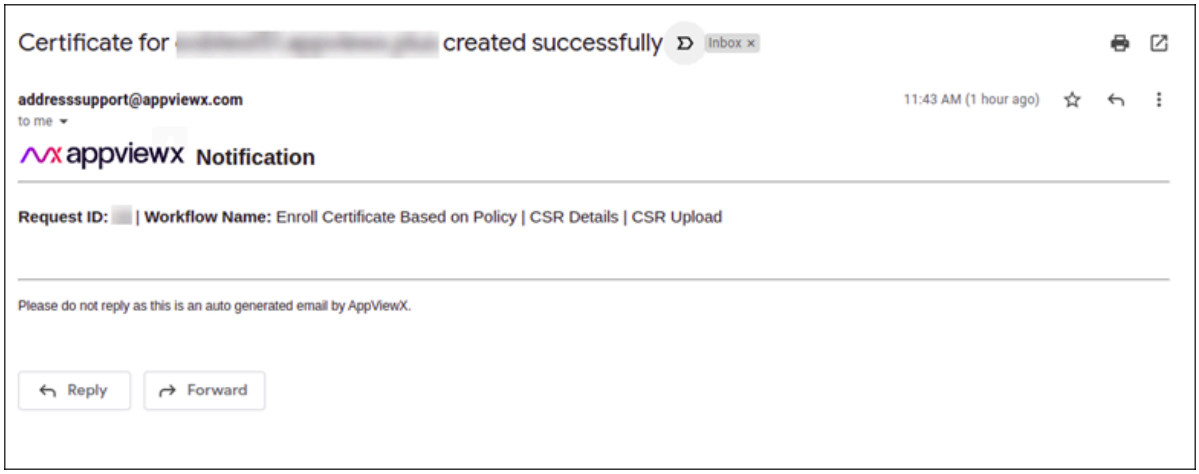
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.

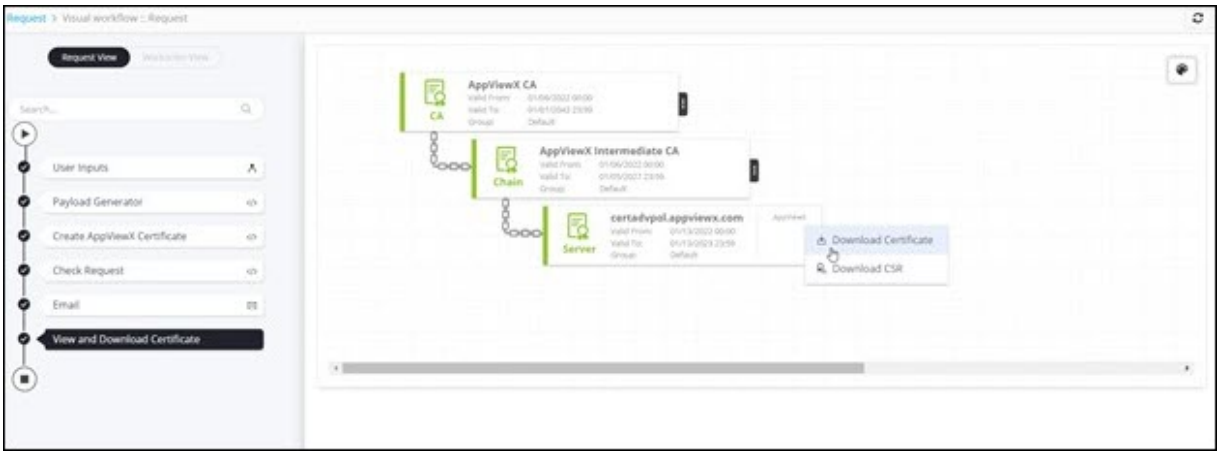
• AppViewX certificate created.



• Email notification received.



14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



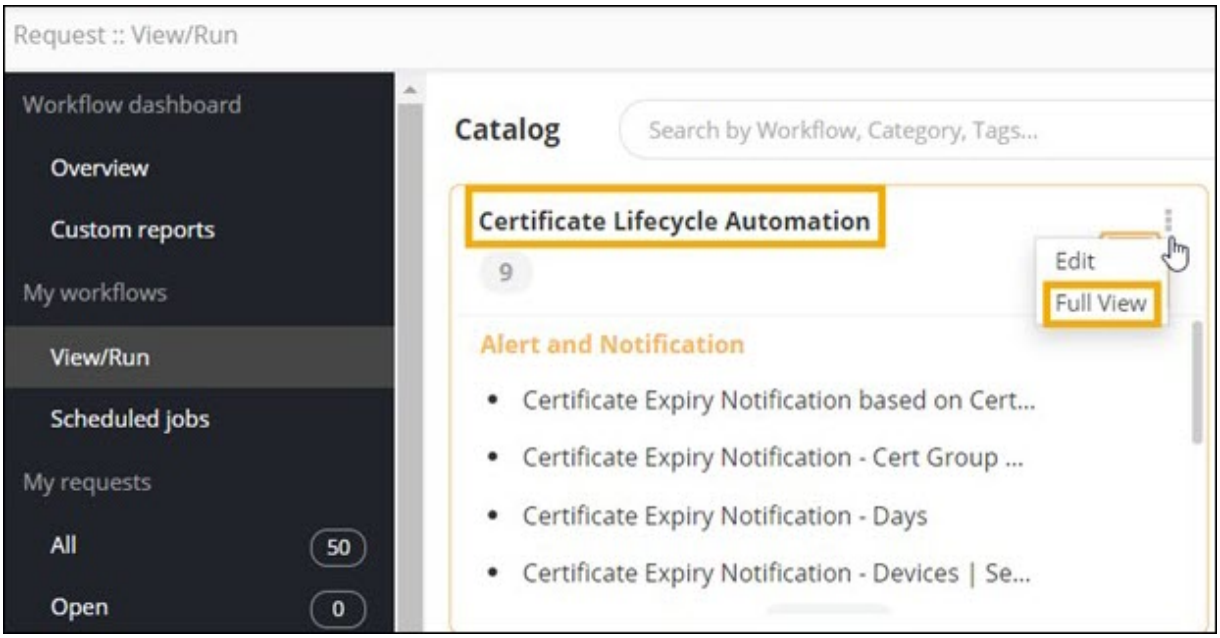
15. Hover your mouse over to view the **Certificate status**.

Create LTM SSL Profile and Enroll Certificate

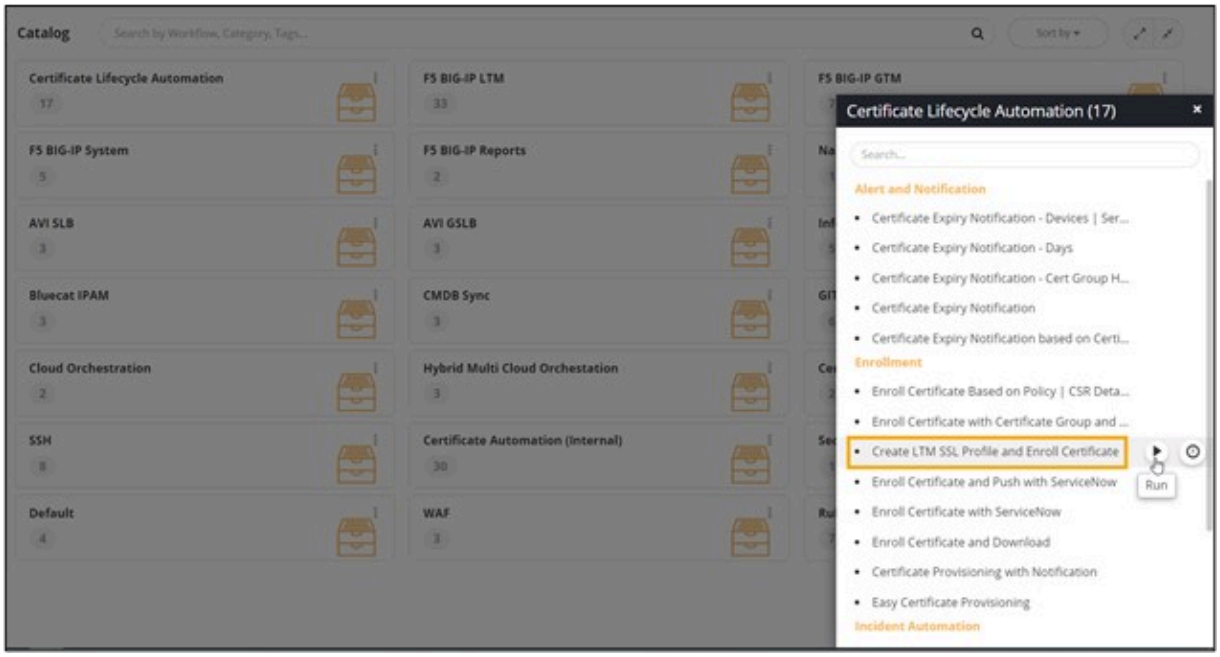
This workflow allows you to create individual server certificates along with LTM SSL profile creation based on the selected certificate group.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

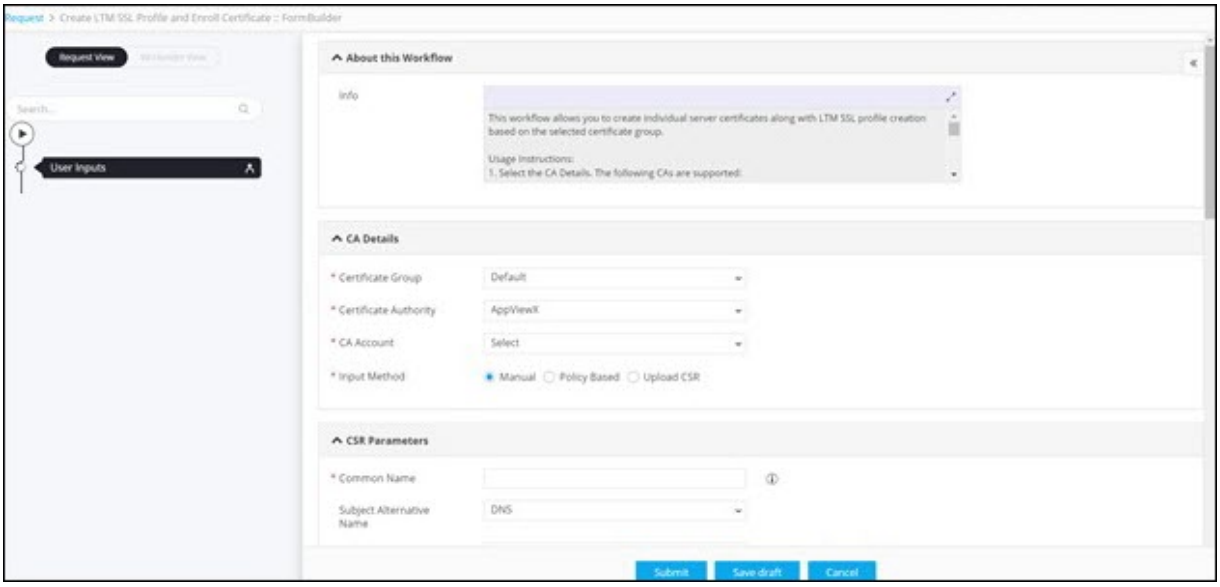


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Create LTM SSL Profile and Enroll Certificate**workflow and click .

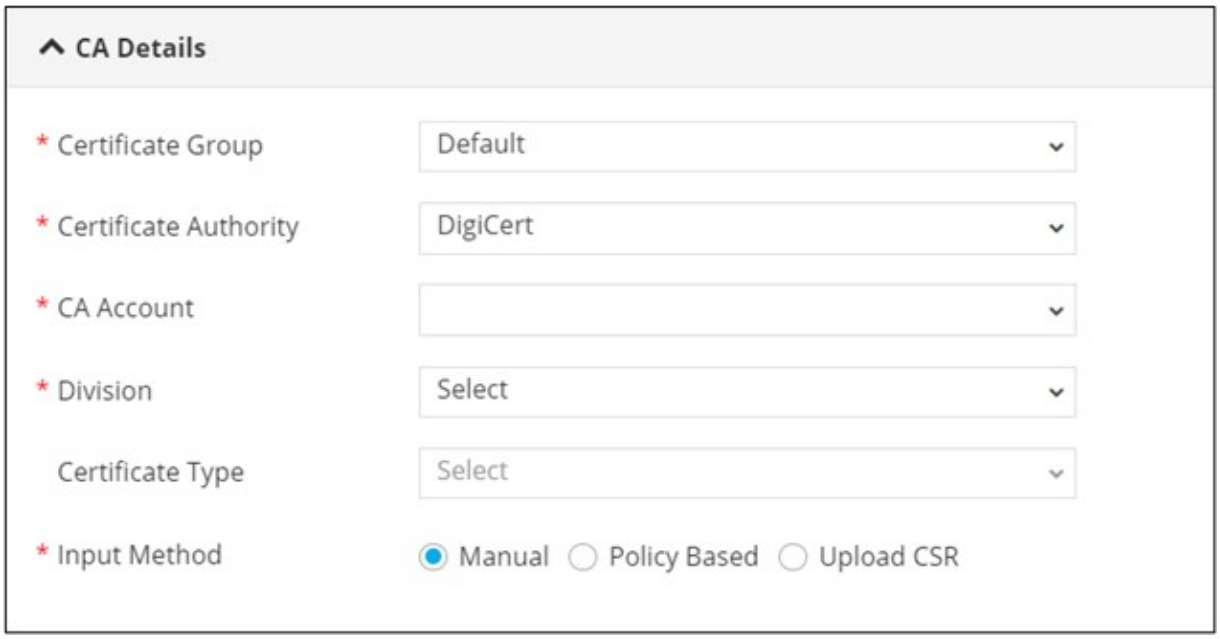


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **CA Details** section, select the following field information:



The following table describes the fields in the **CA Details** section:

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** The **Certificate Authority** field is populated based on the selected **Certificate Group**.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** The **CA Account** field is populated based on the selected **Certificate Authority**.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual:** If you select the **Input Method** as Manual, the CSR parameters will have to be entered/selected manually. • **Policy Based:** If you select the **Input Method** as Policy Based, the CSR parameters fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR:** If you select the **Input Method** as Upload CSR, you can upload the CSR file to fetch the CSR parameters.

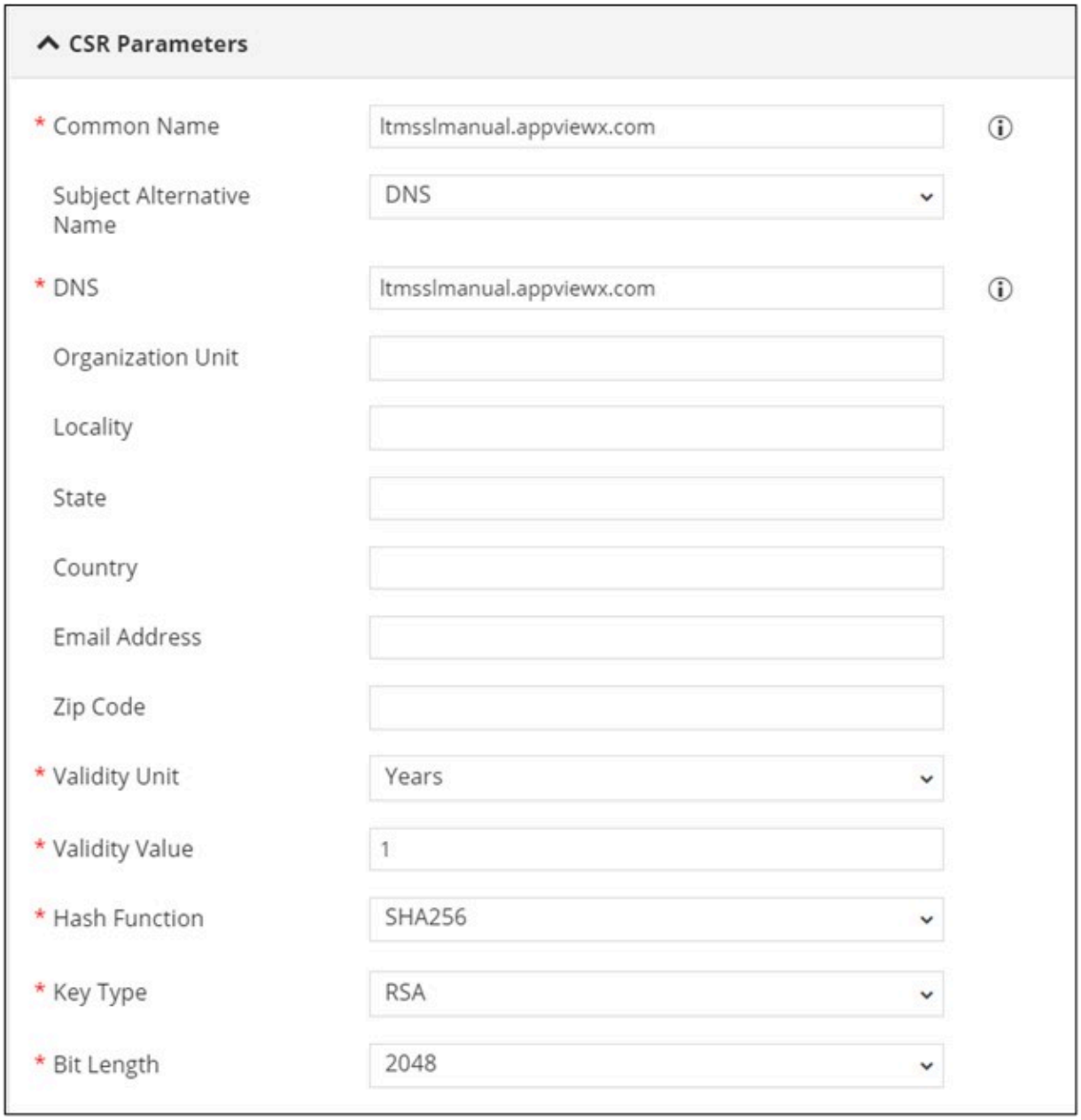
Field	Description
	Note: Manual is the default **Input Method**.
All asterisk (*) marked fields are mandatory.	

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter the field information as shown.



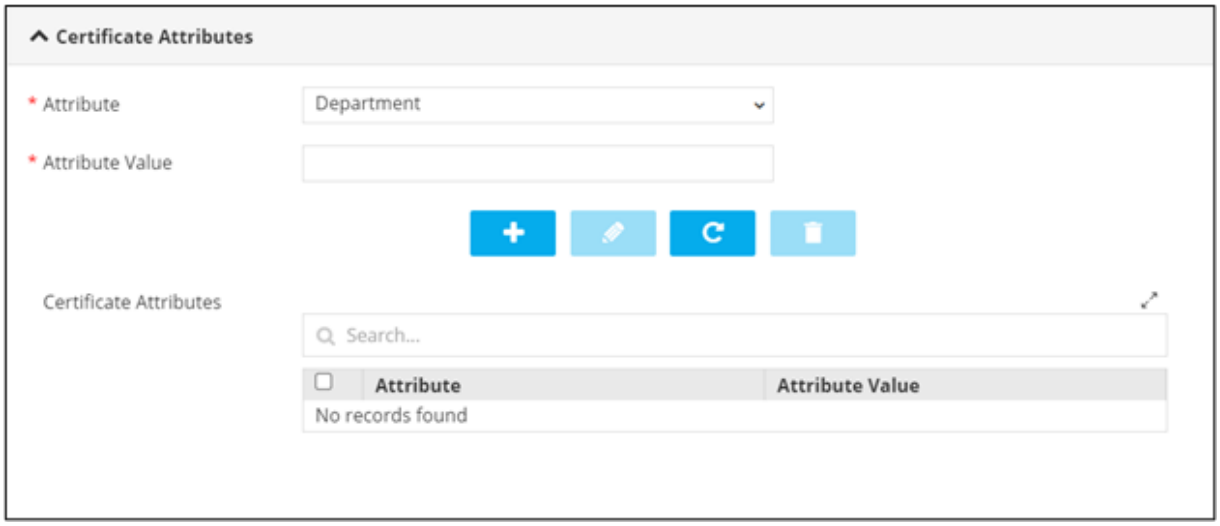
The following table describes the field information in the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.

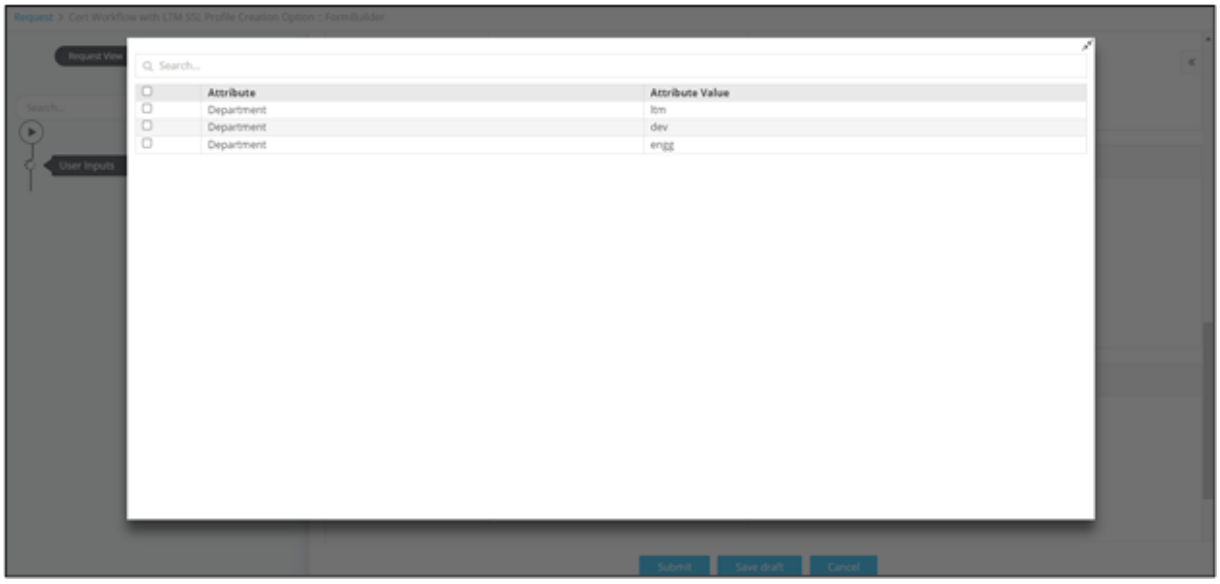
Field	Description
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field. **Note:** This field is displayed if DNS is selected in the **The email id of the logged in user is populated automatically.** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field. **Note:** This field is displayed if IP Address is selected in the **Subject Alternative Name** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***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. **Note:** This field will be populated based on the selected **Key Type**.

Field	Description
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

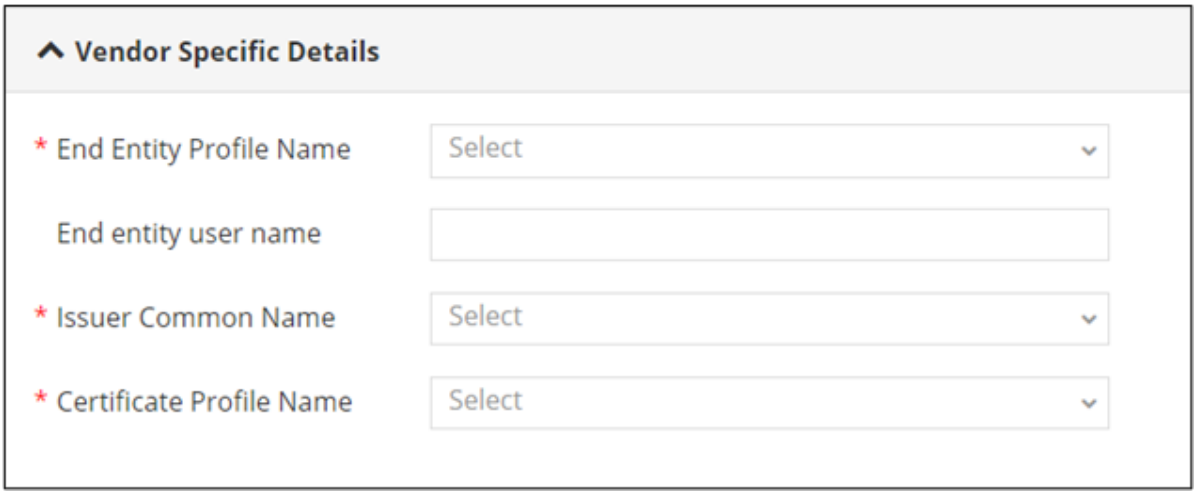


4. To add this attribute to the **Certificate Attributes** grid, click  .
5. To edit the value of a particular attribute, select the attribute in the grid and click  .
6. Enter the new value for the attribute in the **Value** field and click  again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click  .
8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



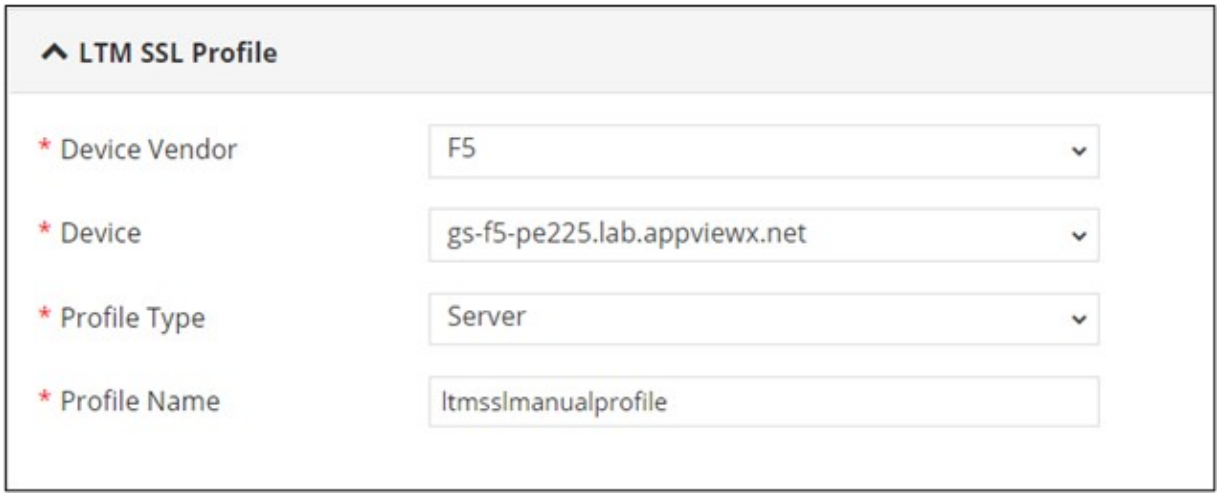
9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

11. Under the **LTM SSL Profile** section, select the field information as shown.

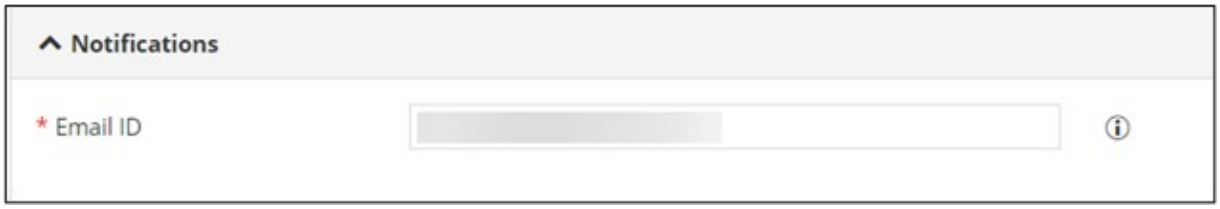


The following table describes the field information in the **LTM SSL Profile** section:

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown.

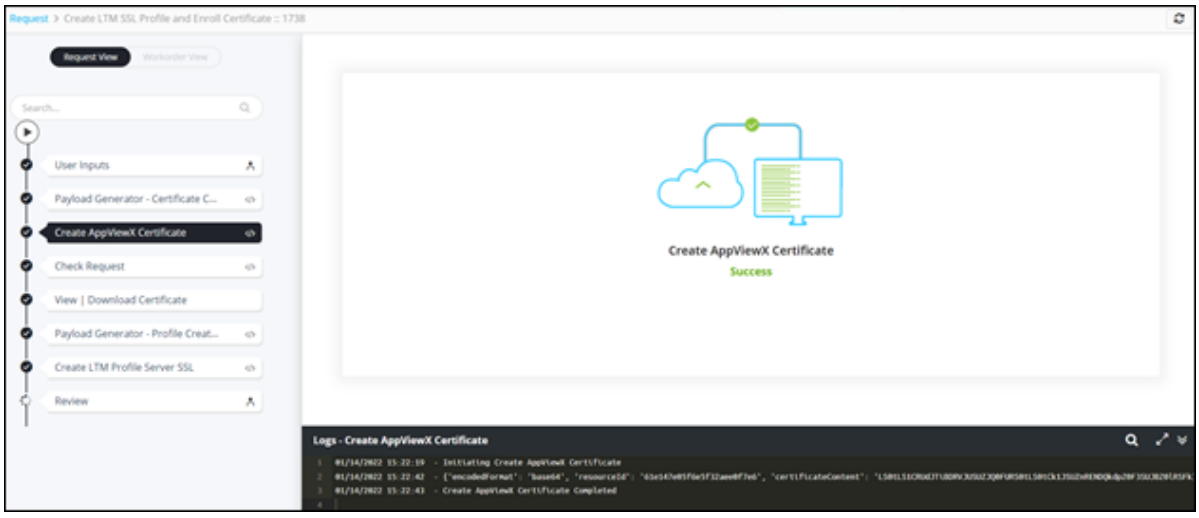
Field	Description
	Note: This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

12. Under the **Email Notification** section, enter the email address(es).

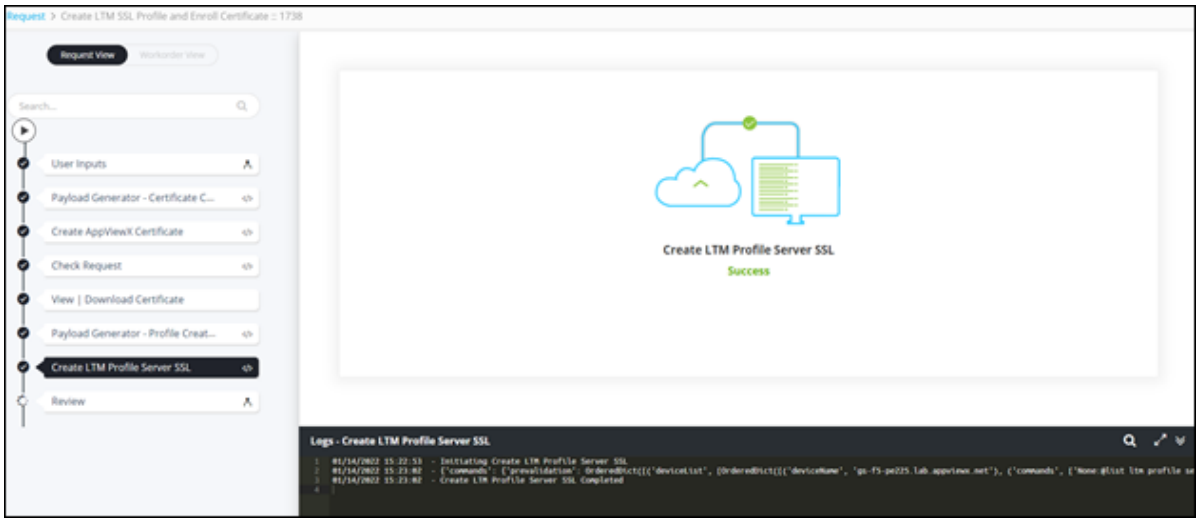


Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

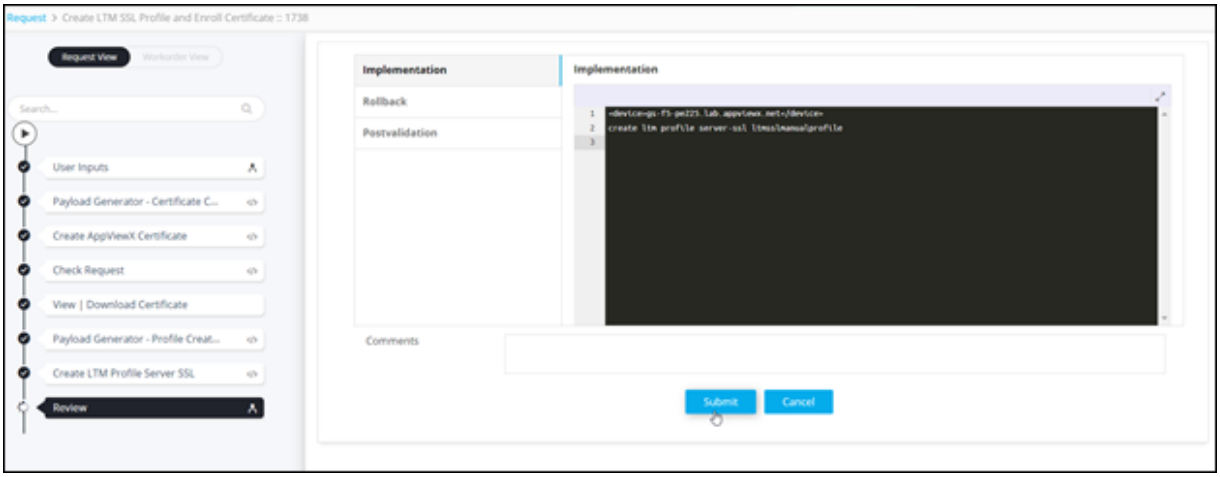
13. Click **Submit**.
    - AppViewX Certificate is generated successfully.



    - LTM Profile on Server SSL created successfully.

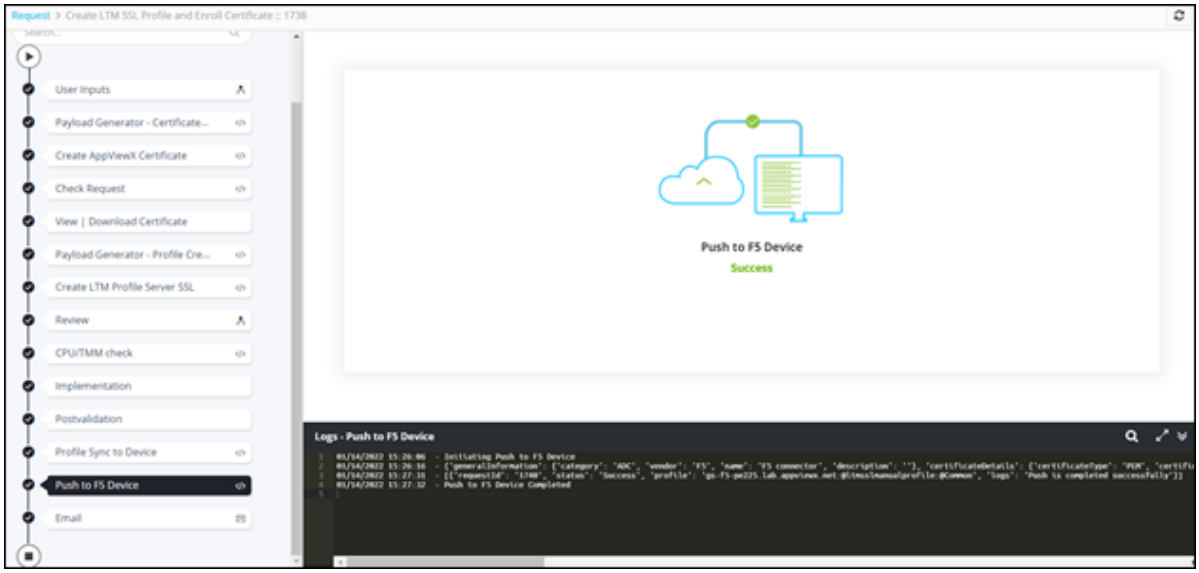


14. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

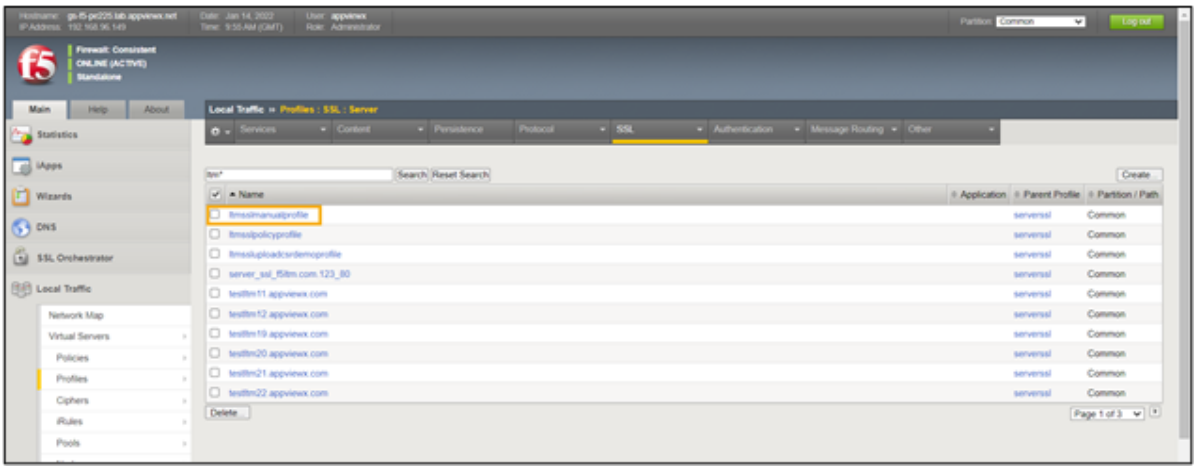


Note: You can change the profile name at this stage.

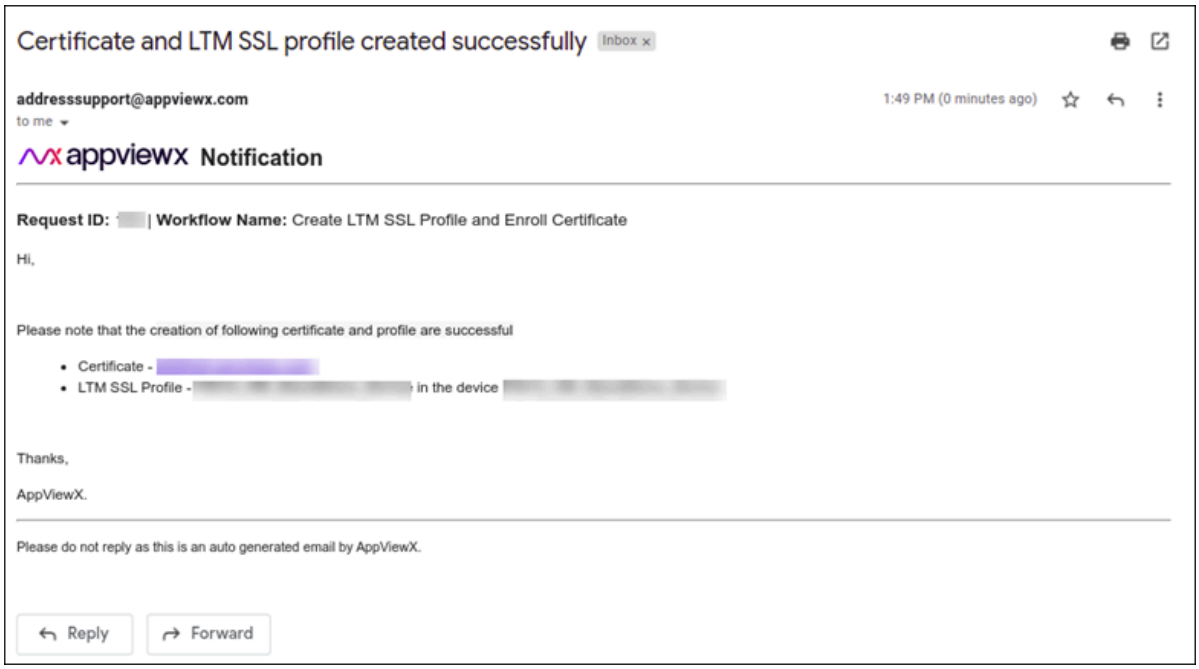
- Profile created on the selected F5 device.



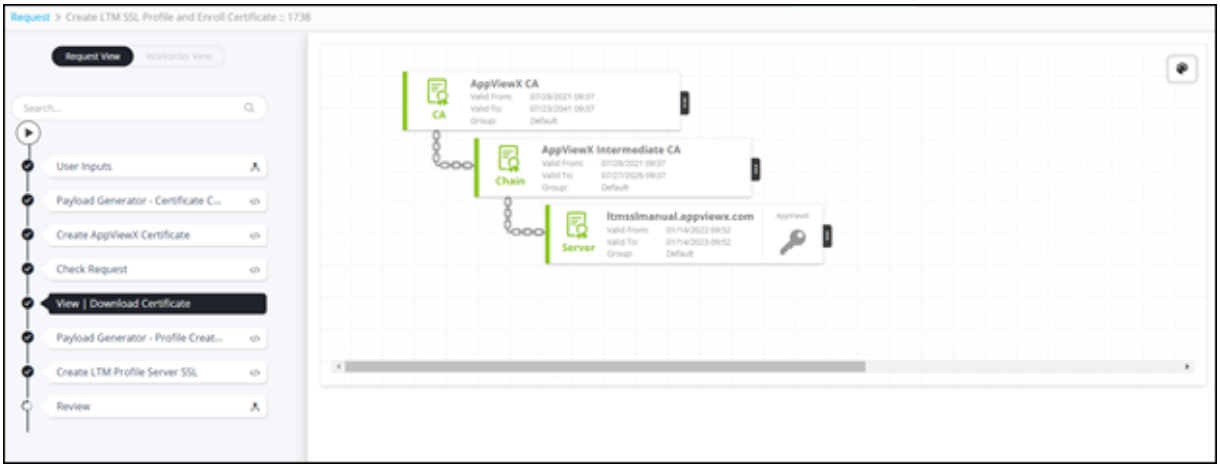
- Profile pushed to the selected F5 device.



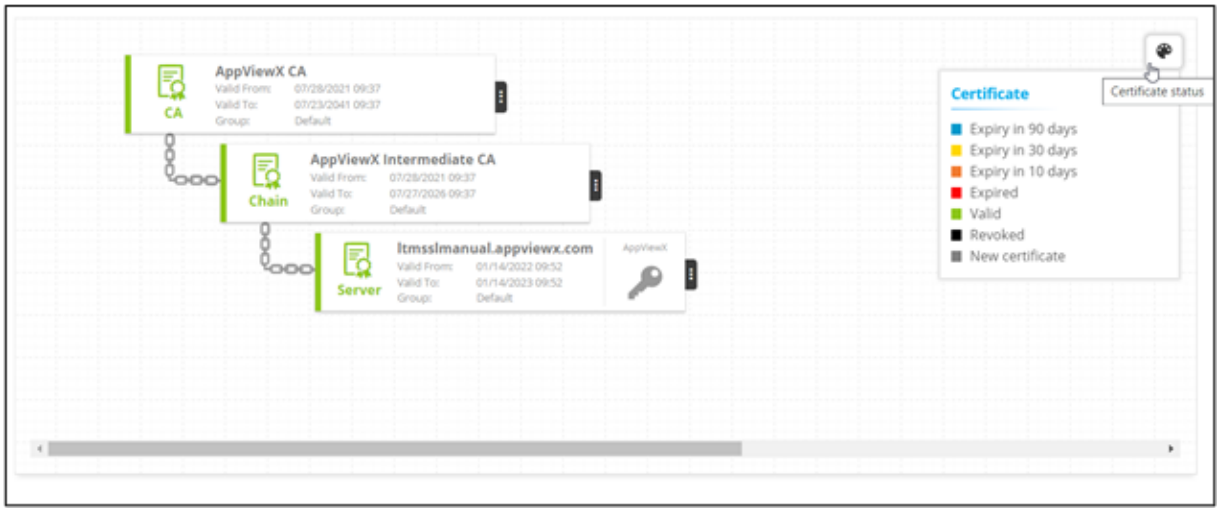
- Email notification received.



15. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



16. Hover your mouse over  to view the **Certificate status**.

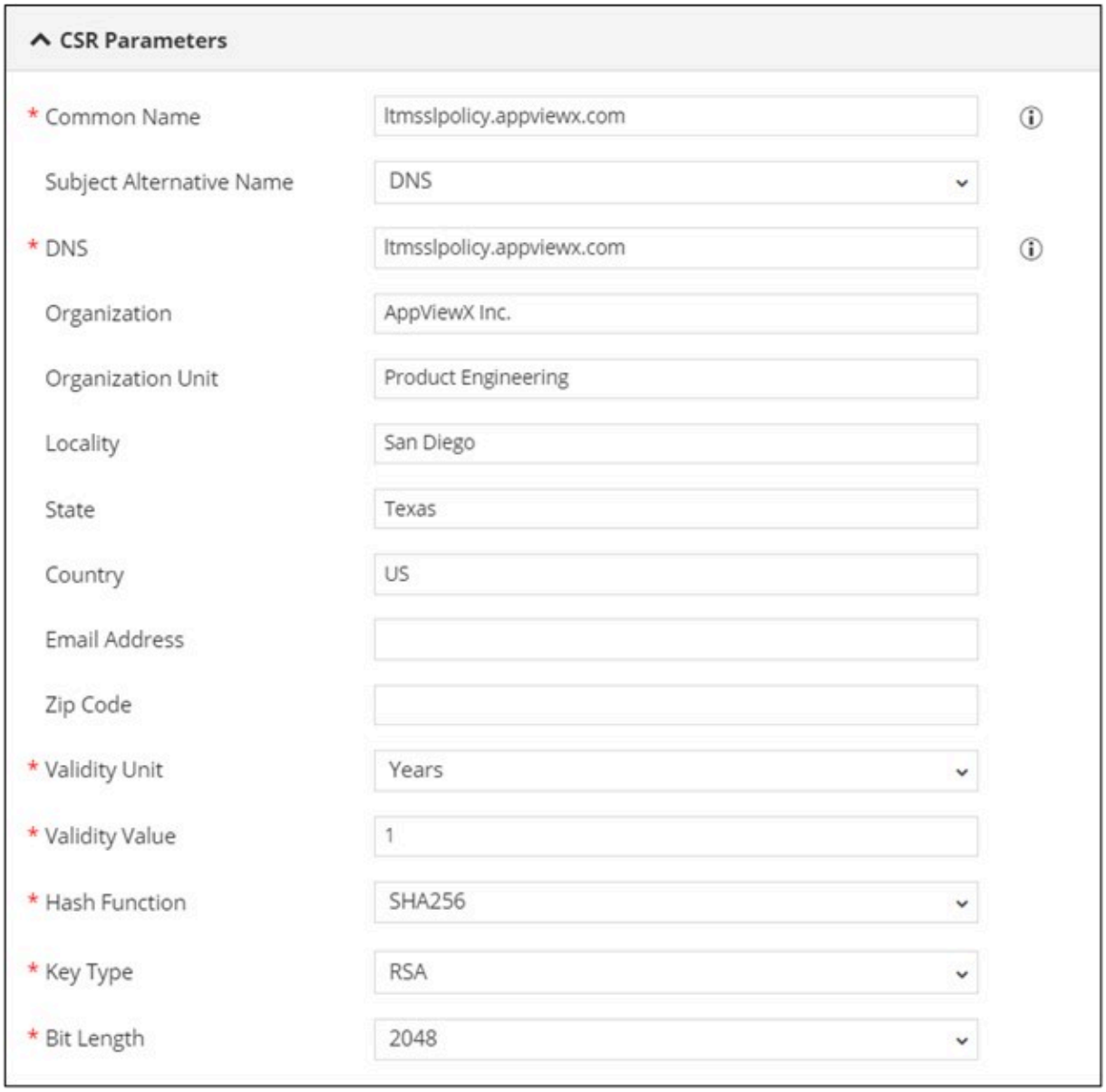


Policy Based

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

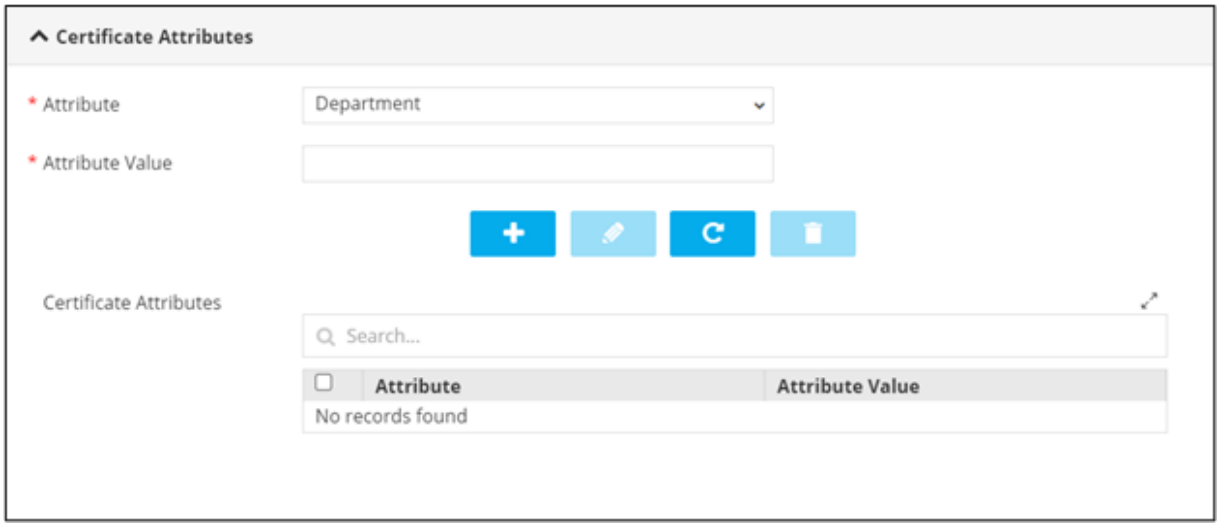
1. Under the **CSR Parameters** section, enter the field information as shown.

> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.

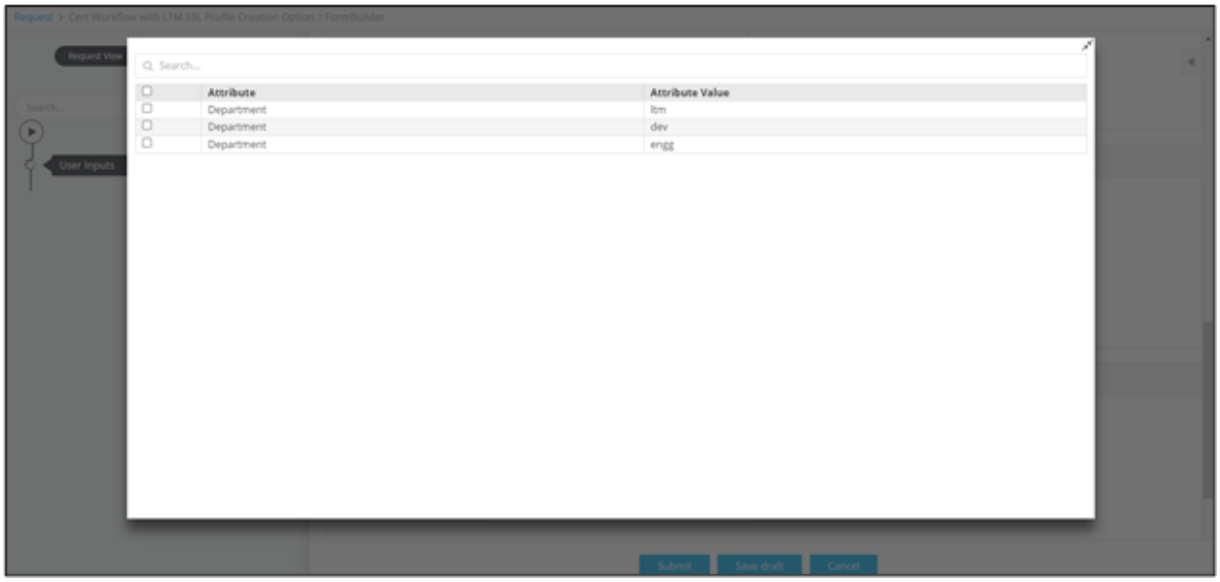


Note: For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



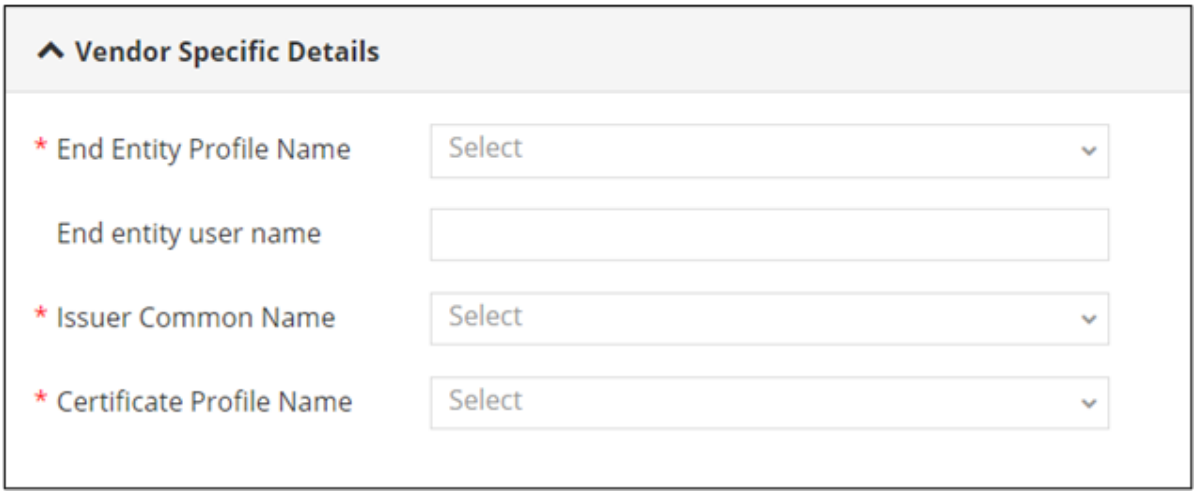
4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .
6. Enter the new value for the attribute in the **Value** field and click again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click .
8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

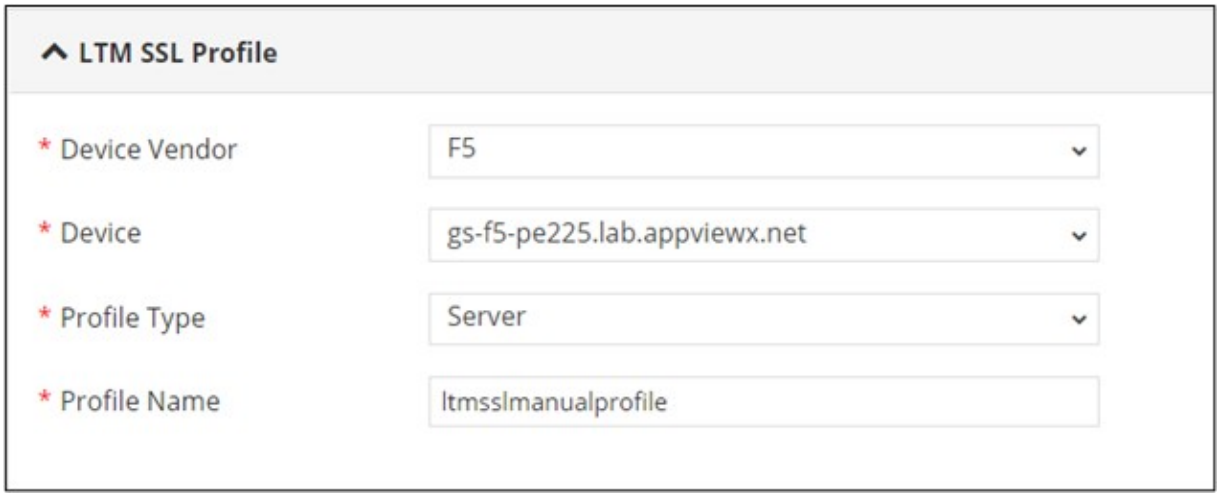
• When Digicert is selected as CA.

• When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

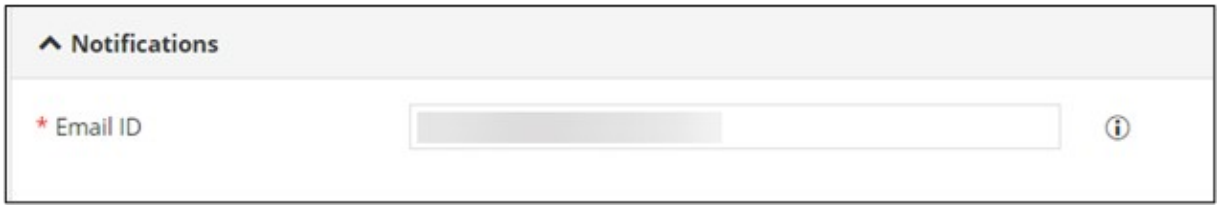
11. Under the **LTM SSL Profile** section, select the field information as shown.



The following table describes the field information in the **LTM SSL Profile** section:

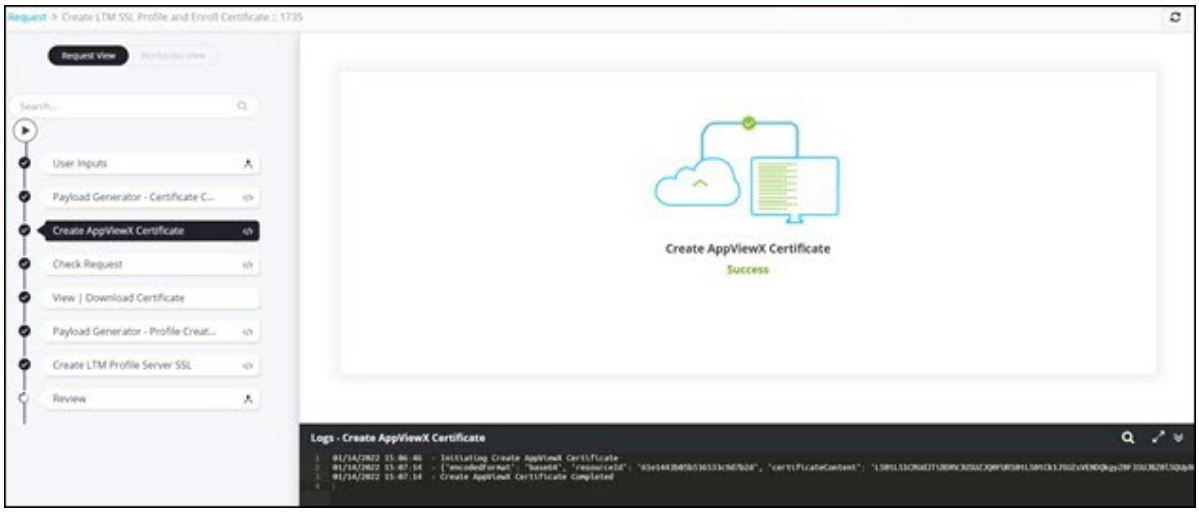
Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

12. Under the **Email Notification** section, enter the email address(es).

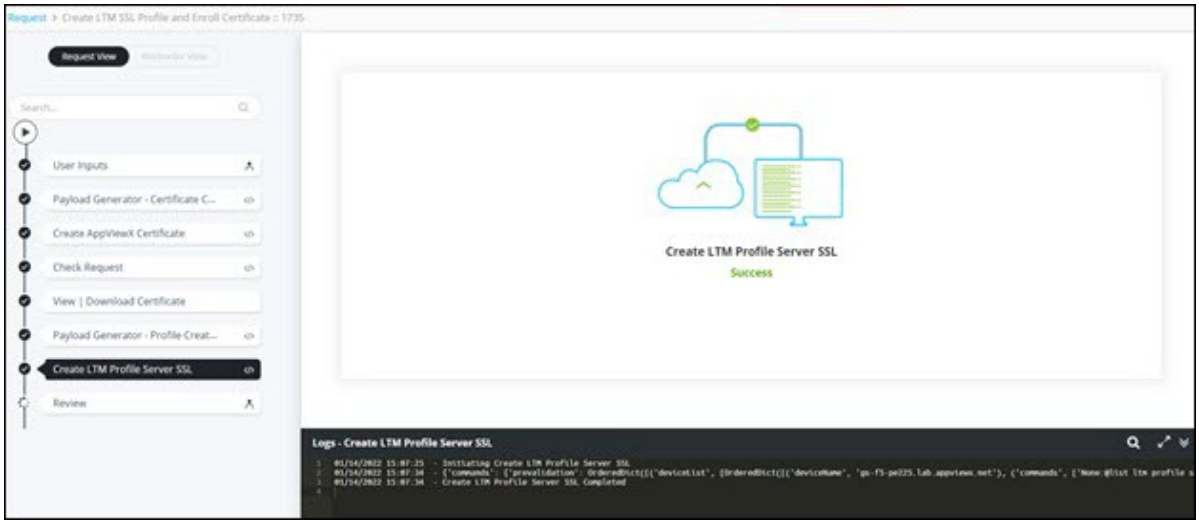


Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

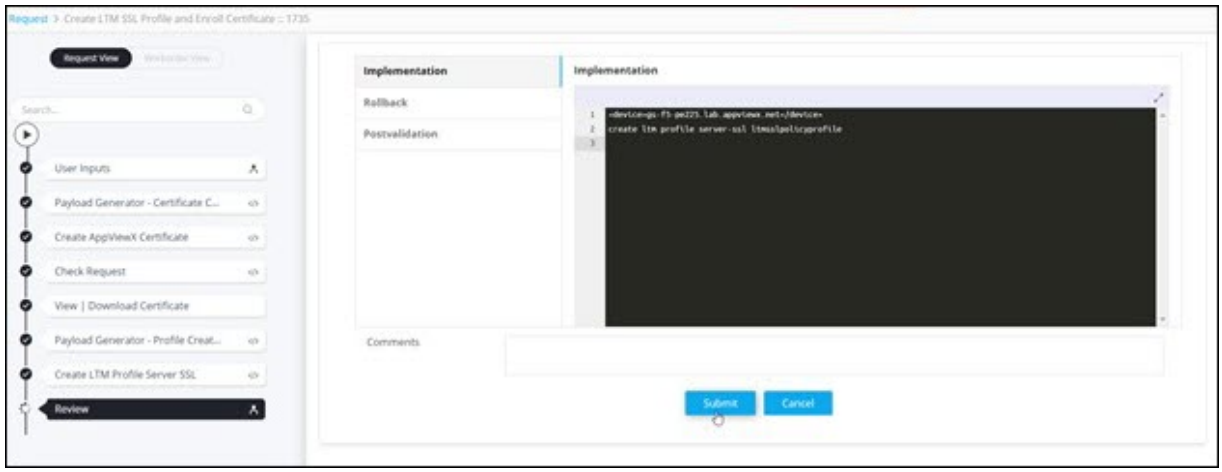
13. Click **Submit**.
    - AppViewX Certificate is generated successfully.



    - LTM Profile on Server SSL created successfully.

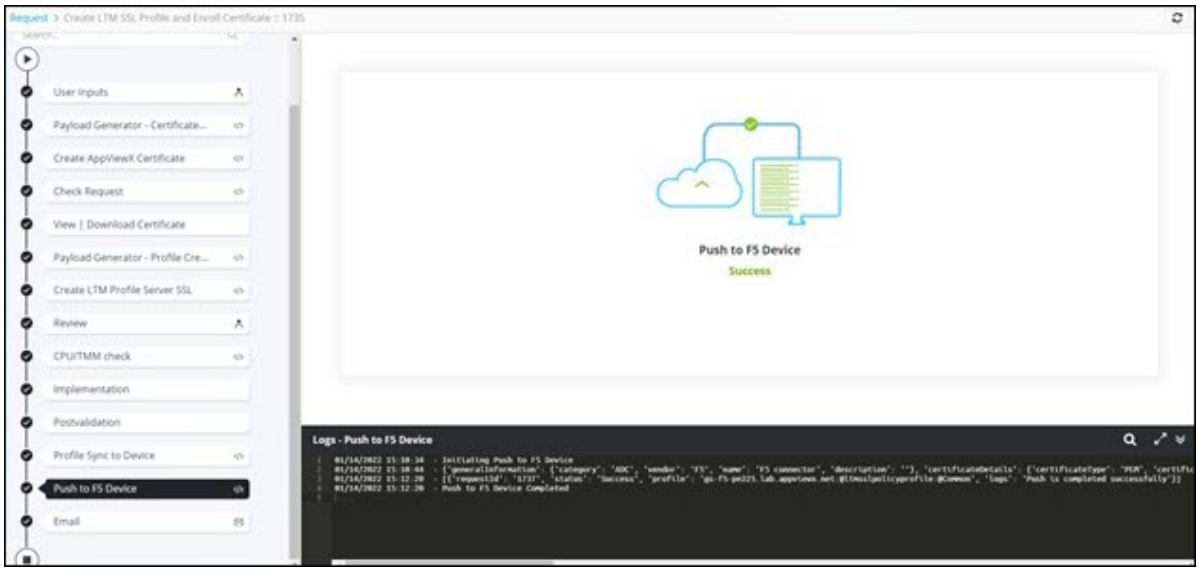


14. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

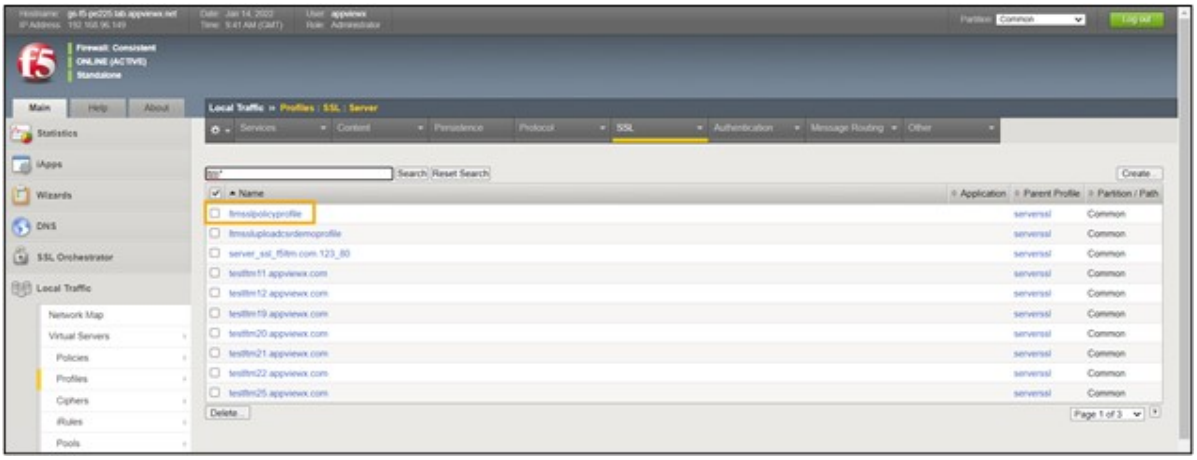


Note: You can change the profile name at this stage.

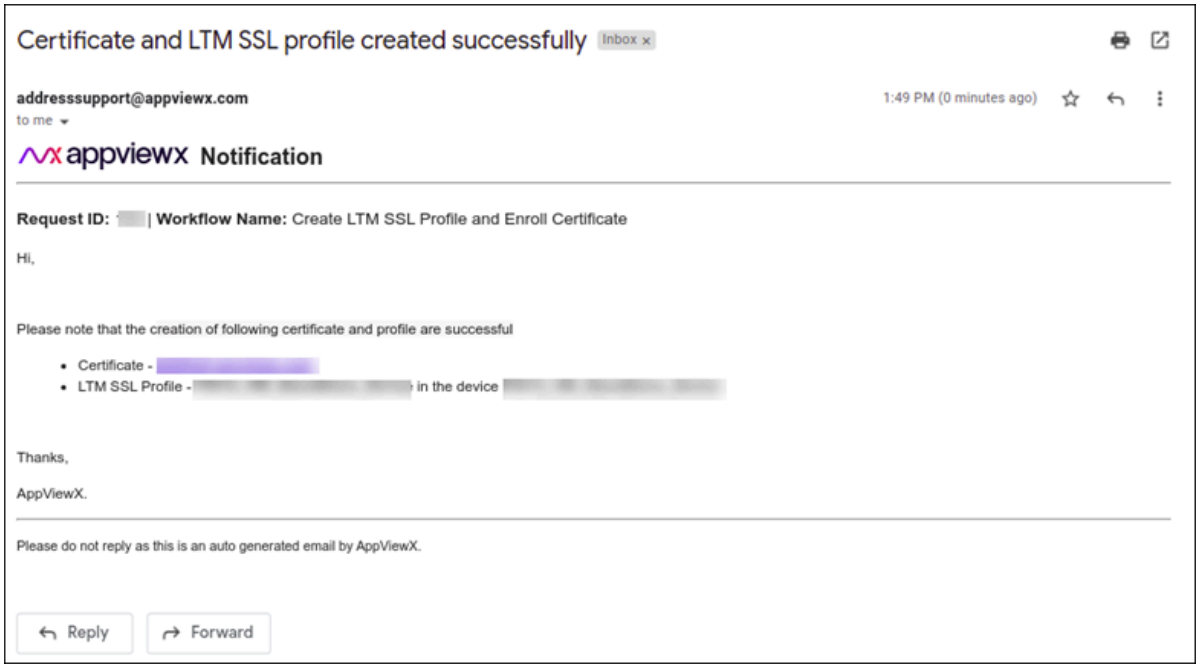
- Profile created on the selected F5 device.



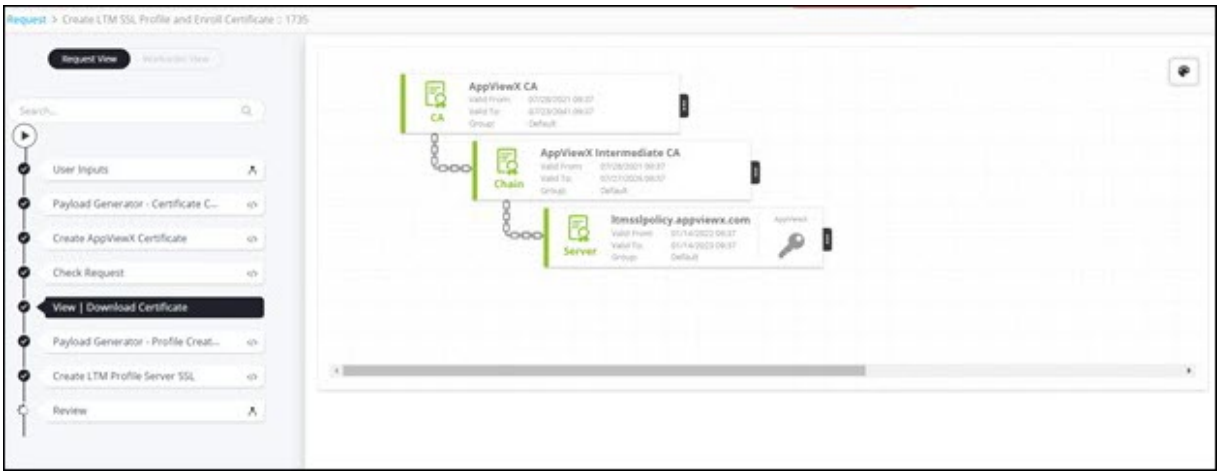
- Profile pushed to the selected F5 device.



- Email notification received.



15. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

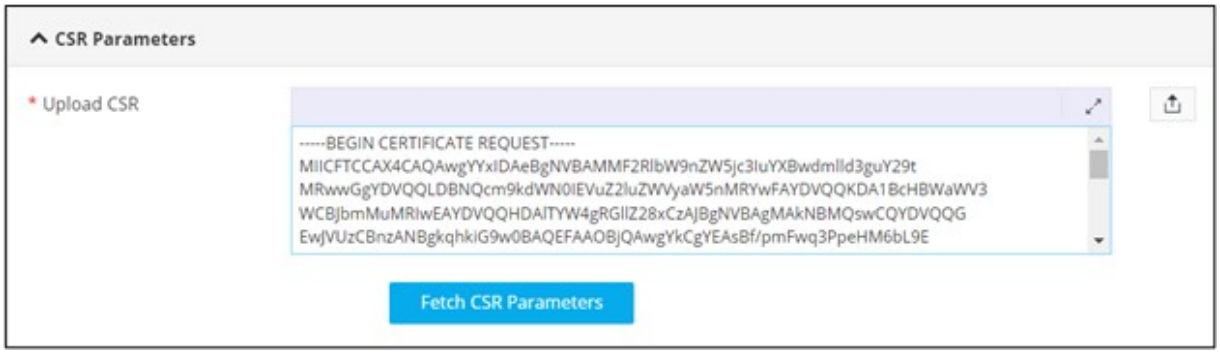


16. Hover your mouse over  to view the **Certificate status**.

Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

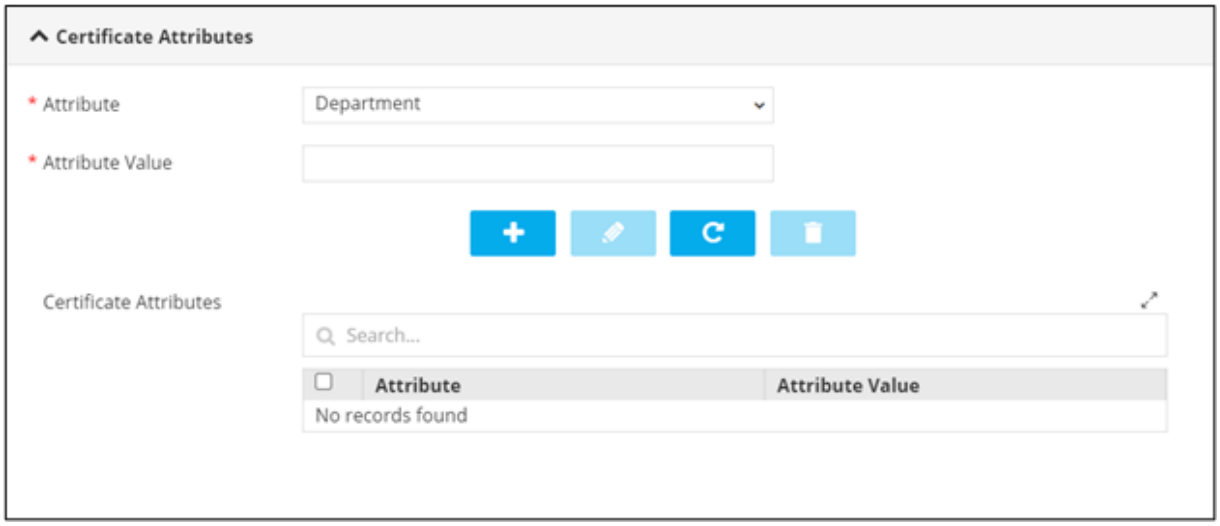
1. Under the **CSR Parameters** section, to **Upload CSR**, click  .



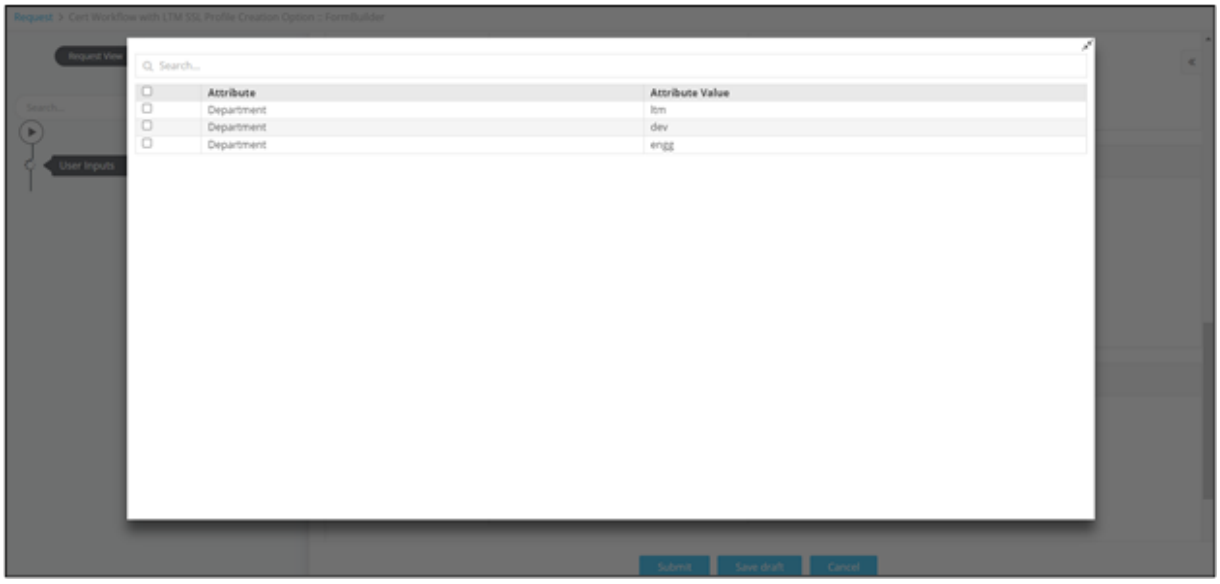
2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.

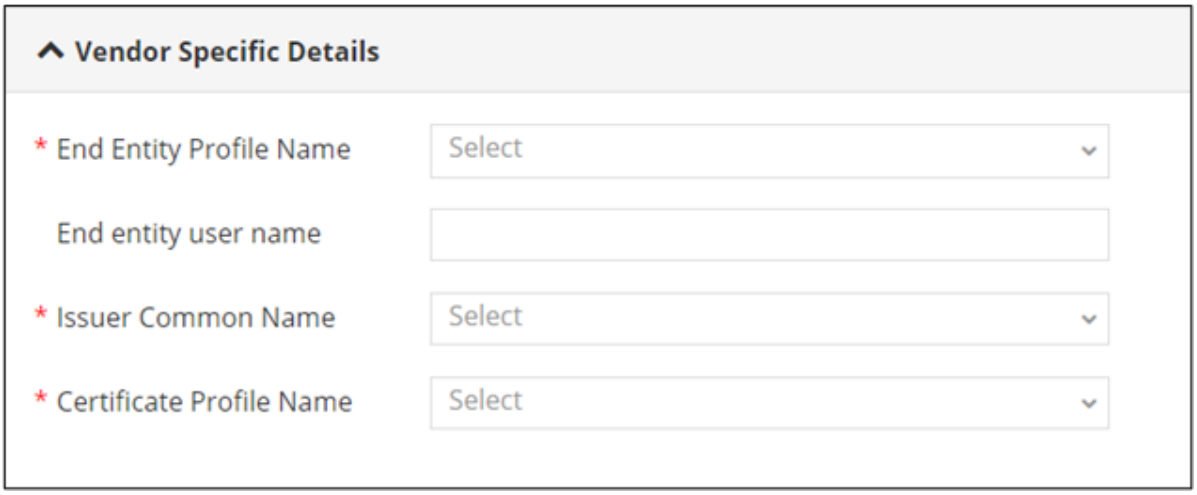


5. To add this attribute to the **Certificate Attributes** grid, click  .
6. To edit the value of a particular attribute, select the attribute in the grid and click  .
7. Enter the new value for the attribute in the **Value** field and click  again to update the value.
8. To delete a certificate attribute, select the attribute in the grid and click  .
9. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



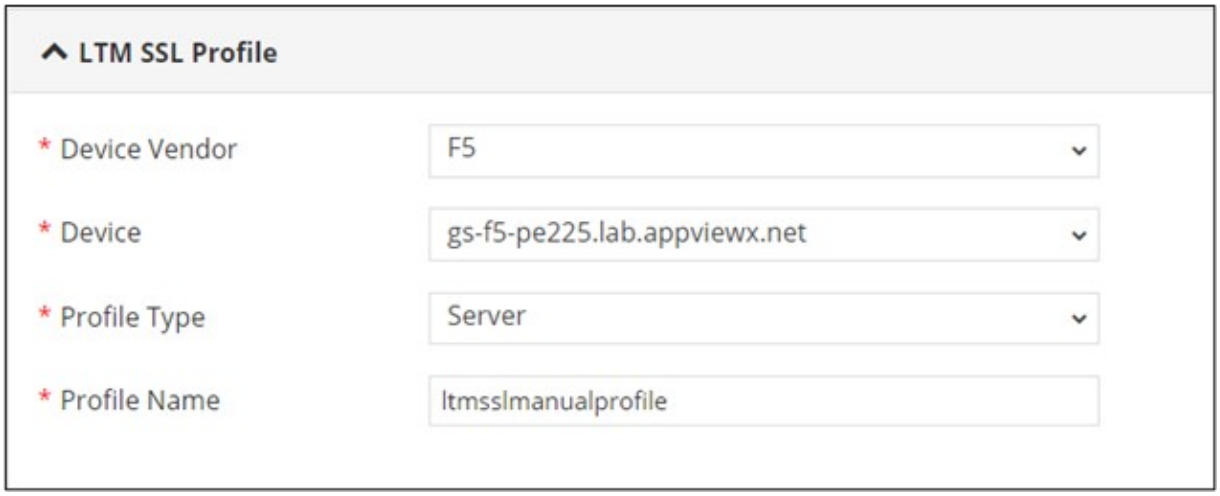
10. To search for a particular attribute in the grid, type the keyword(s) in the search field.
11. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

12. Under the **LTM SSL Profile** section, select the field information as shown.

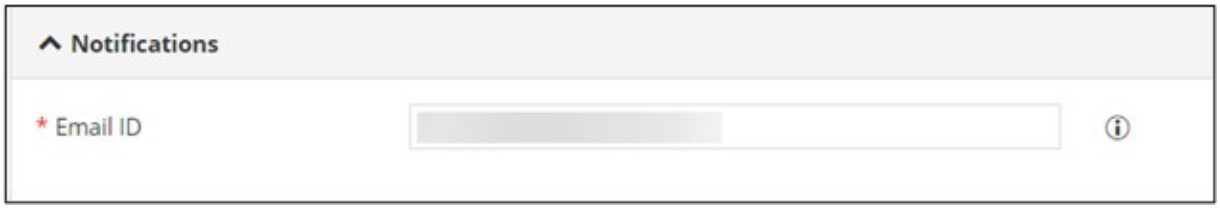


The following table describes the field information in the **LTM SSL Profile** section:

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown.

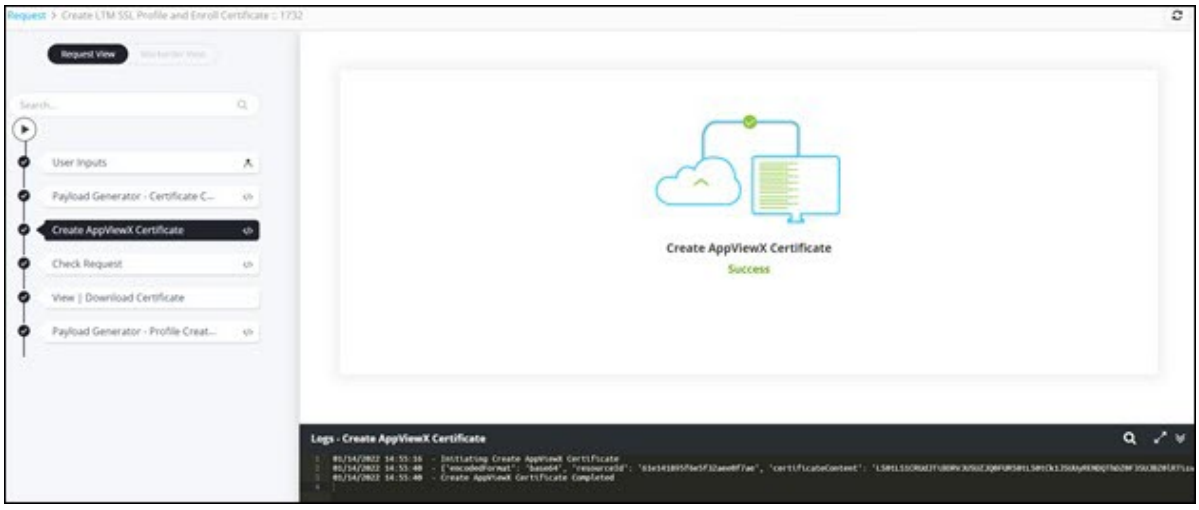
Field	Description
	Note: This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

13. Under the **Email Notification** section, enter the email address(es).



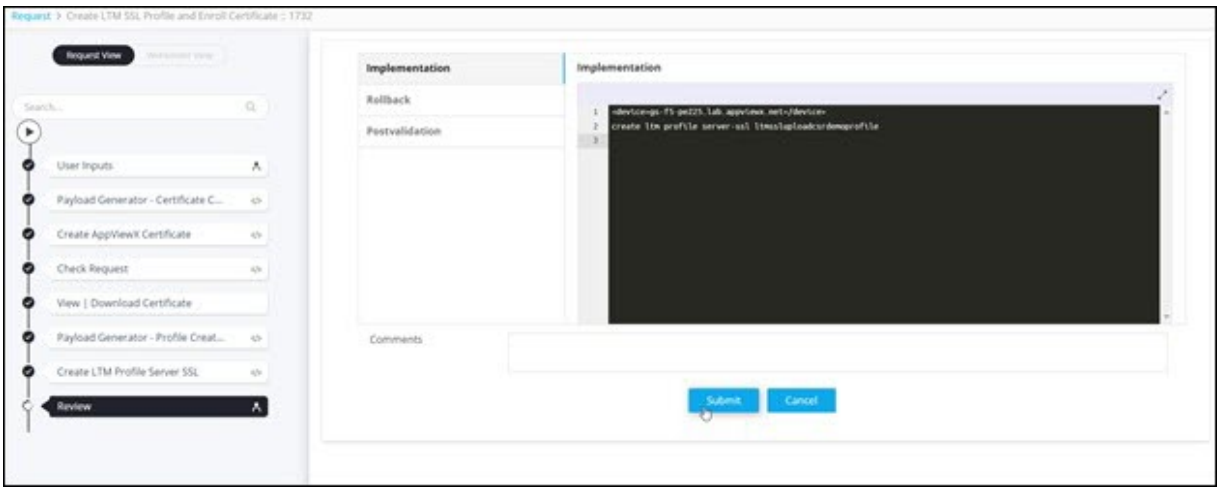
Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

14. Click **Submit**.
    - AppViewX Certificate generated.



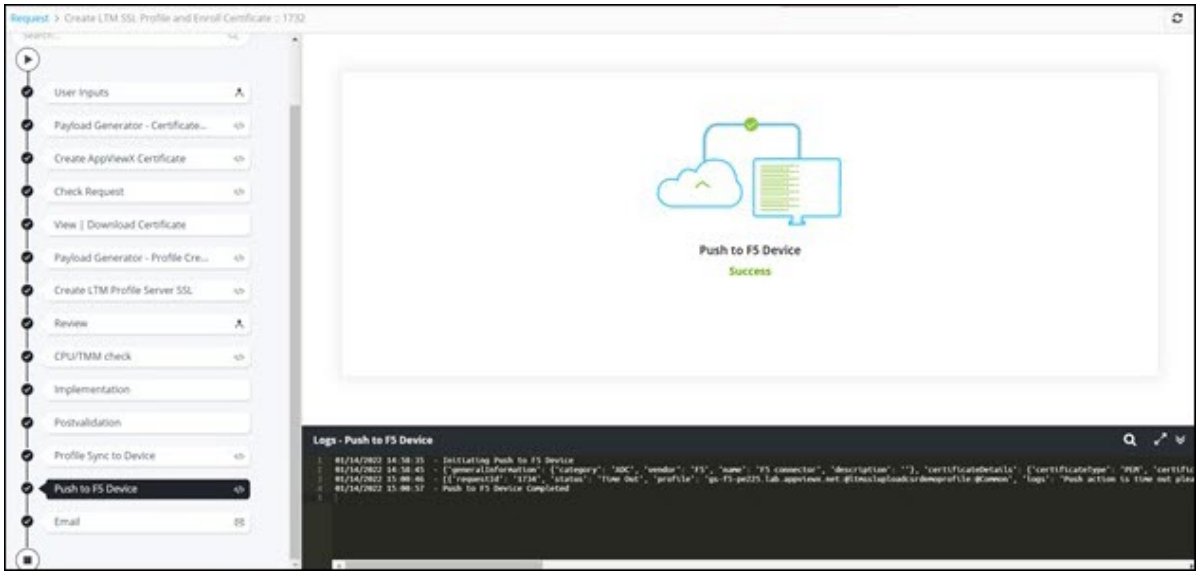
    - LTM Profile on Server SSL created successfully.

15. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

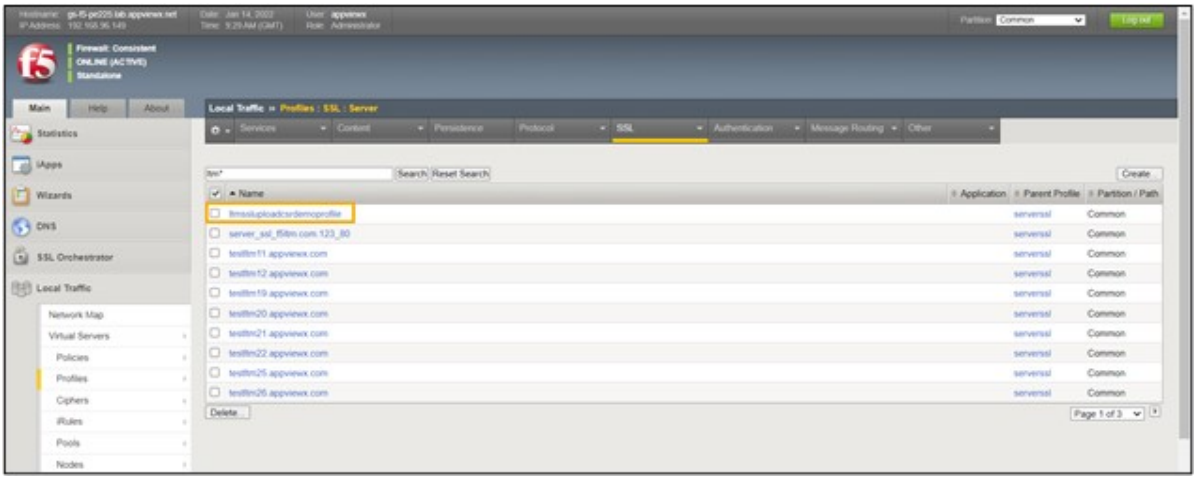


Note: You can change the profile name at this stage.

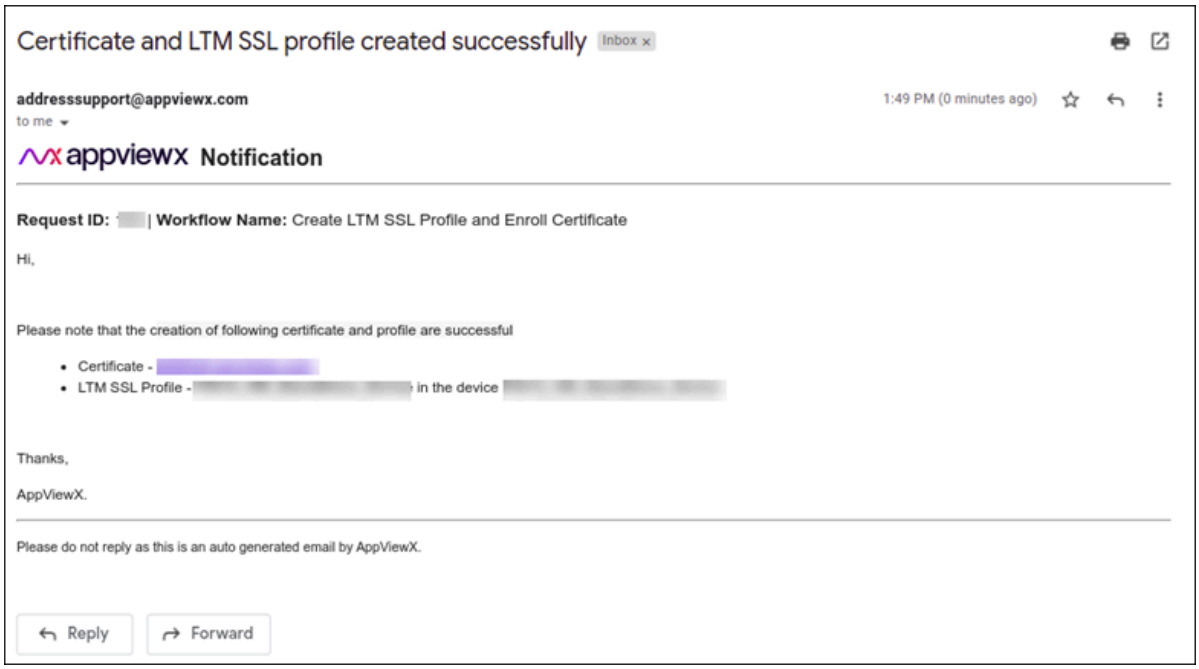
- Profile created on the selected F5 device.



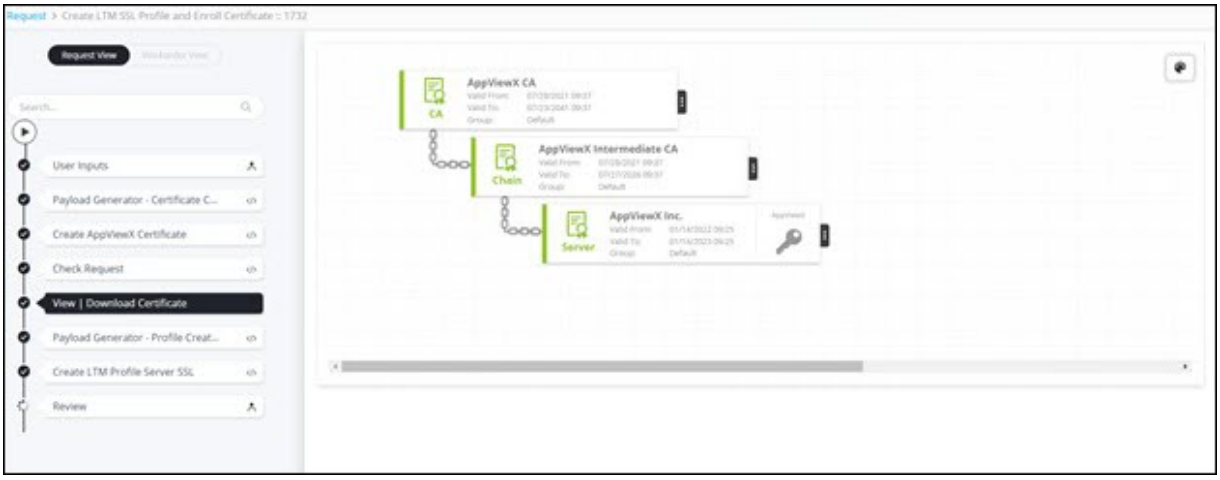
- Profile pushed to the selected F5 device.



- Email notification received.



16. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



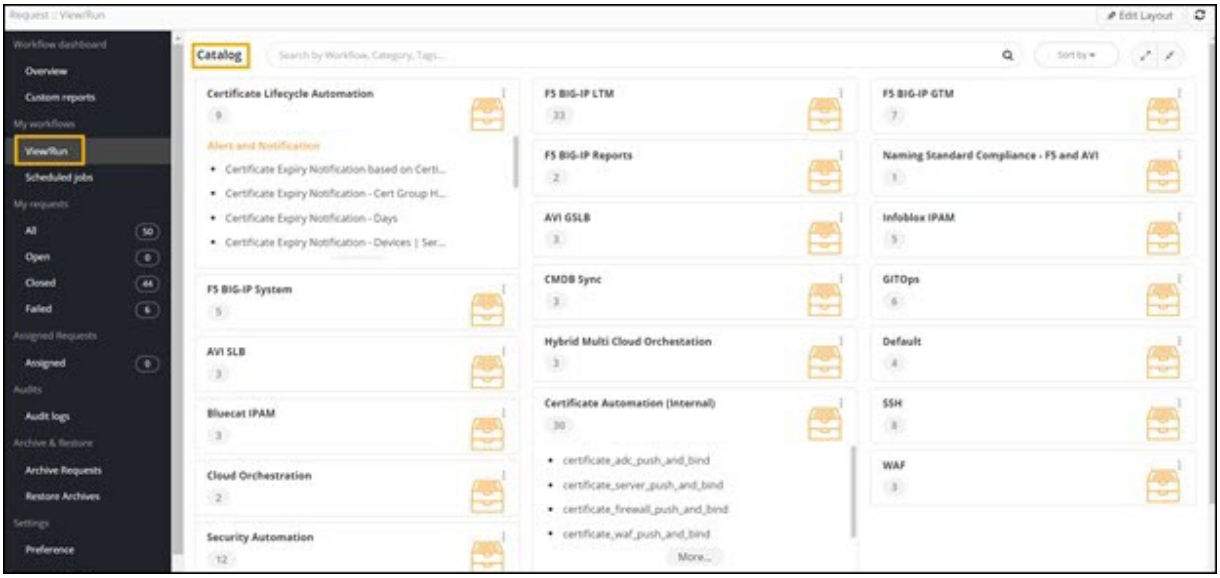
17. Hover your mouse over  to view the **Certificate status**.

Enroll Certificate with Certificate Group and CSR Upload

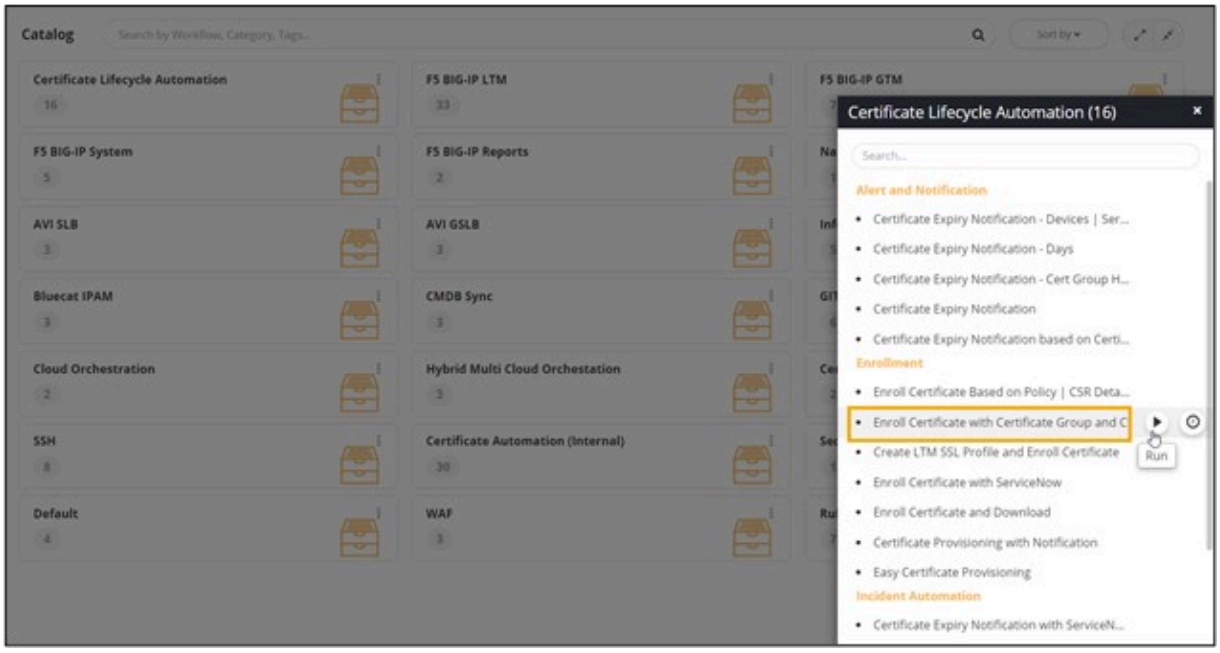
This workflow allows you to create a certificate with minimal input. The Certificate Authority (CA) must be associated with the respective policy and Certificate group. In case there are multiple CAs associated with a policy, the first available CA will be considered for certificate creation.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

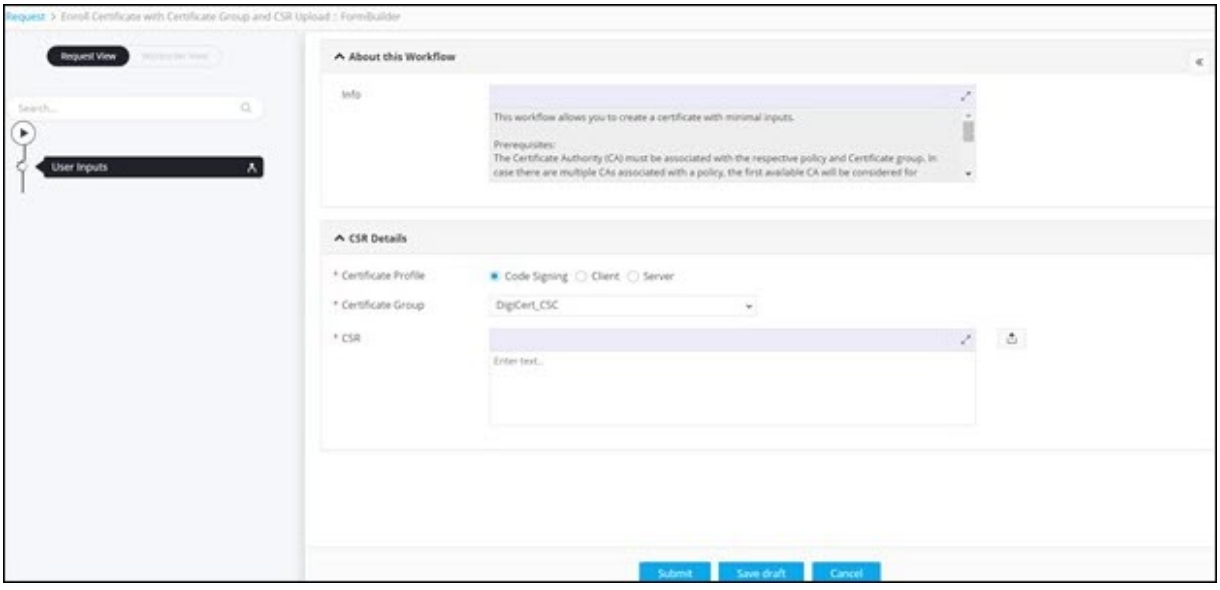


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with Certificate Group and CSR Upload** workflow and click .

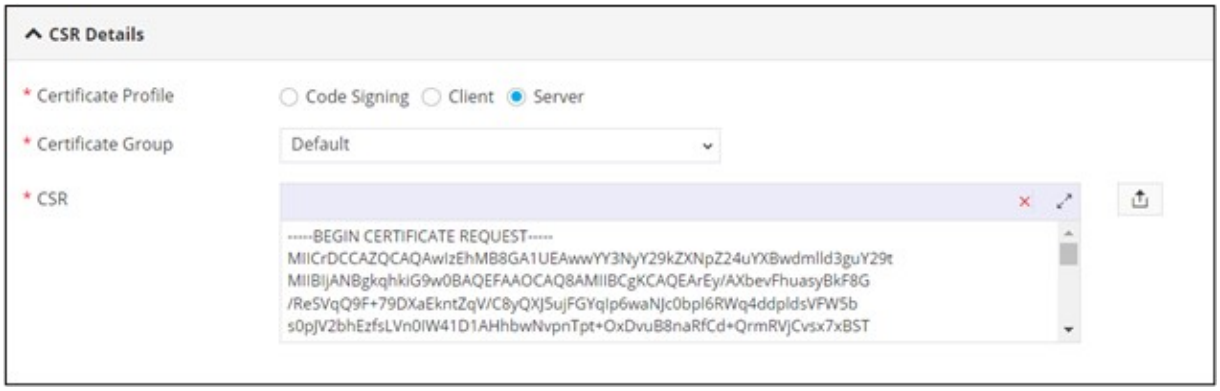


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **CSR Details** section, select the following information:

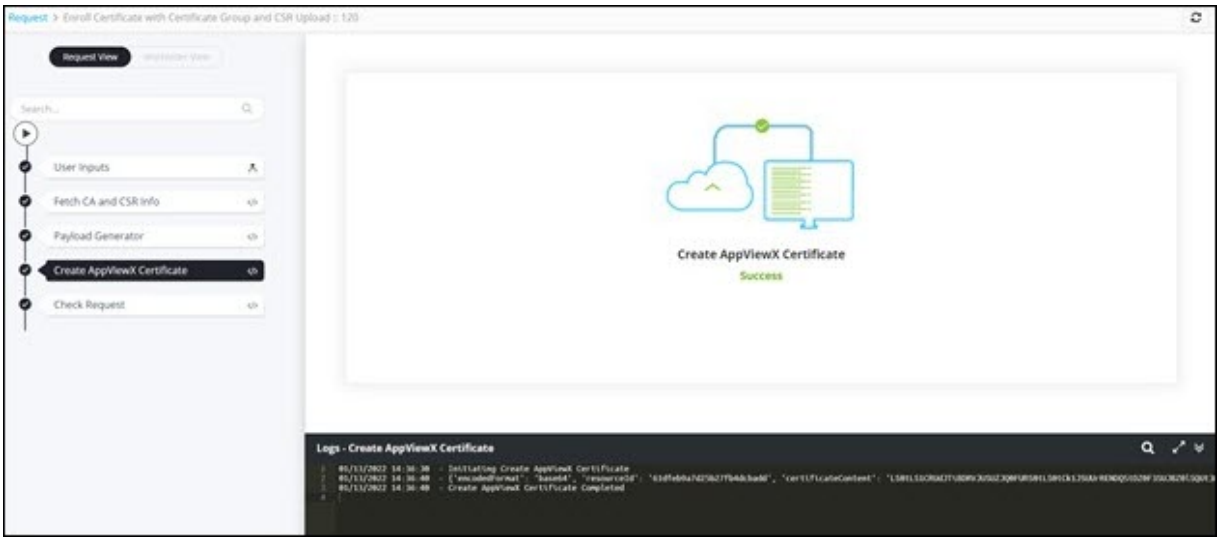


The following table describes the fields in the **CSR Details** section:

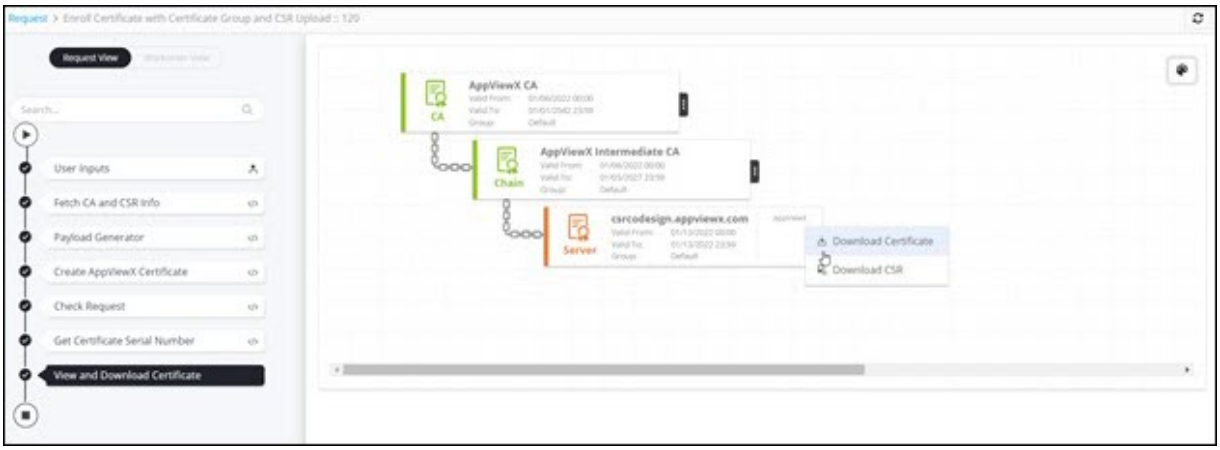
Field	Description
***Certificate Profile**	Select the **Certificate Profile** from the following options: • **Code Signing** • **Server** • **Client** **Note**: **Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***CSR**	Click to upload the **CSR** file.
All asterisk(*) marked fields are mandatory.	

6. Click **Submit**.

   AppViewX Certificate is generated successfully.



7. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  , and from the options displayed, click **Download Certificate**.



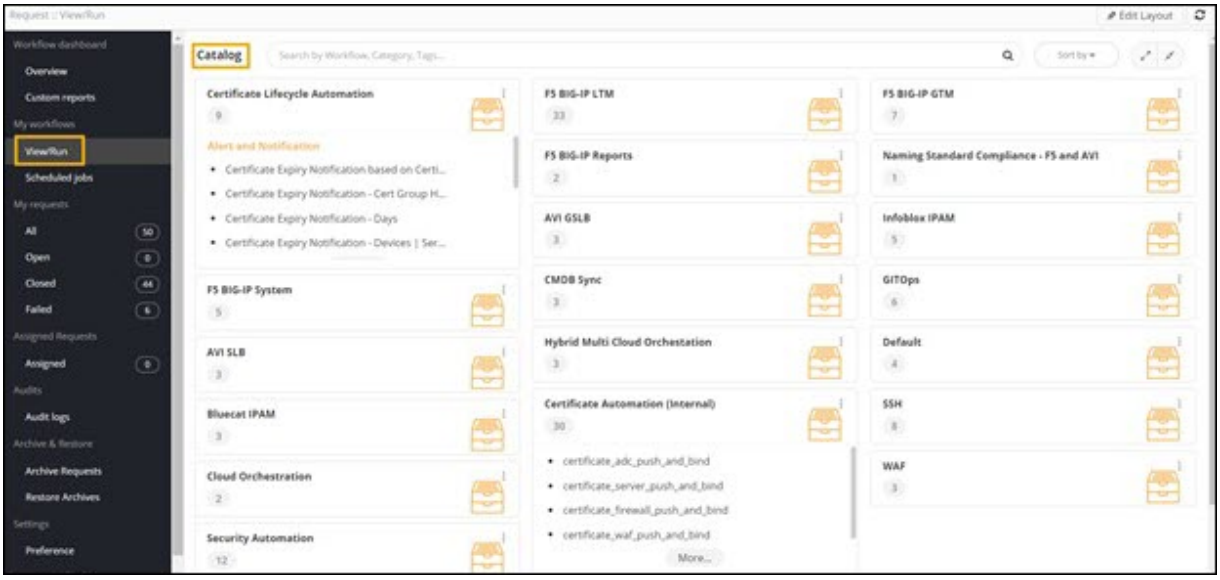
8. Hover your mouse over  to view the Certificate status.

Enroll Certificate With ServiceNow

This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM).

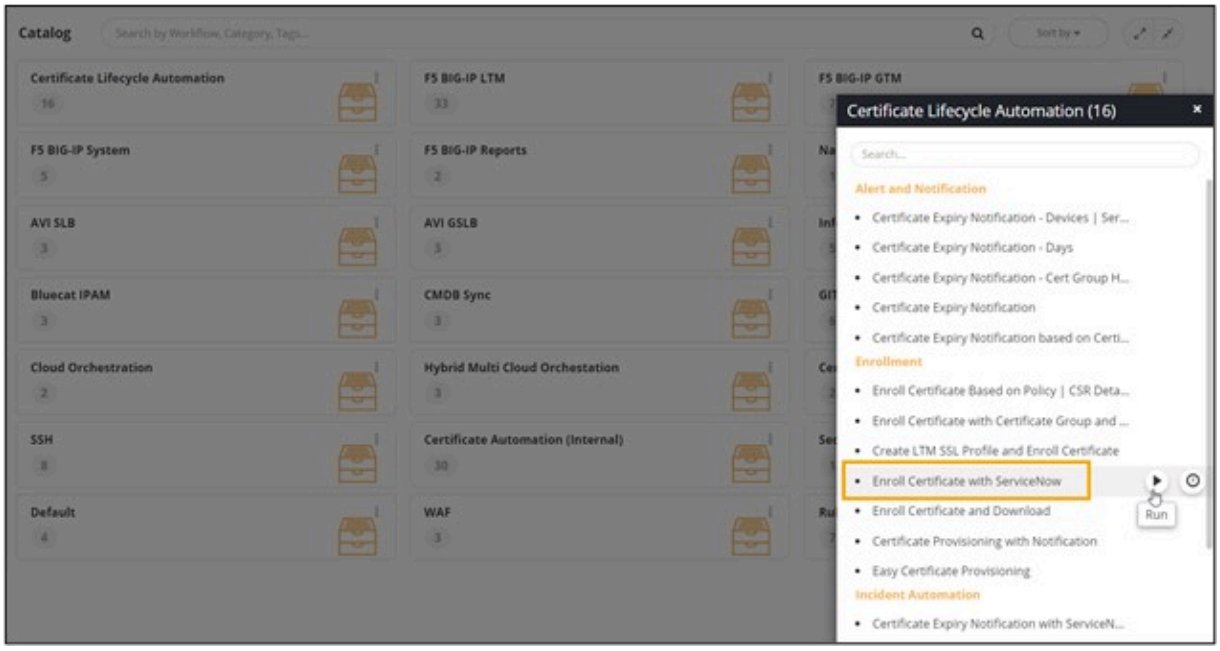
To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.



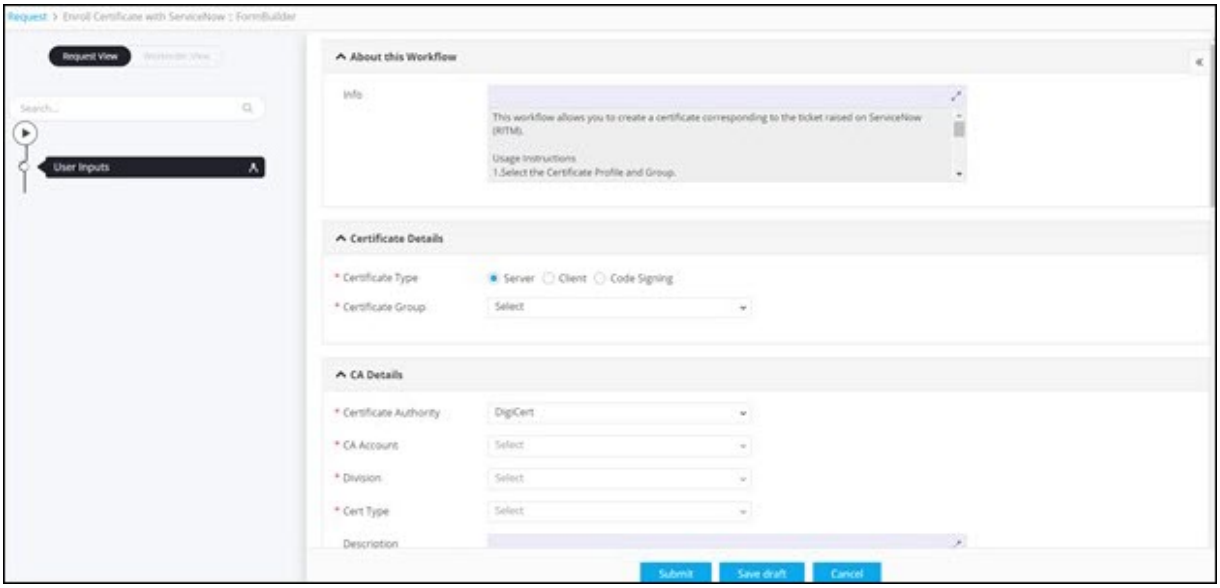
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click ⋮ .
3. From the options displayed, select **Full View**.

4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with ServiceNow** workflow and click ▶.

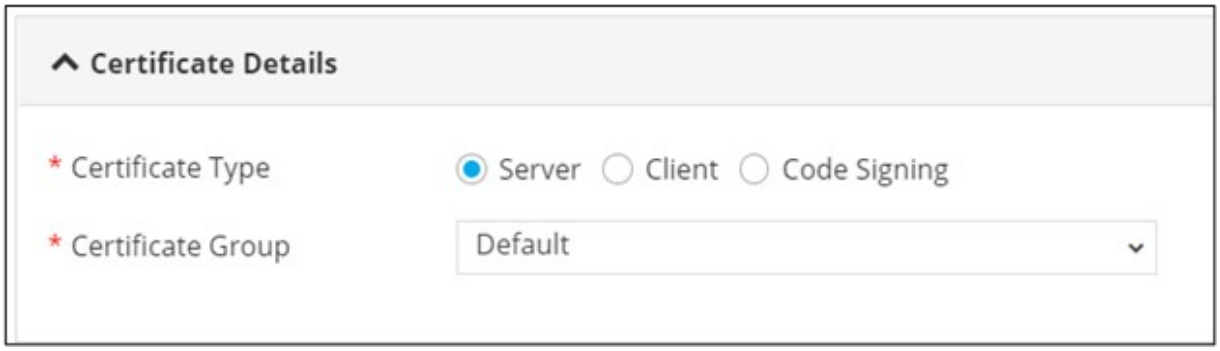


> **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



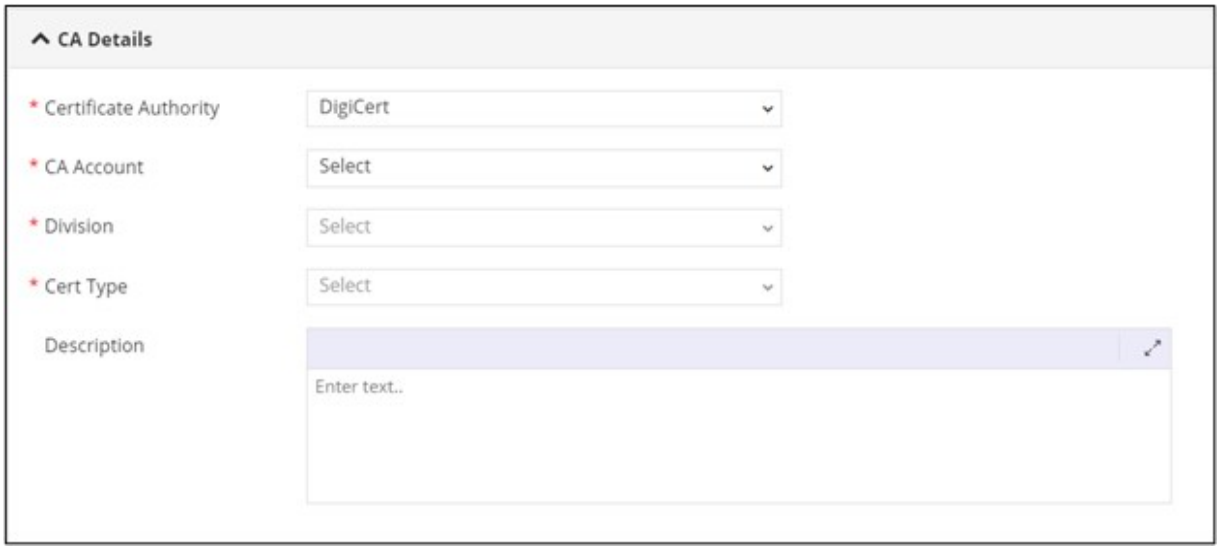
5. Under the **Certificate Details** section, select the following field information as shown.



The following table describes the field information under the **Certificate Details** section:

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note**: **Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

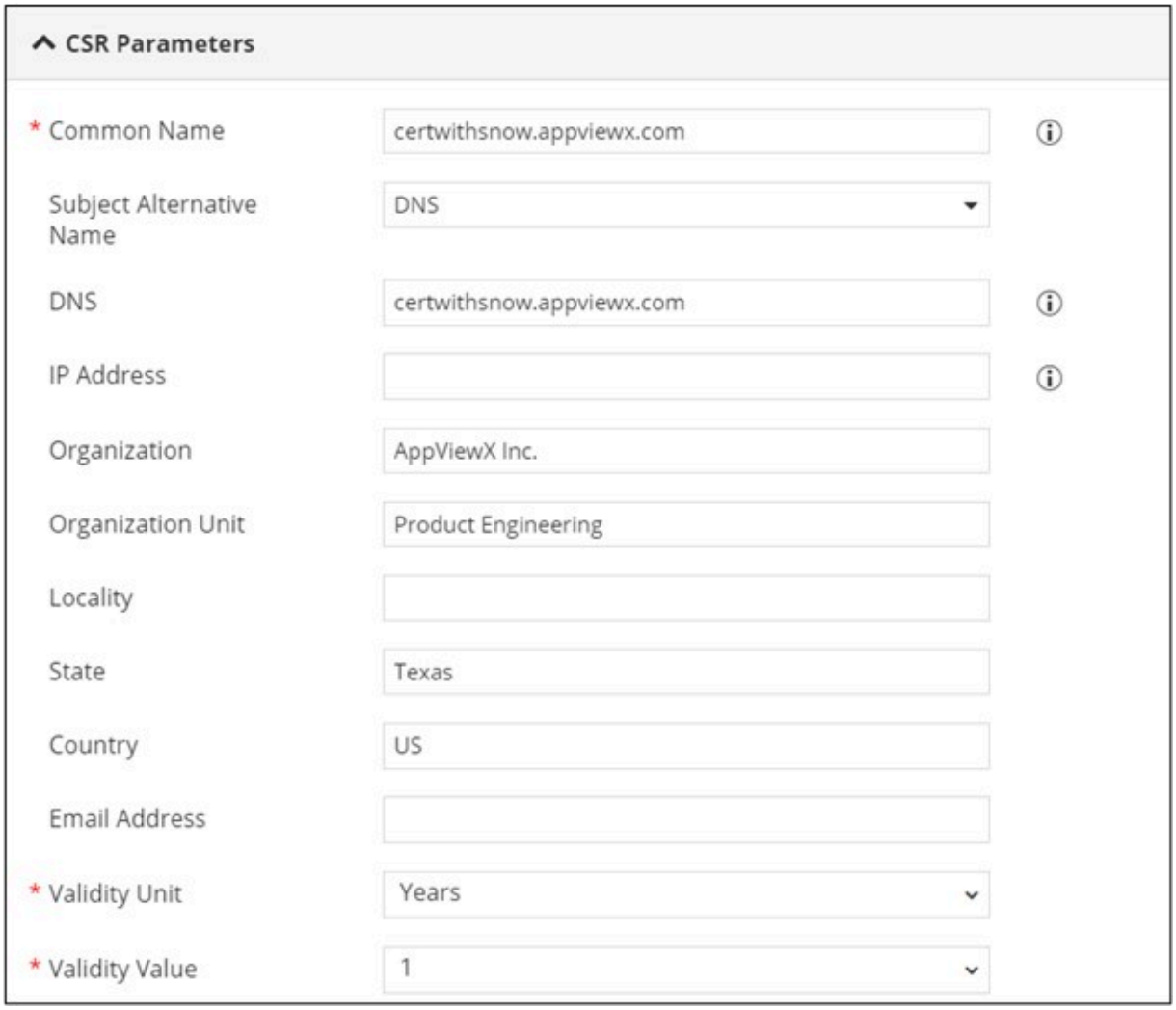
6. Under the **CA Details** section, enter or select the following field information:

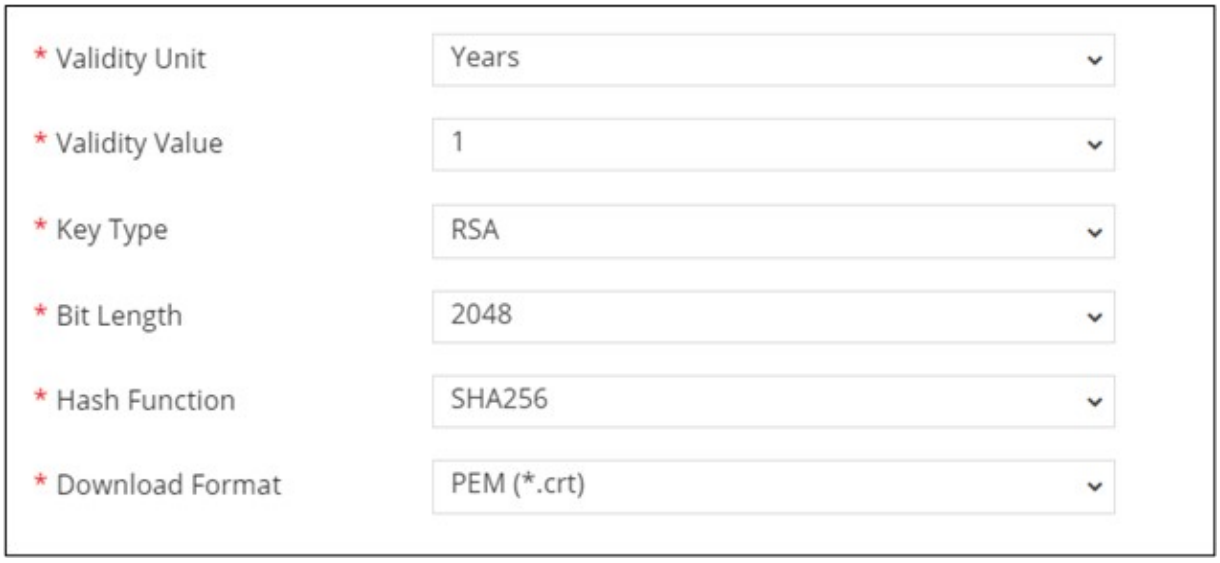


The following table describes the field information under the **CA Details** section:

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Provide a Description for the workflow, if required.
All asterisk (*) marked fields are mandatory.	

7. Under the **CSR Parameters** section, enter or select the following field information:



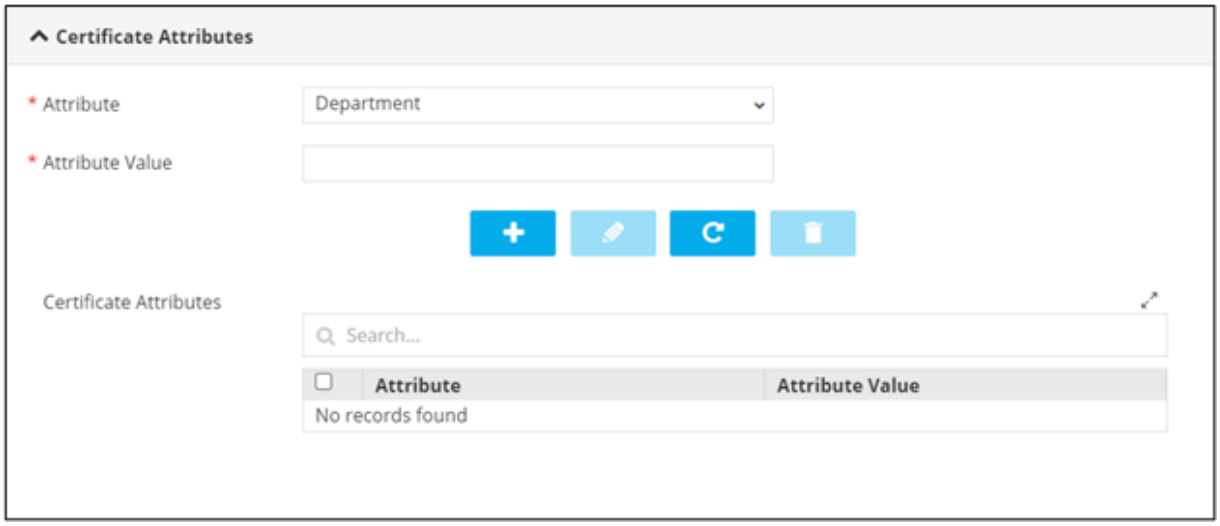


The following table describes the fields under the **CSR Parameters** section:

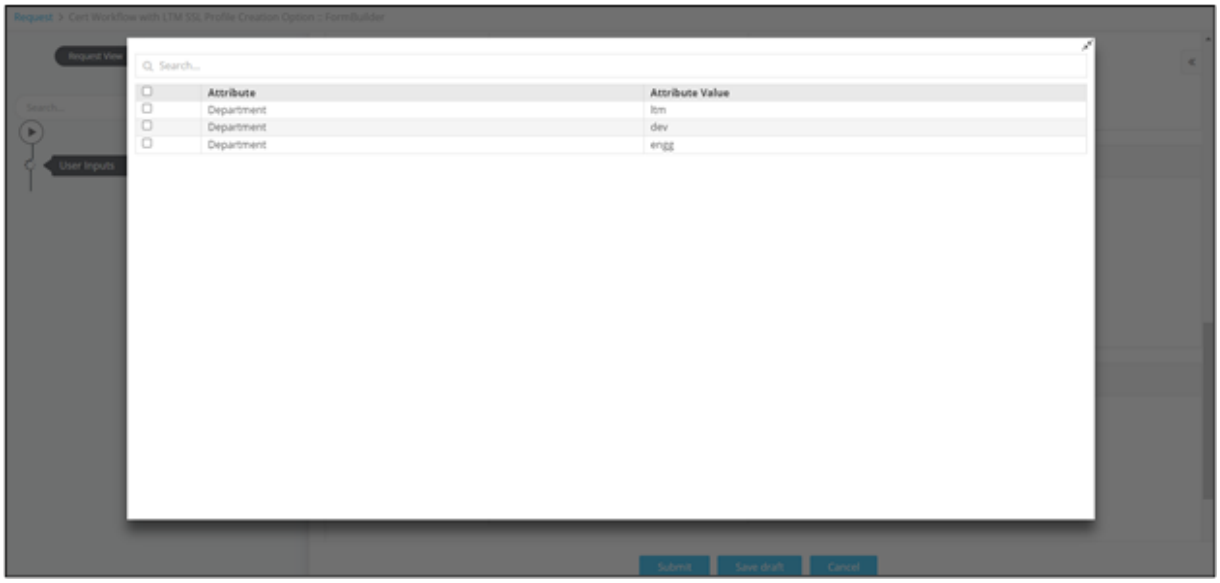
Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.
***Subject Alternative Name (SAN)**	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
***Organization**	Enter the name of the organization .
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

Field	Description
	Note: This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.

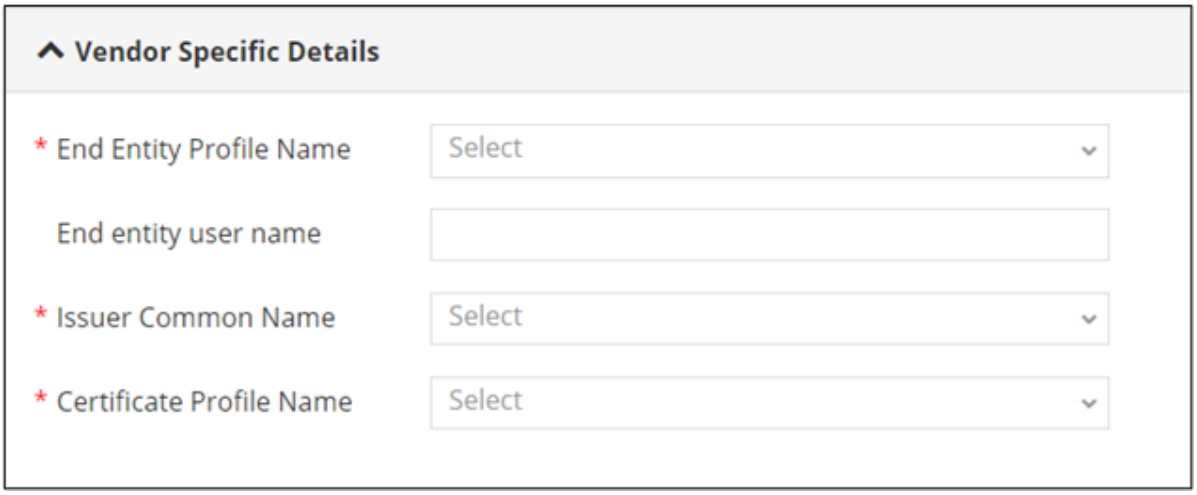


10. To add this attribute to the **Certificate Attributes** grid, click  .
11. To edit the value of a particular attribute, select the attribute in the grid and click  .
12. Enter the new value for the attribute in the **Value** field and click  again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click  .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

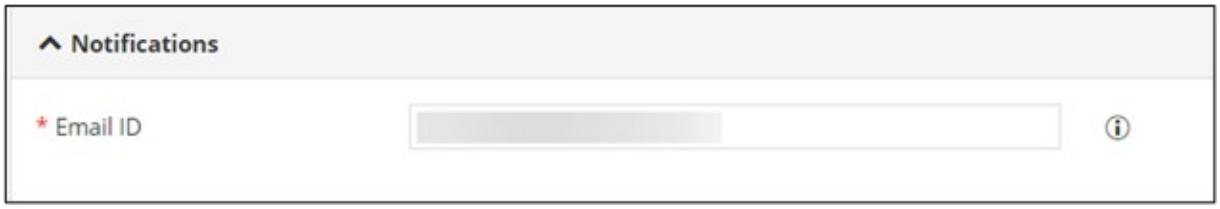
    - When EJBCA is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

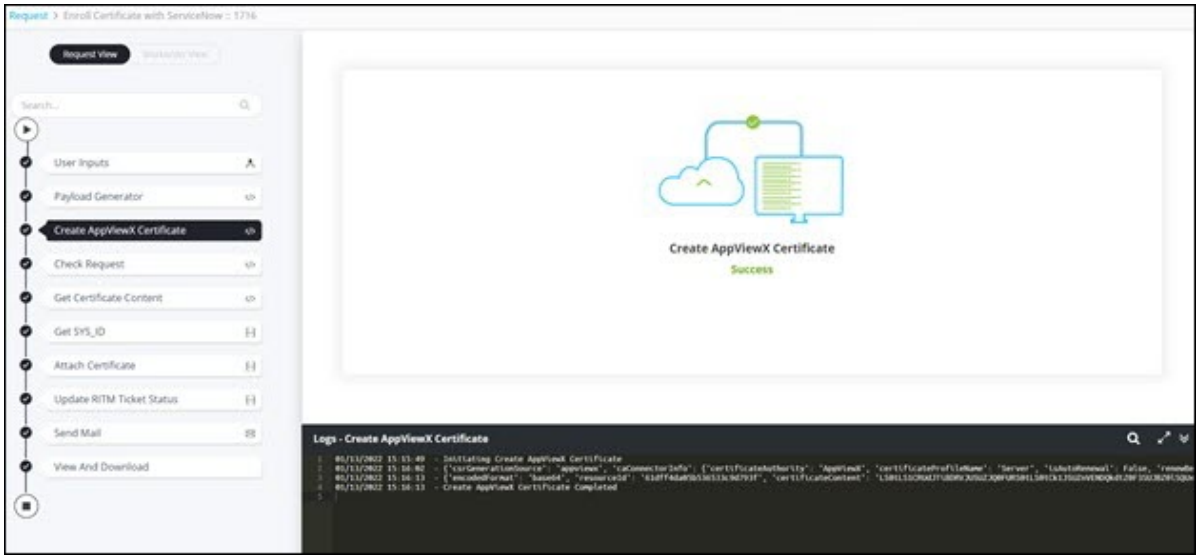
17. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
18. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).

19. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.



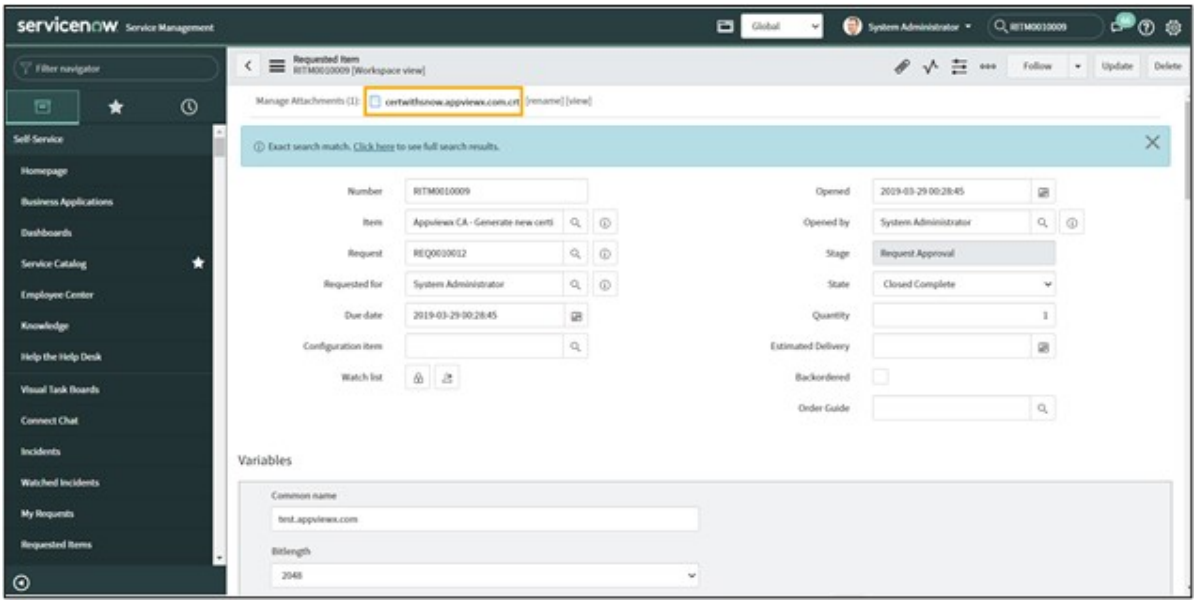
20. Click **Submit**.

• AppViewX Certificate is created successfully.

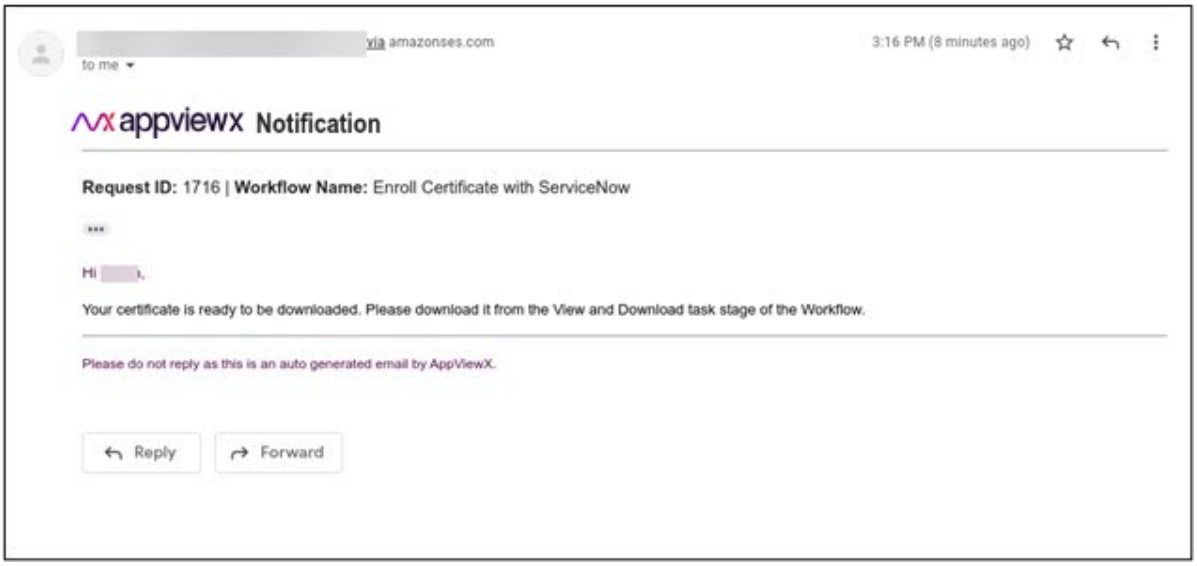


• RITM ticket status updated.

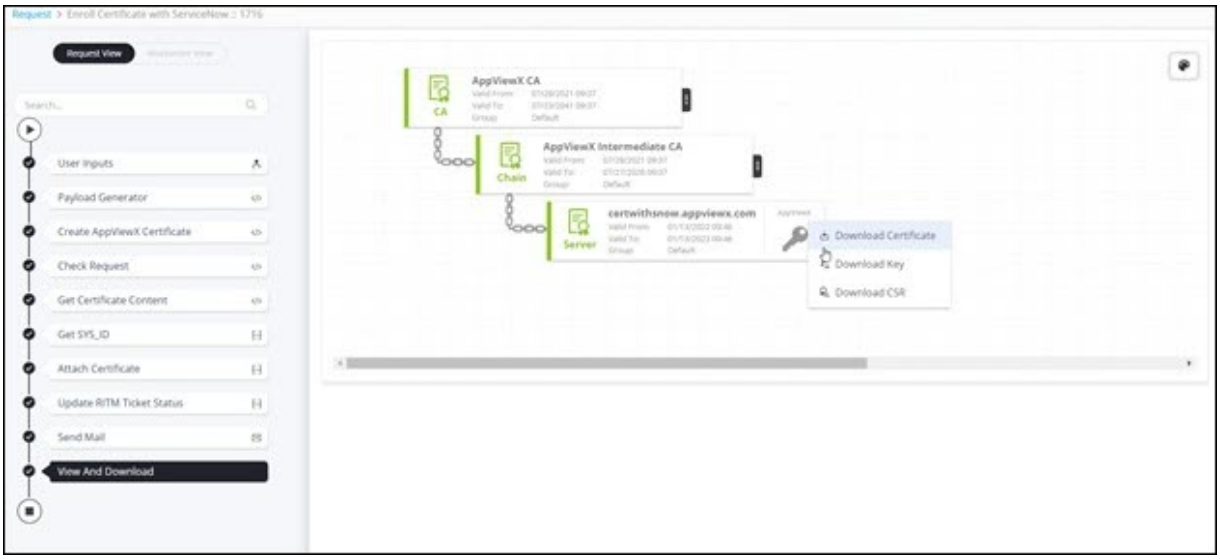
• Certificate updated in the ServiceNow ticket.



- Email notification received.



21. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.



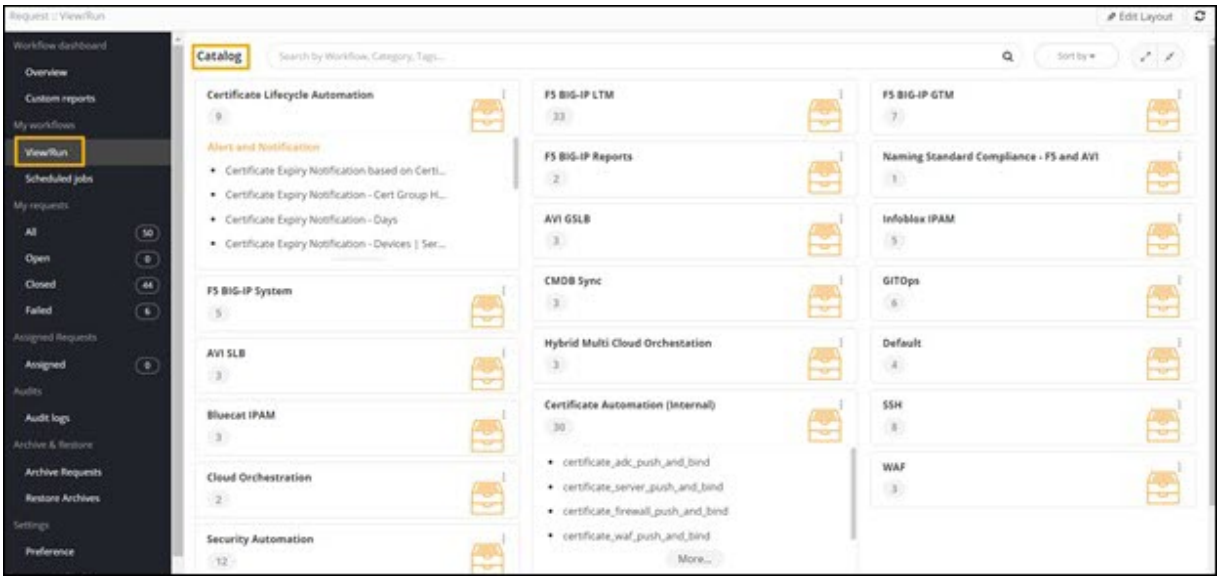
22. Hover your mouse over  to view the Certificate status.

Enroll Certificate and Push with ServiceNow

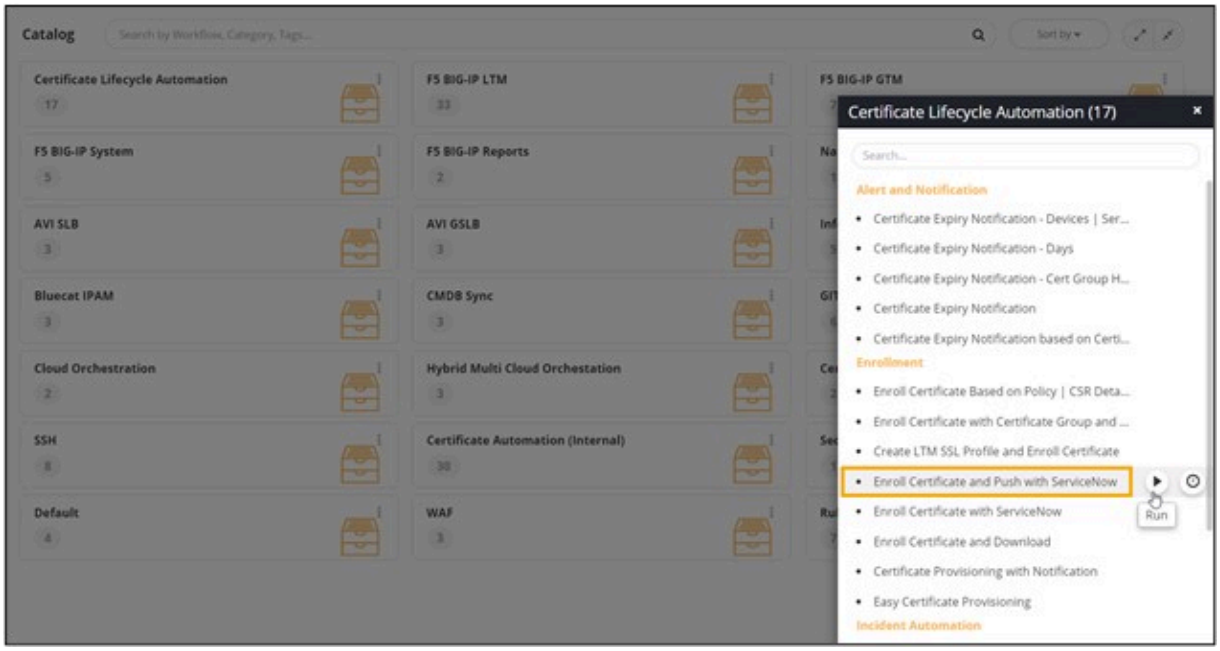
This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

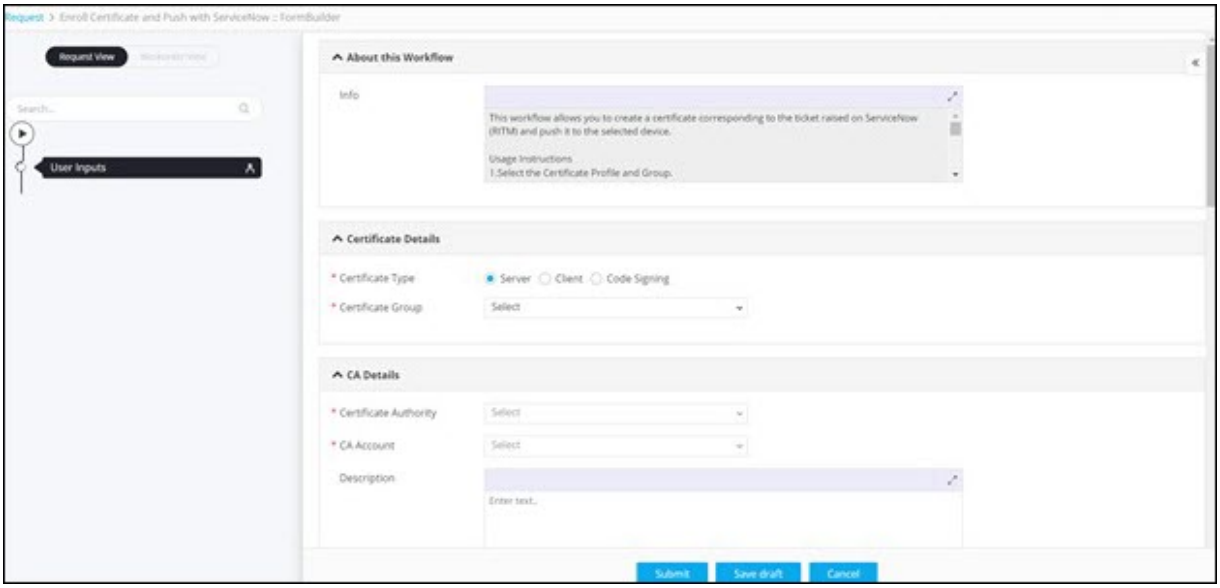


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click ⋮ .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push with ServiceNow** workflow and click ▶.

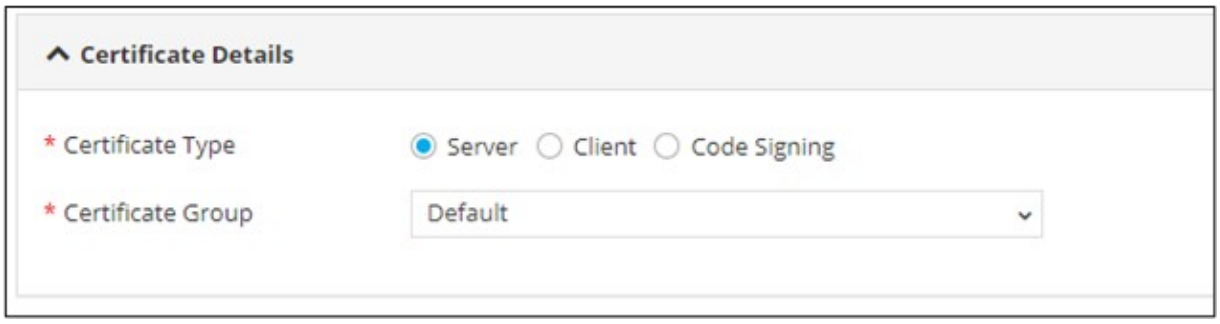


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **Certificate Details** section, select the following field information as shown.

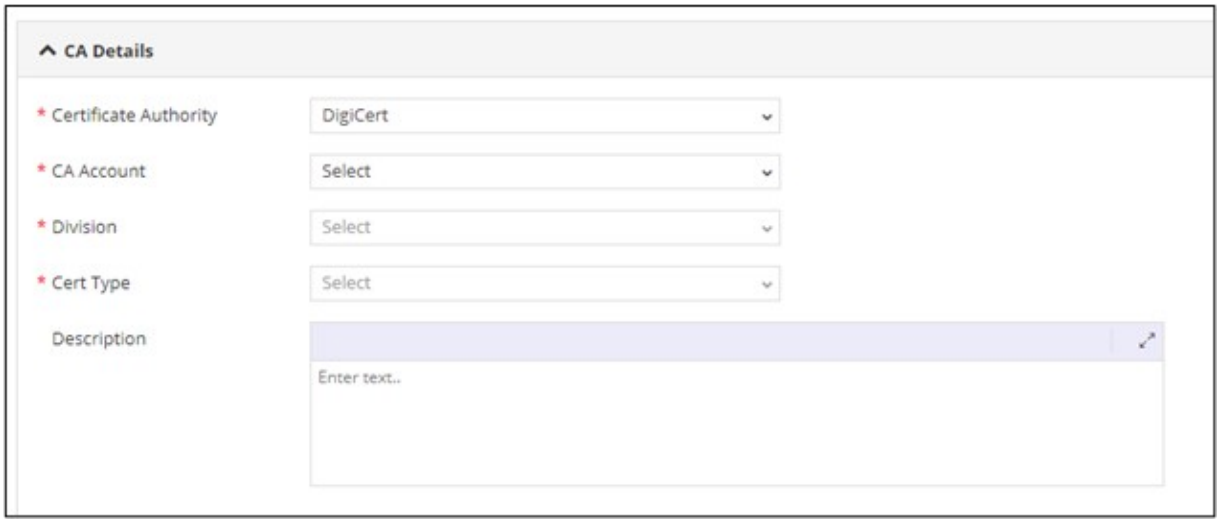


The following table describes the field information under the **Certificate Details** section:

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note**: **Server** is the default selection.

Field	Description
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

6. Under the **CA Details** section, enter or select the following field information:

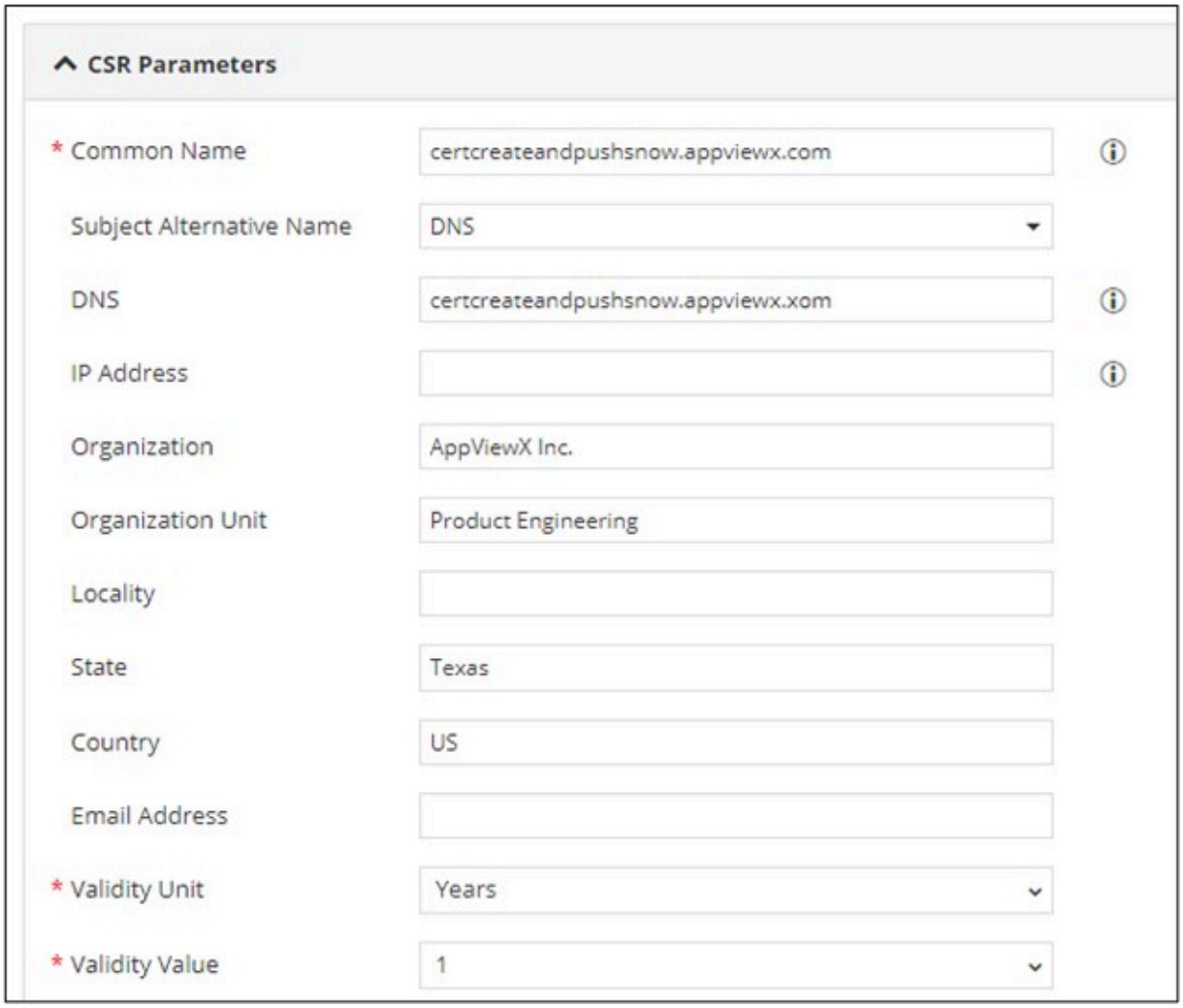


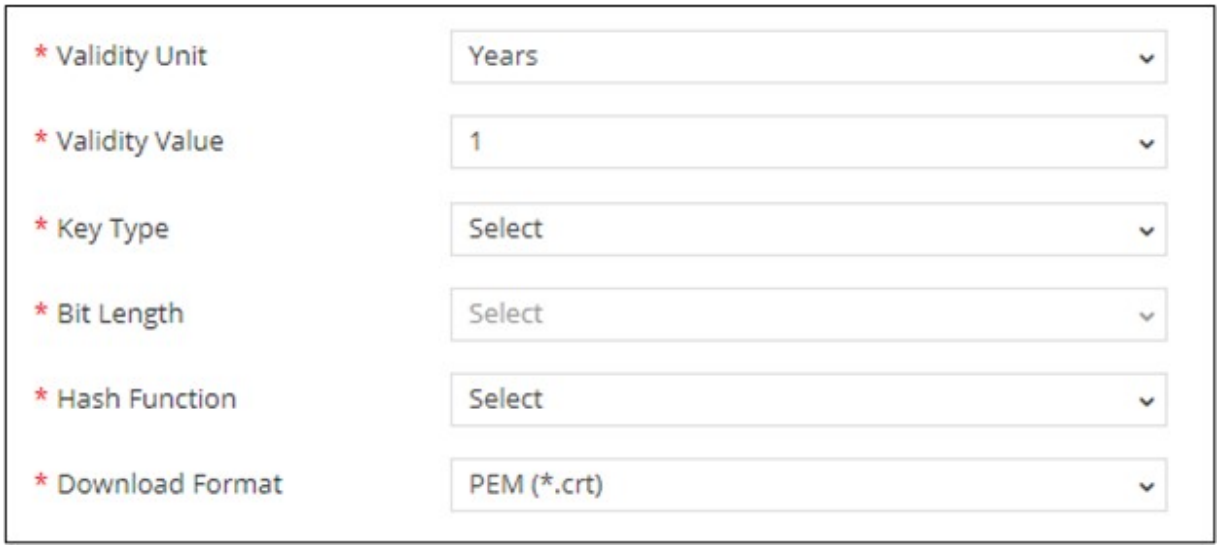
The following table describes the field information under the **CA Details** section:

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown.

Field	Description
	Note: This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Provide a Description for the workflow, if required.
All asterisk (*) marked fields are mandatory.	

7. Under the **CSR Parameters** section, enter or select the following field information:



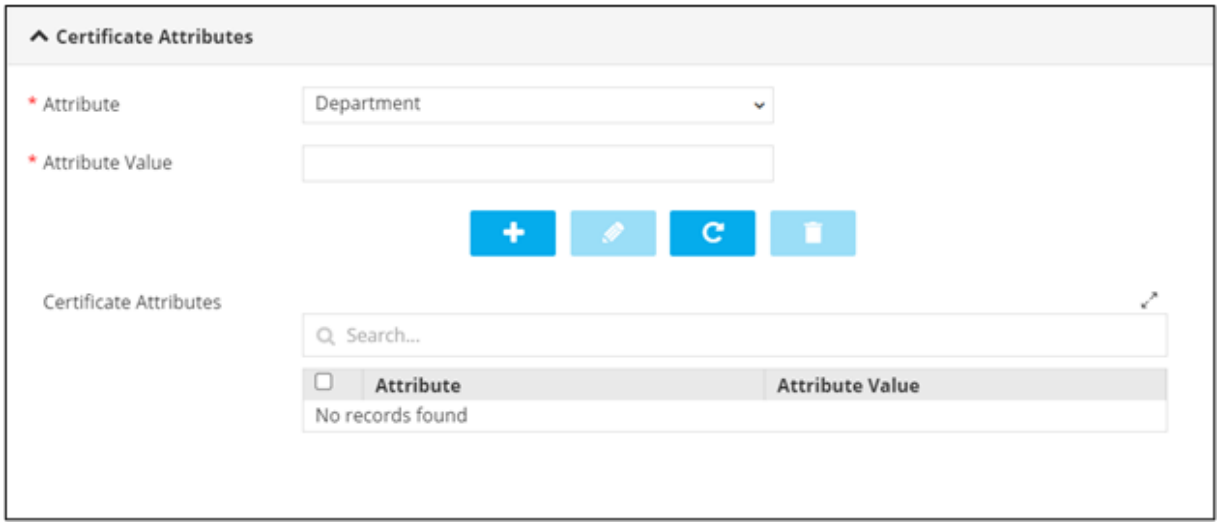


The following table describes the fields under the **CSR Parameters** section:

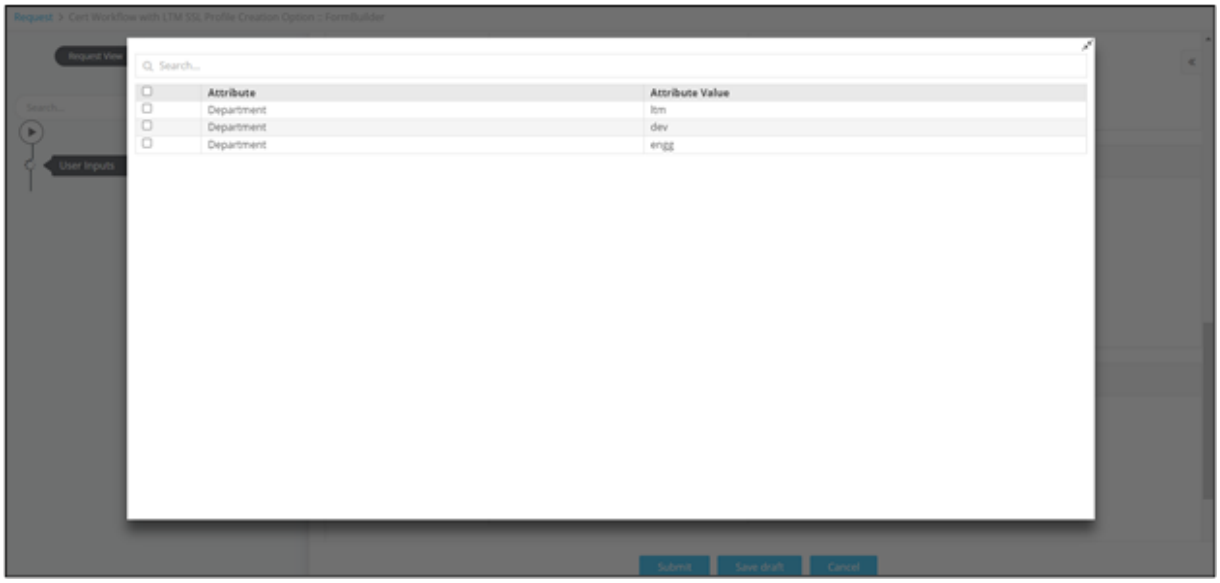
Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
***Organization**	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

Field	Description
	Note: This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

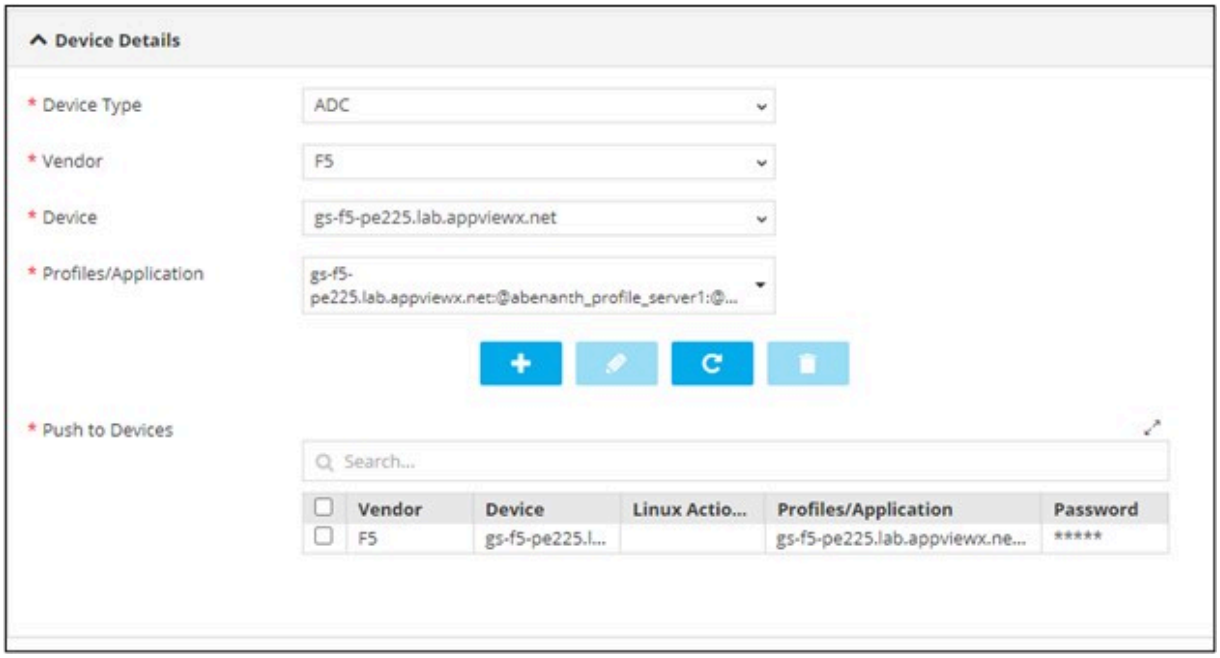
8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.



10. To add this attribute to the **Certificate Attributes** grid, click  .
11. To edit the value of a particular attribute, select the attribute in the grid and click  .
12. Enter the new value for the attribute in the **Value** field and click  again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click  .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Under the **Device Details** section, select the field information as shown.

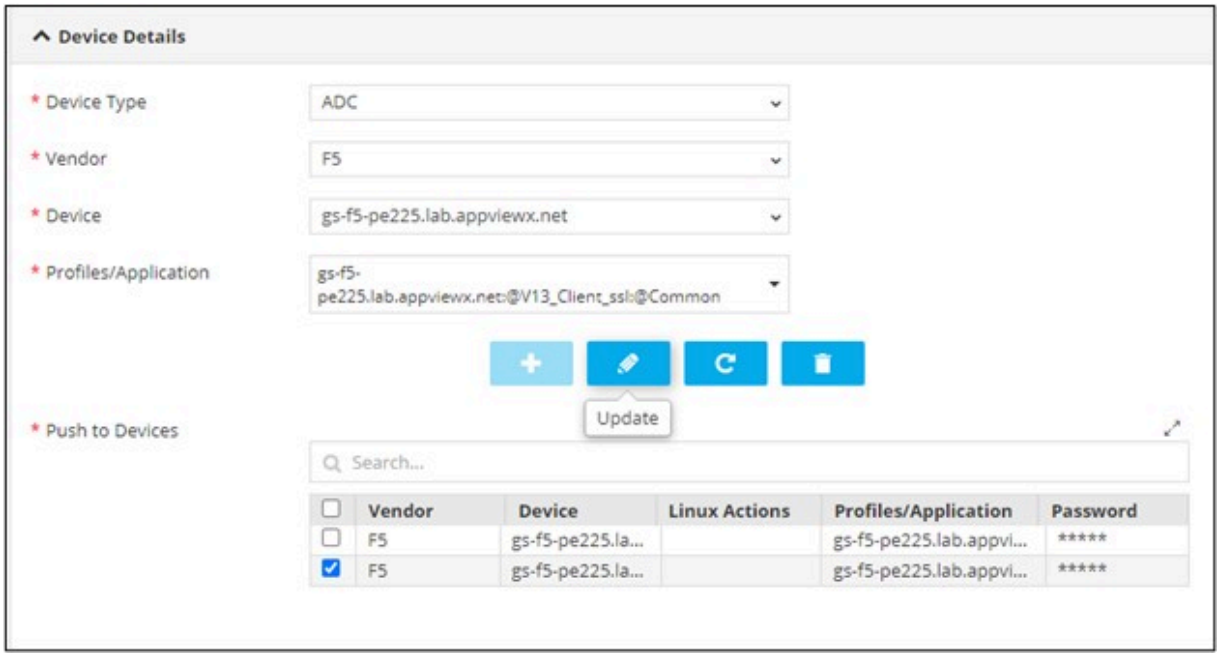


The following table describes the field information in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

17. To add the selected profile/application to the grid, click +.

The **Profile/Application** is added to the **Push to Devices** grid.

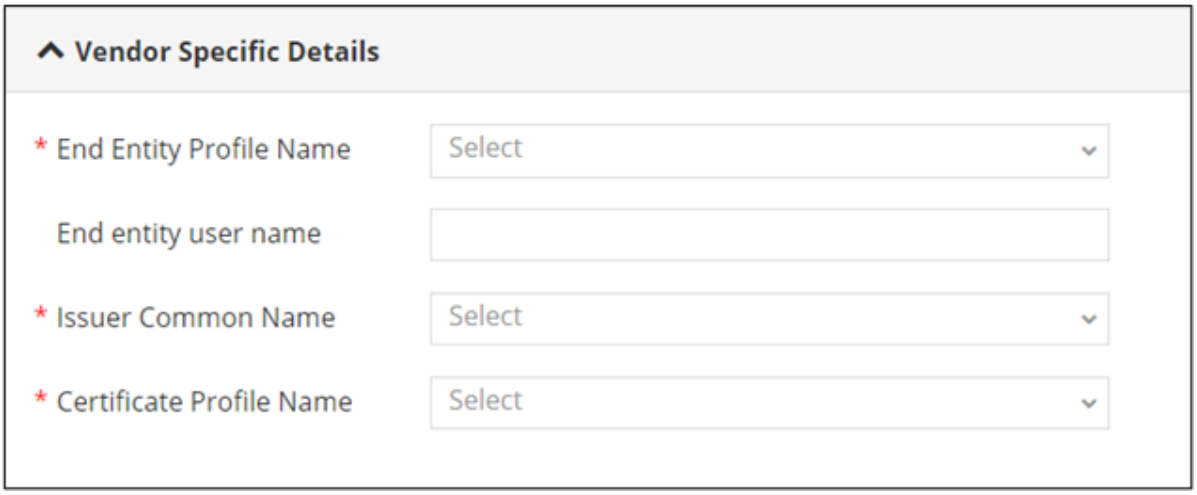


Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

18. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
19. Select a new device and click again to update the value.
20. To delete a profile/application, select the row to be deleted in the grid and click .
21. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
22. To search for a particular profile/application in the grid, type the keyword(s) in the search field.

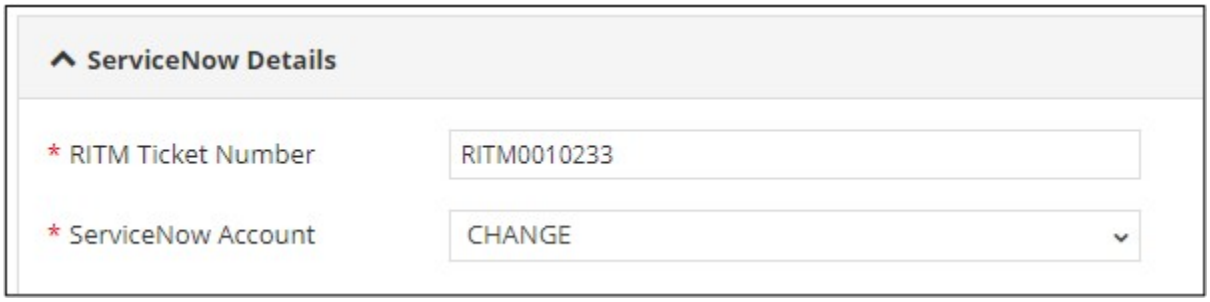
23. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.

    - When EJBCA is selected as CA.

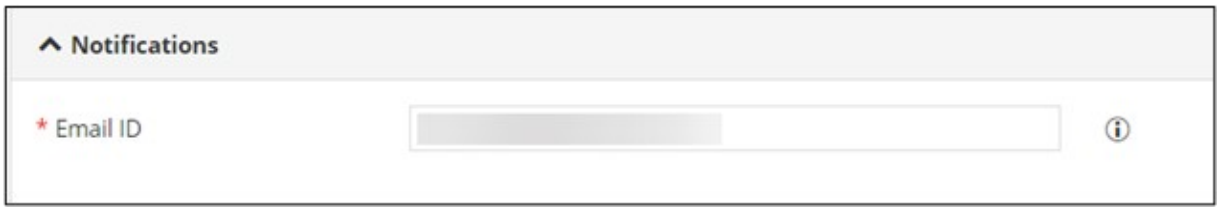


> **Note:** The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

24. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
25. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).



26. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.

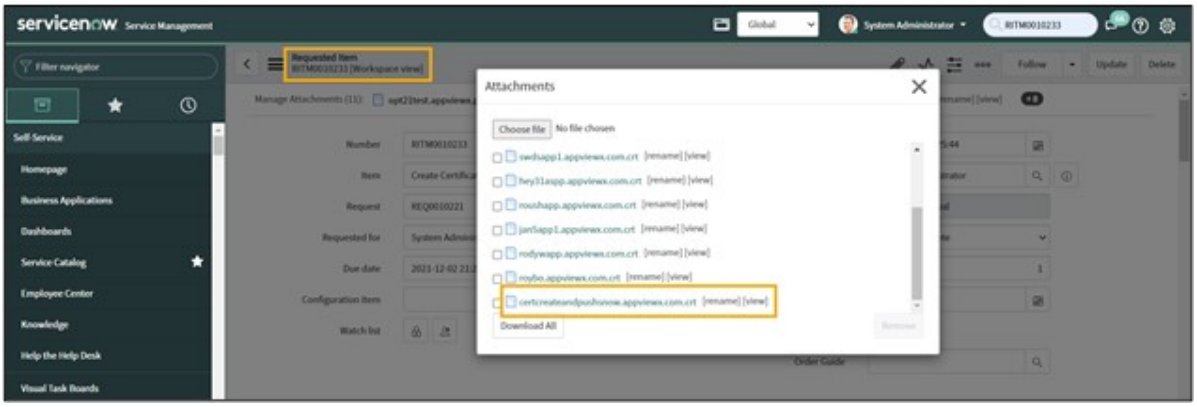


27. Click **Submit**.
    - AppViewX Certificate is created successfully.

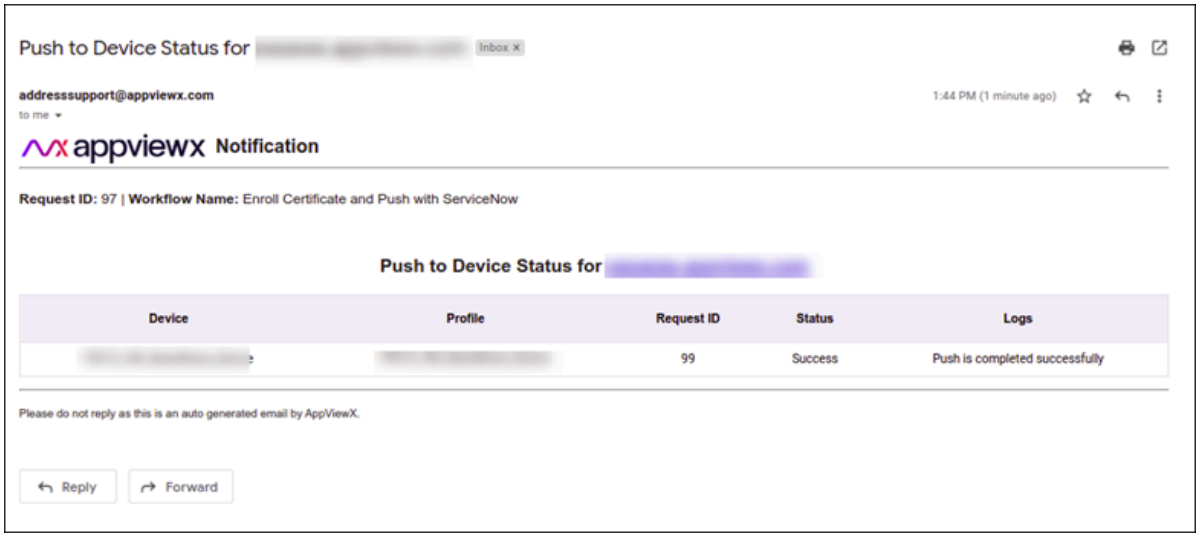
    - Certificate is pushed to the selected device.

- RITM ticket status updated.

- Certificate updated in the ServiceNow ticket.



- Email notification received.



28. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.

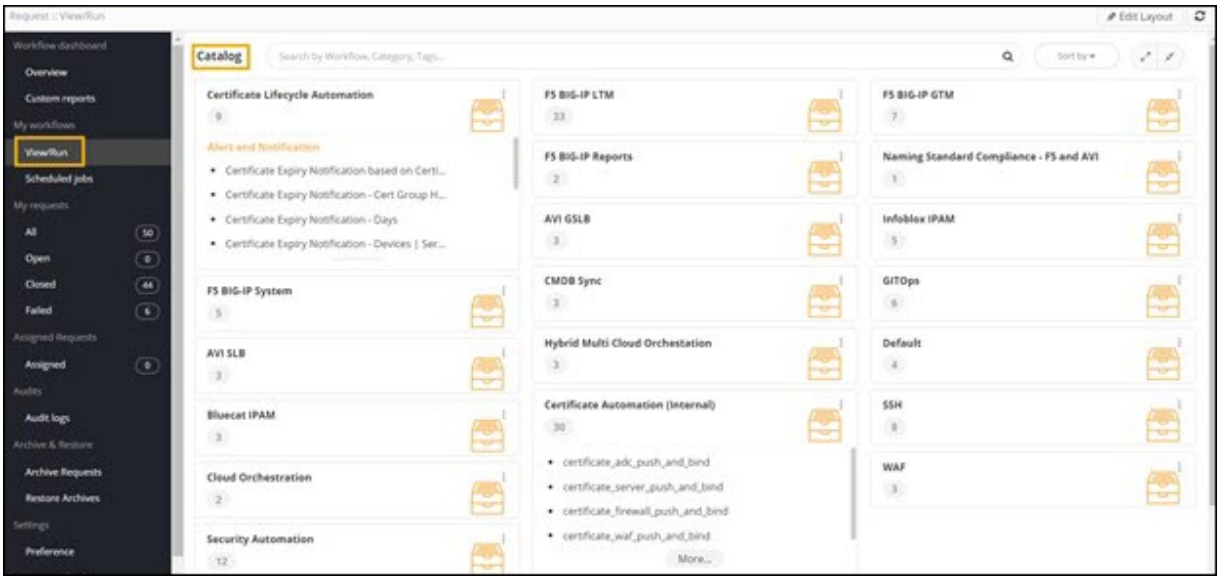
29. Hover your mouse over  to view the Certificate status.

Easy Certificate Provisioning

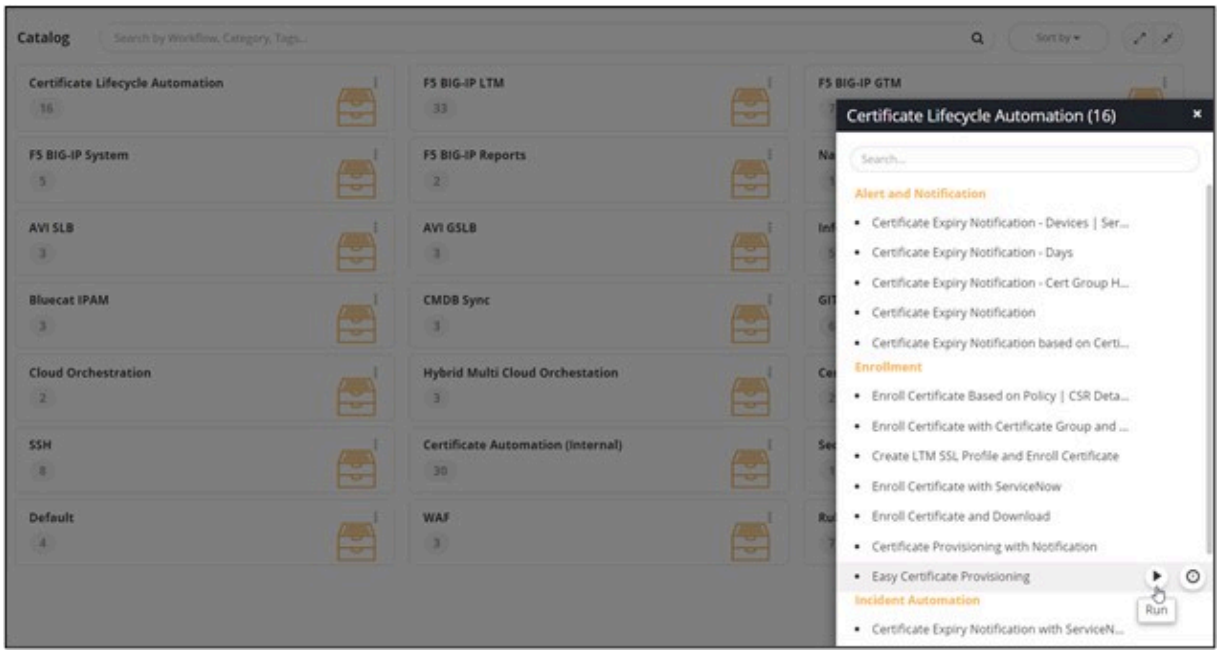
This workflow allows you to create an AppViewX certificate and push to a device available in the instance. Once the certificate is created, an email is sent to the logged in user informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. On the **Workflow Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

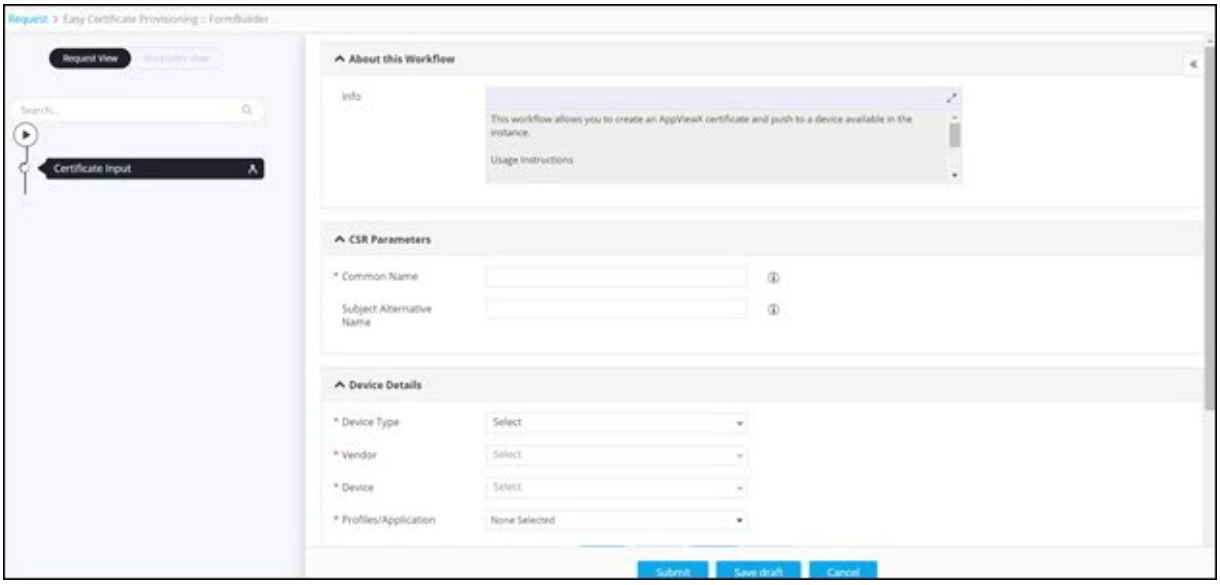


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Enrollment** category, hover your mouse over the **Easy Certificate Provisioning** workflow and click .



Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.

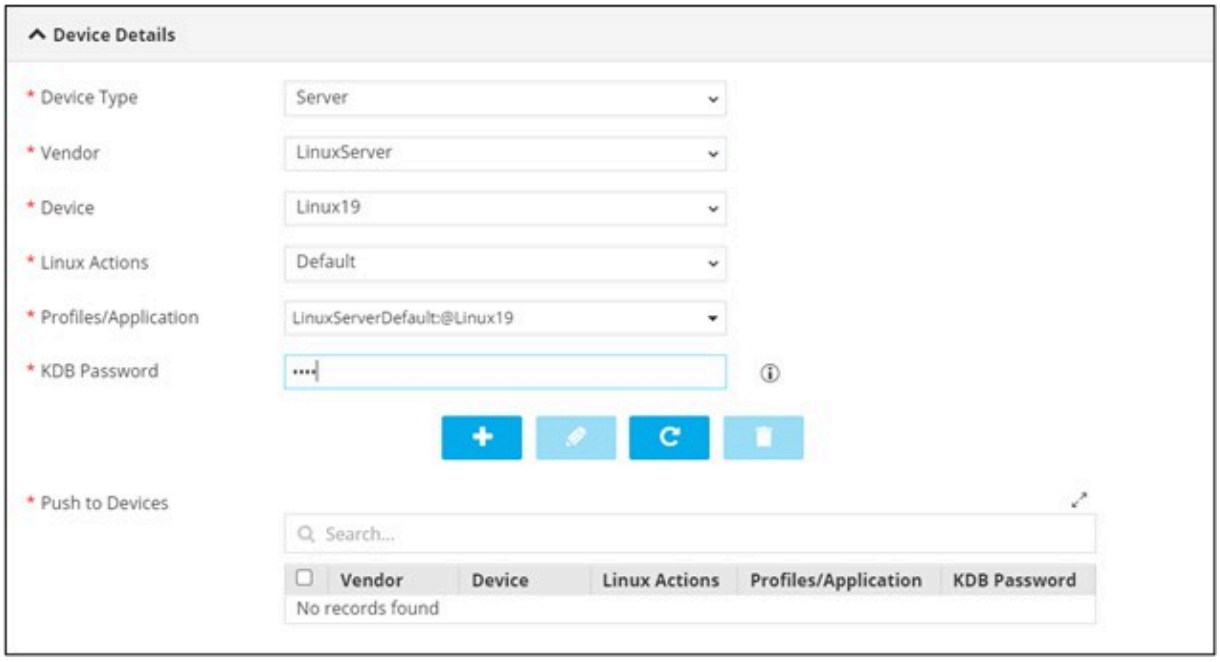


5. Under the **CSR Parameters** section, enter the **Common Name**.

Note: This is a mandatory field.

6. Under the **CSR Parameters** section, enter the **Subject Alternative Name**.

7. Under the **Device Details** section, select the field information as shown.

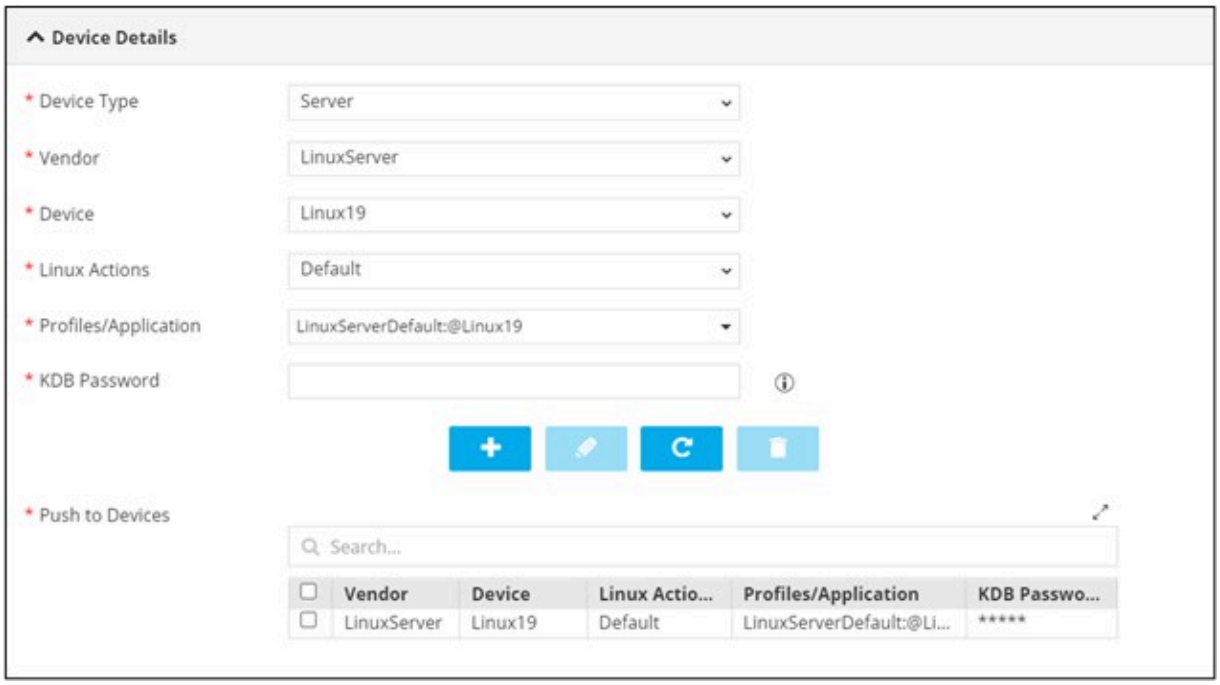


The following table describes the fields in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown.

Field	Description
	Note: The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

8. To add the selected profile/application to the Push to Devices grid, click +.
   The profile/application is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the Push to Devices grid, under the **Profiles/Applications** column as comma-separated values.

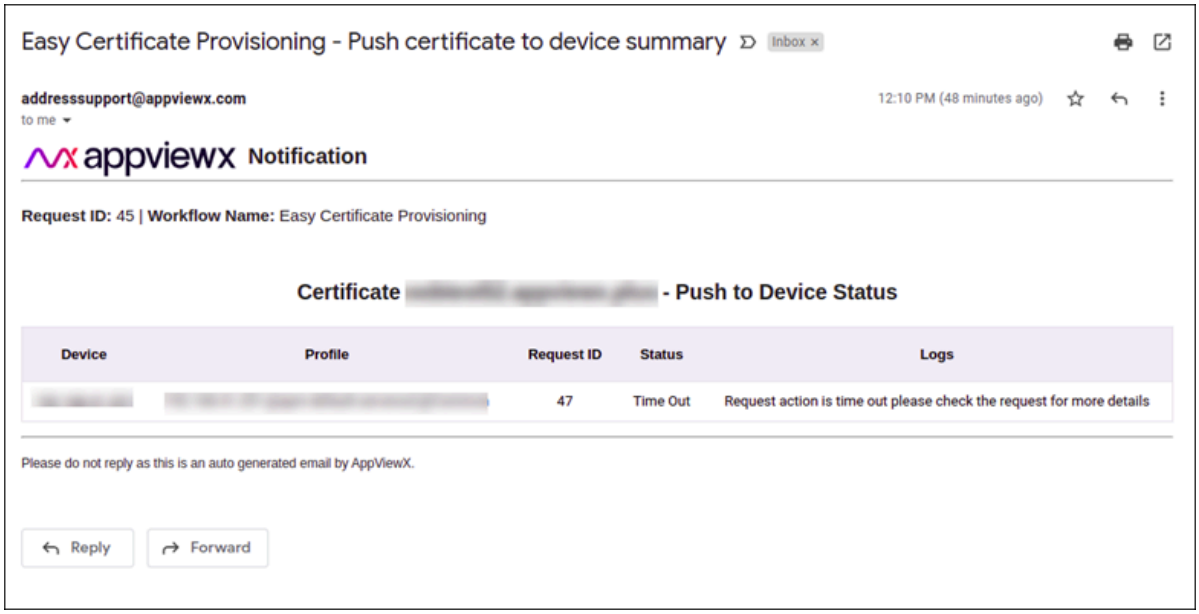
9. To modify the details of the device to which the certificate is to be pushed, select the device in the grid and click  .
10. Select a new device and click  again to update the value.
11. To delete a profile/application, select the row to be deleted in the grid and click  .
12. To maximize the Push to Devices grid, from the top right corner of the grid, click  .
13. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
14. Click **Submit**.
    - The workflow is executed and an AppViewX certificate is created.

    - Certificate pushed to selected Linux Server.

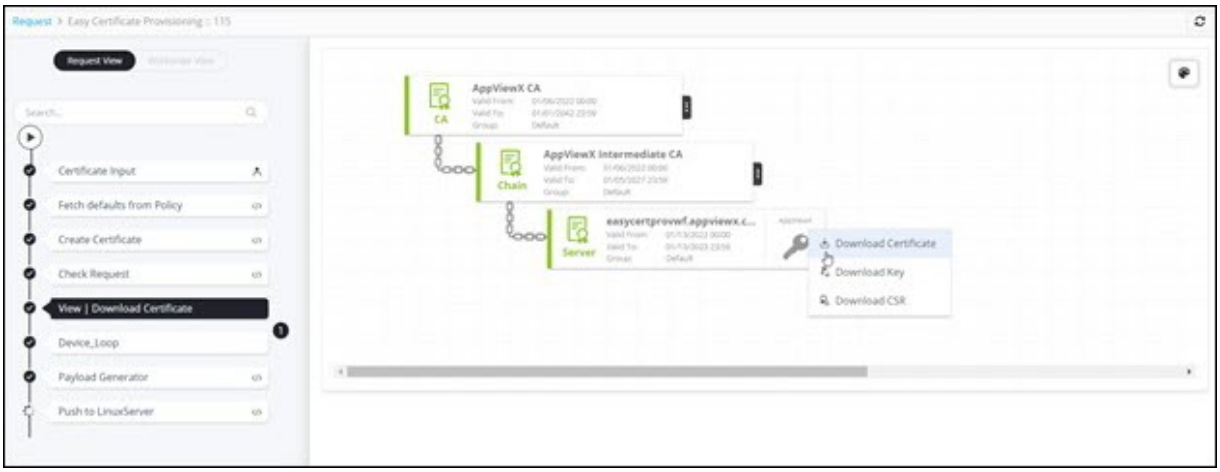
    - Push to Device Status **Summary** displayed.

Note: To download the Push to Device Status Summary, from the top right corner of the screen, click  .

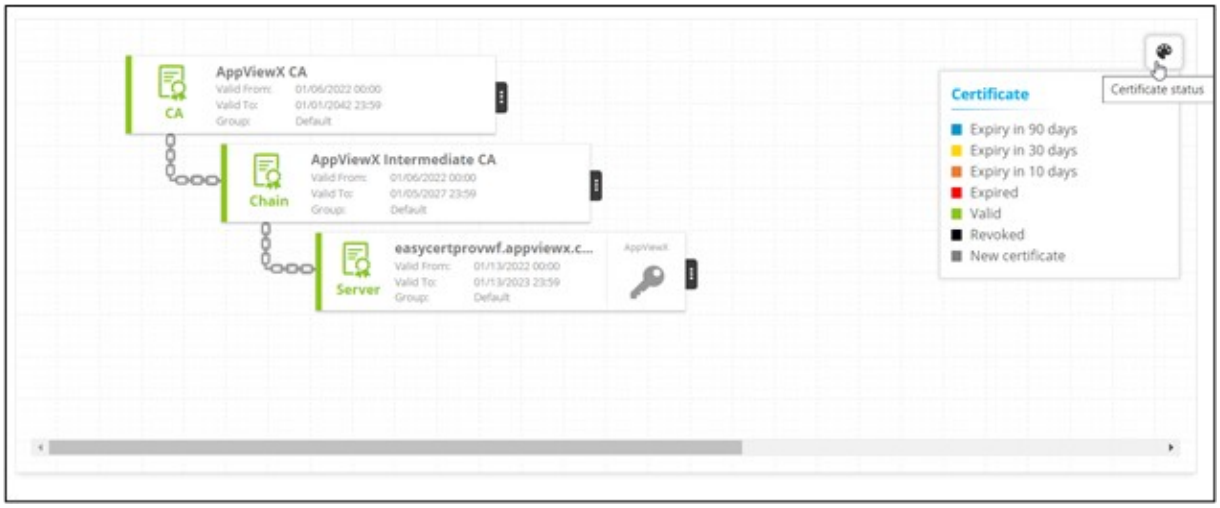
• Email notification received.



15. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  , and from the options displayed, click **Download Certificate**.



16. Hover your mouse over to view the Certificate status.

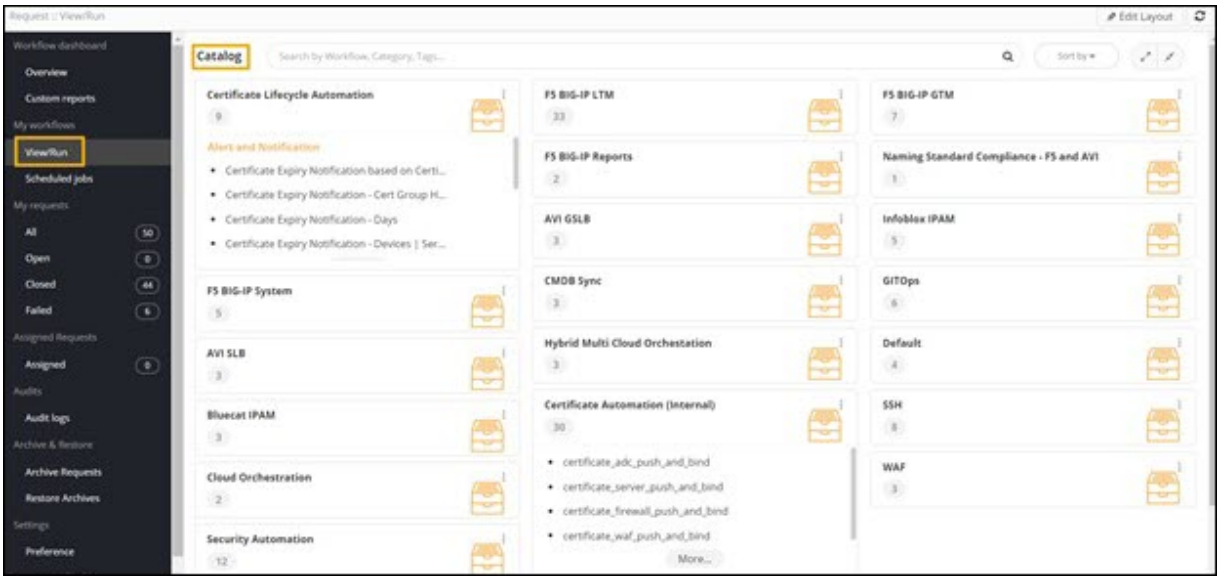


Enroll Certificate with CAA Validation

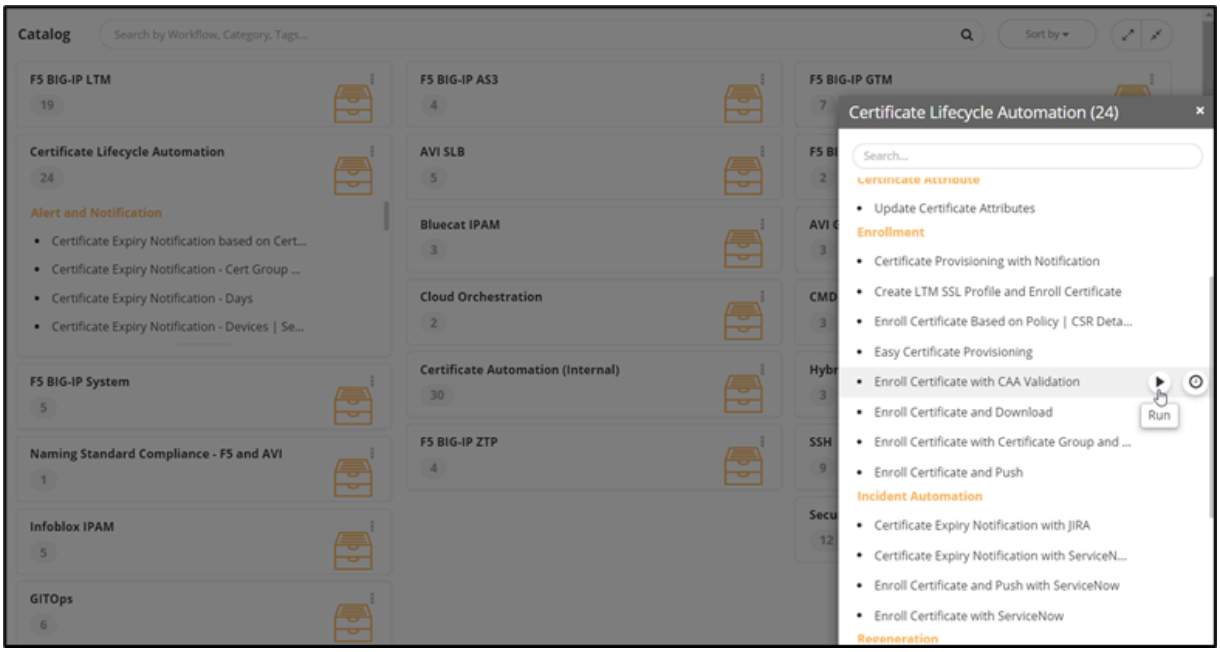
This workflow allows you to create a certificate by validating the Certificate Authority that can issue the certificate based on the given domain name.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .

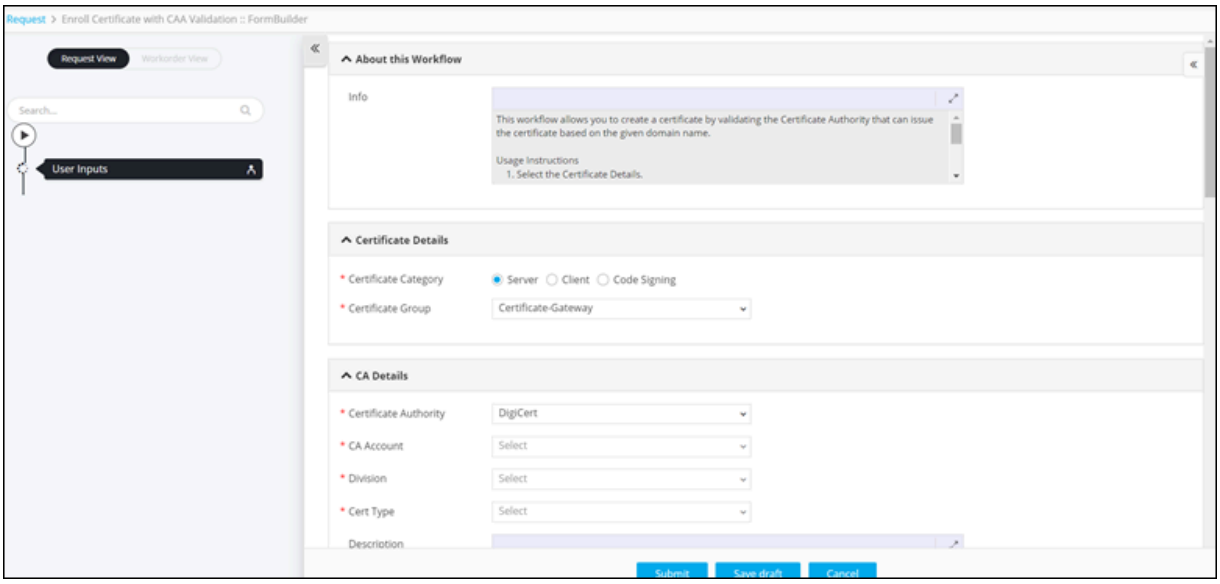


3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with CAA Validation** workflow and click ▶.

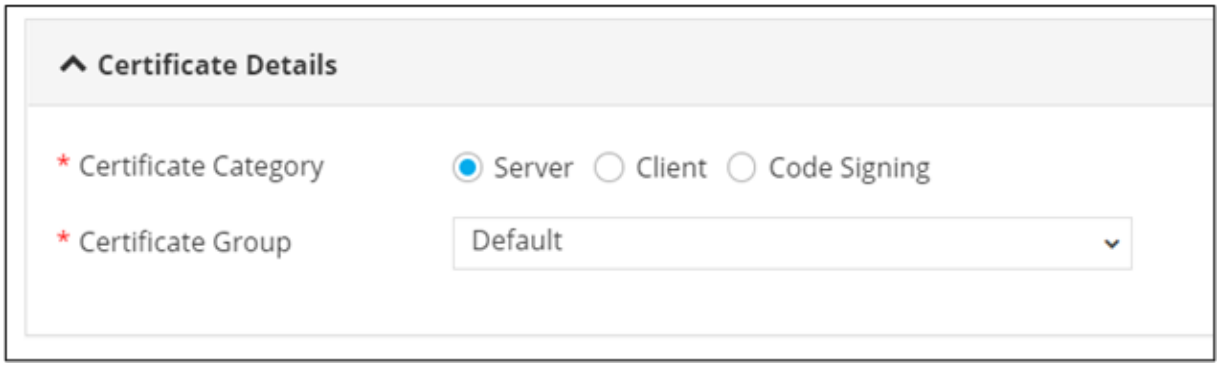


> **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **Certificate Details** section, select the field information as shown.

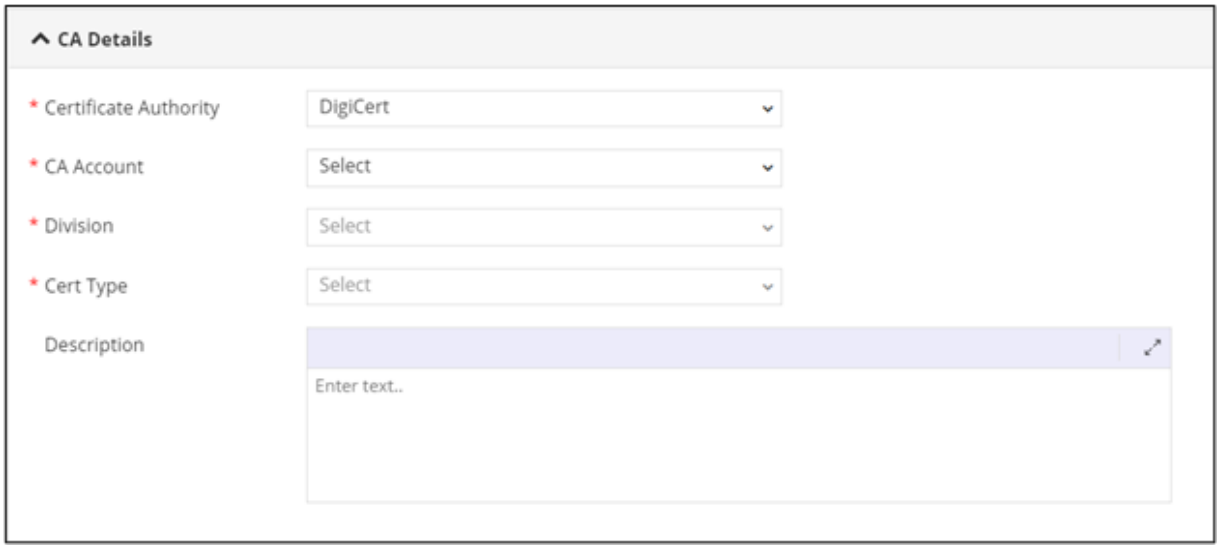


The following table describes the field information under the **Certificate Details** section:

Field	Description
***Certificate Category**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.

Field	Description
All asterisk (*) marked fields are mandatory.	

6. Under the **CA Details** section, enter or select the field information as shown.

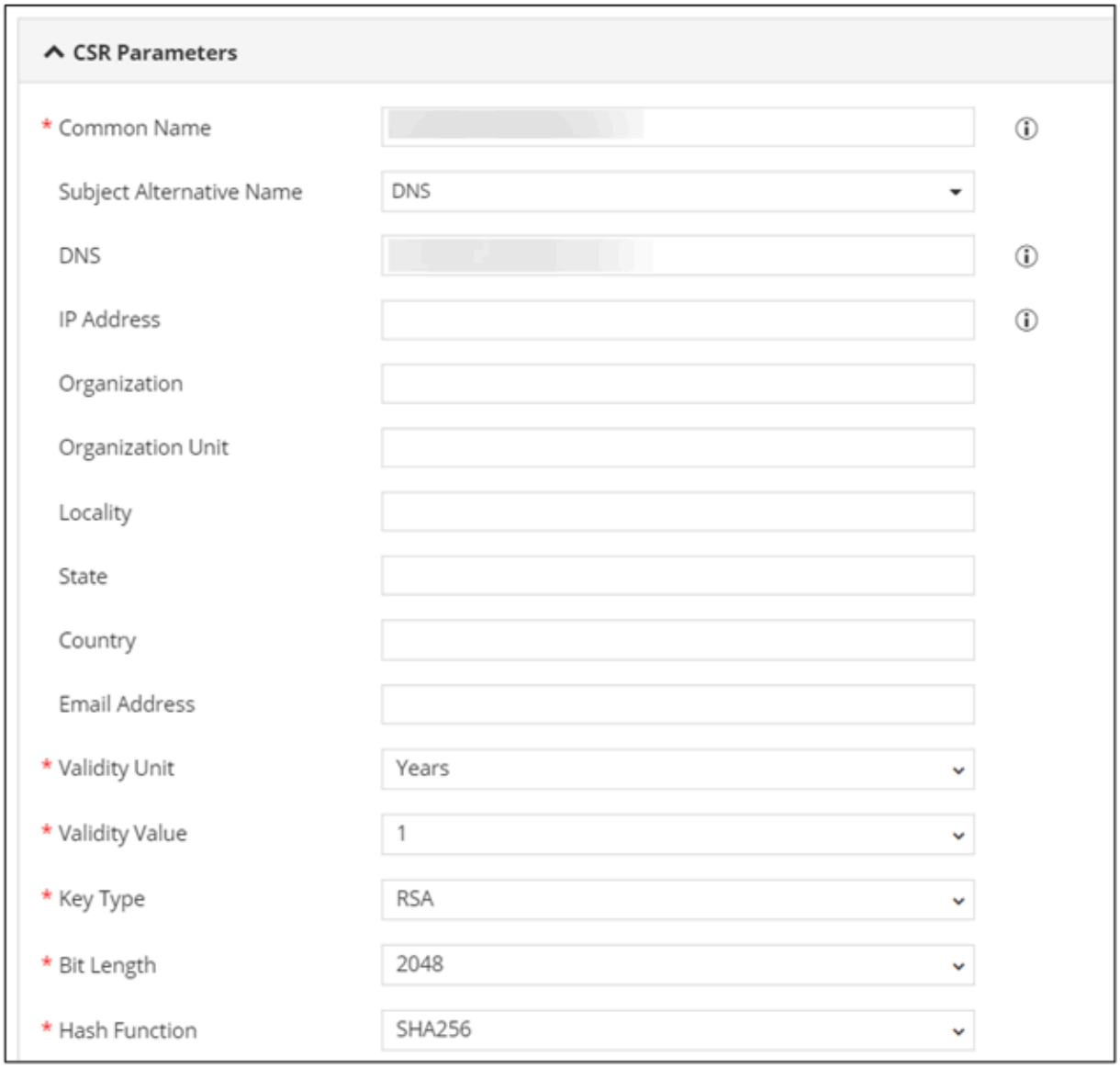


The following table describes the field information under the **CA Details** section:

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown.

Field	Description
	Note: This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Provide a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

7. Under the **CSR Parameters** section, enter or select the field information as shown.

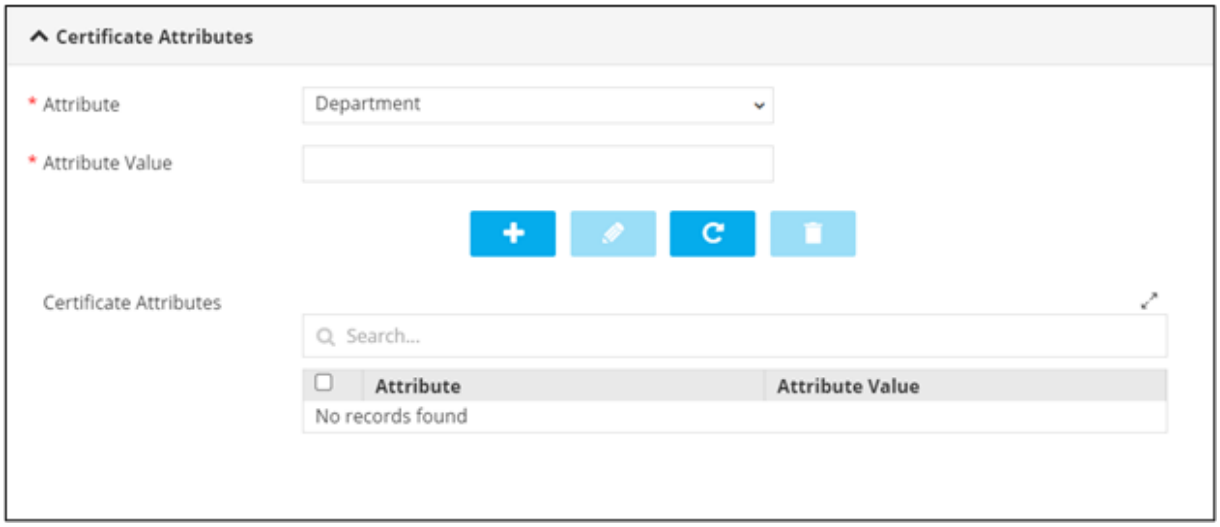


The following table describes the fields under the **CSR Parameters** section:

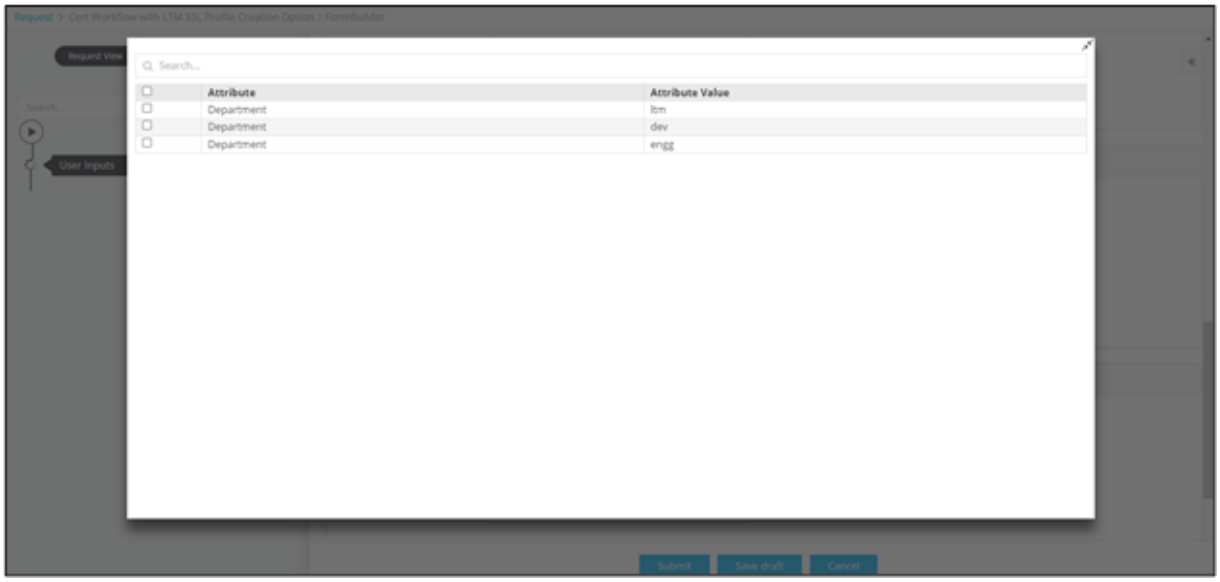
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.

Field	Description
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.



10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



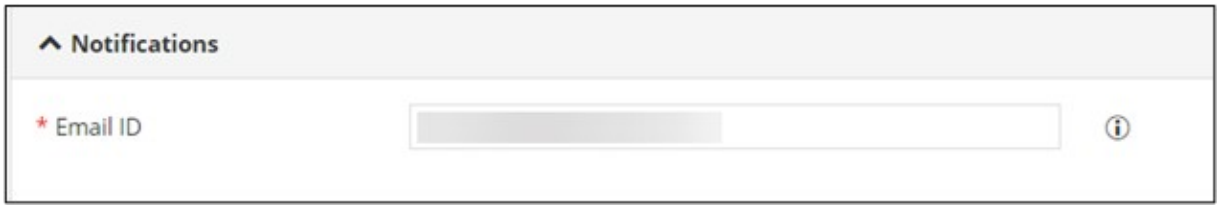
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

• When Digicert is selected as CA.

• When EJBCA is selected as CA.

Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

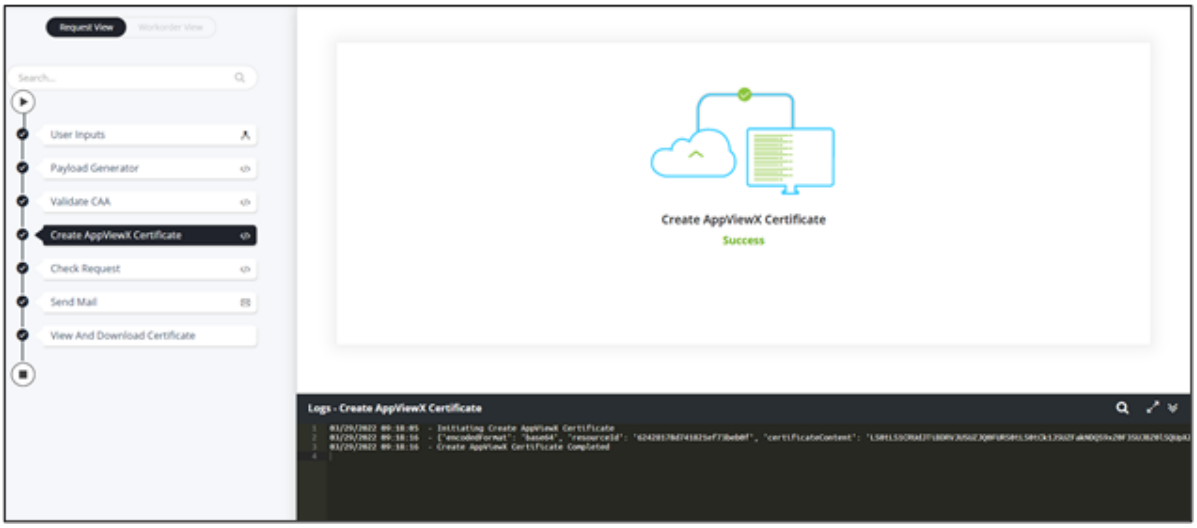
17. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



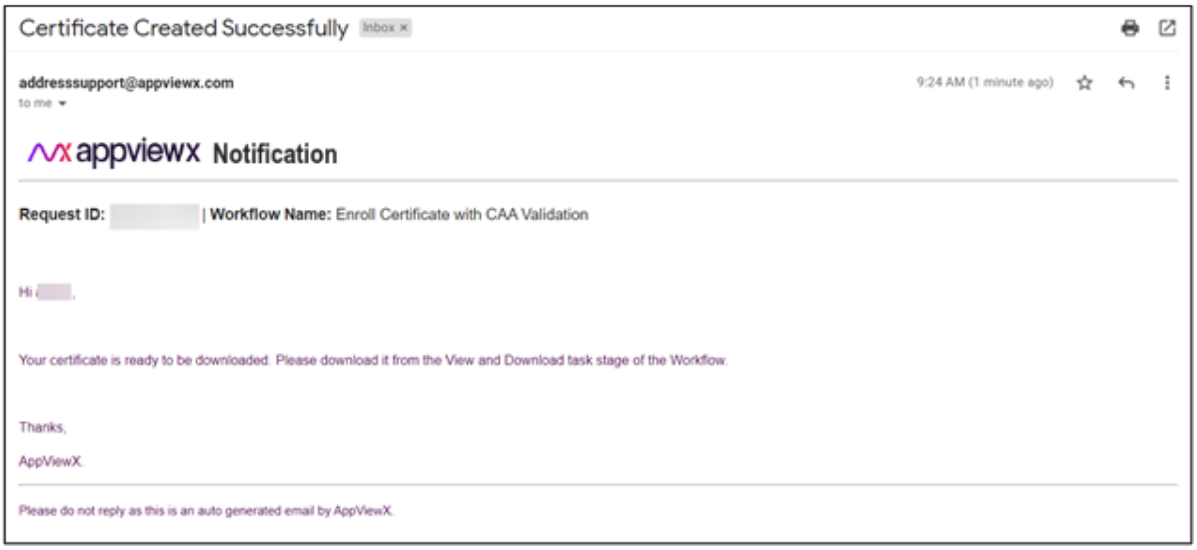
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

18. Click **Submit**.
    - CAA Validation successful.

    - Certificate created successfully.



    - Email notification received.



19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

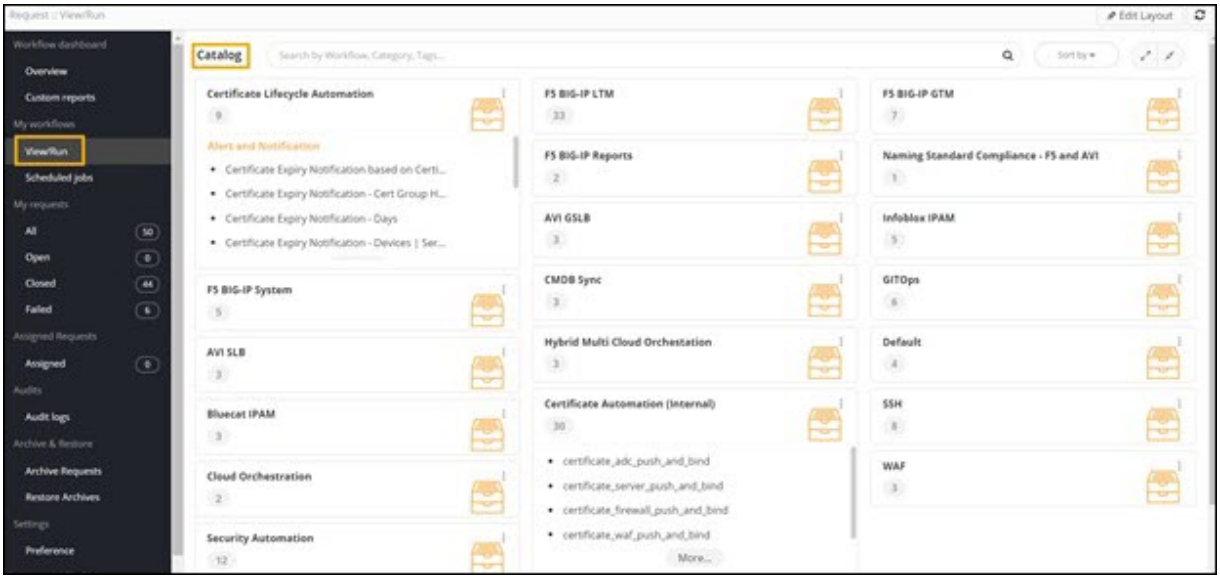
20. Hover your mouse over  to view the **Certificate status**.

Enroll Certificate and Push

This workflow allows you to create a certificate and push it to the selected device.

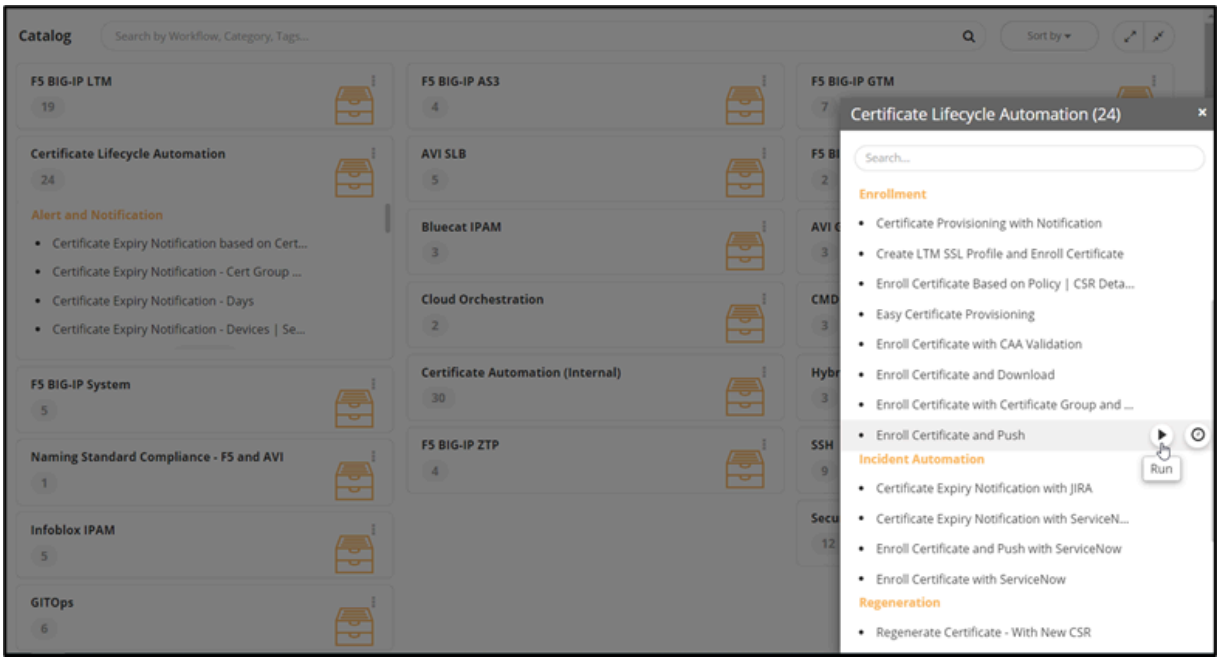
To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.



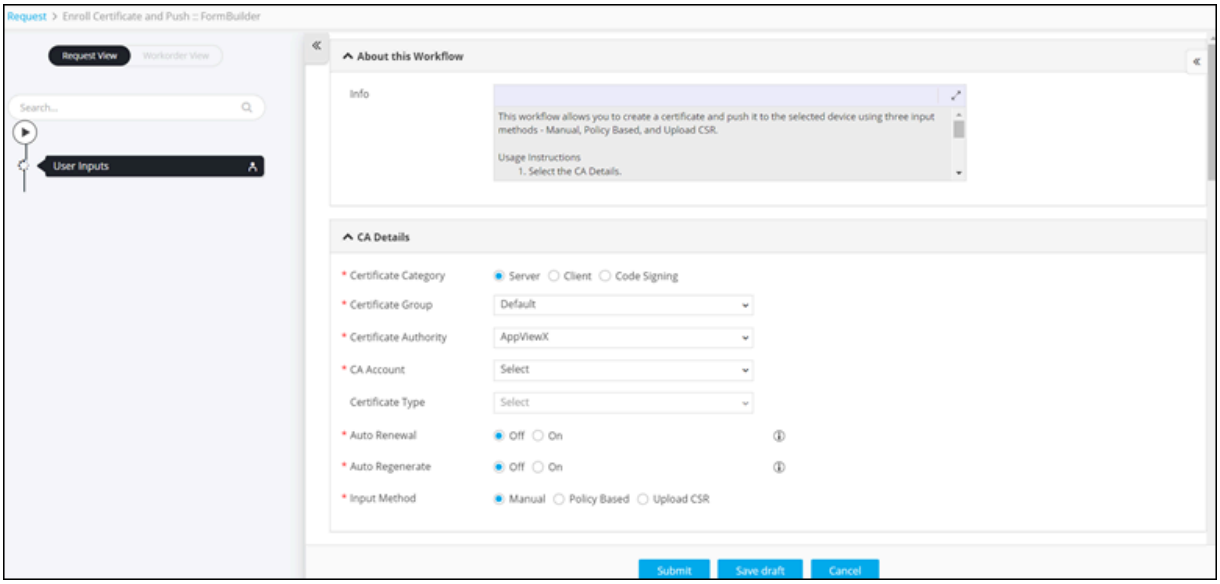
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click ⋮ .
3. From the options displayed, select **Full View**.

4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push** workflow and click  .

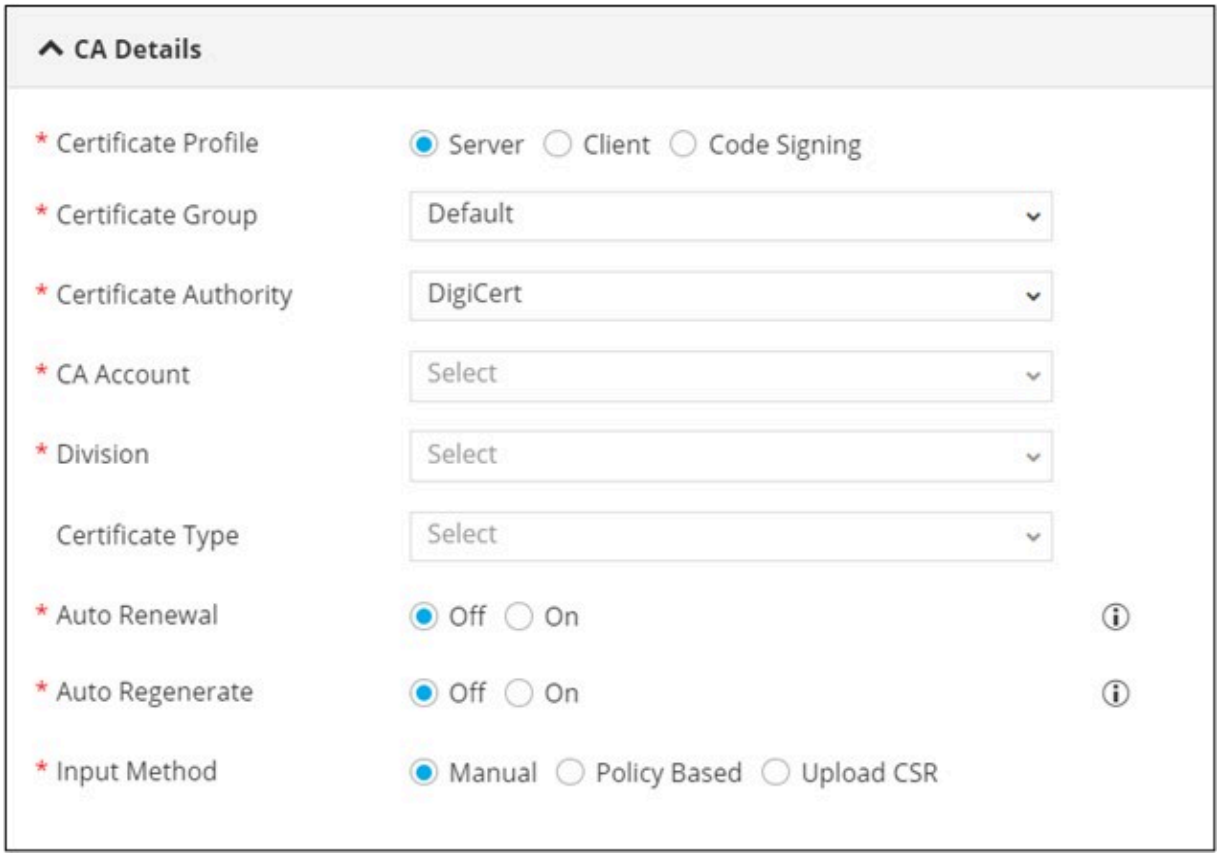


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **CA Details** section, select the following field information:



The following table describes the fields in the **CA Details** section:

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA

Field	Description
	• Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field. **Note:** This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are:

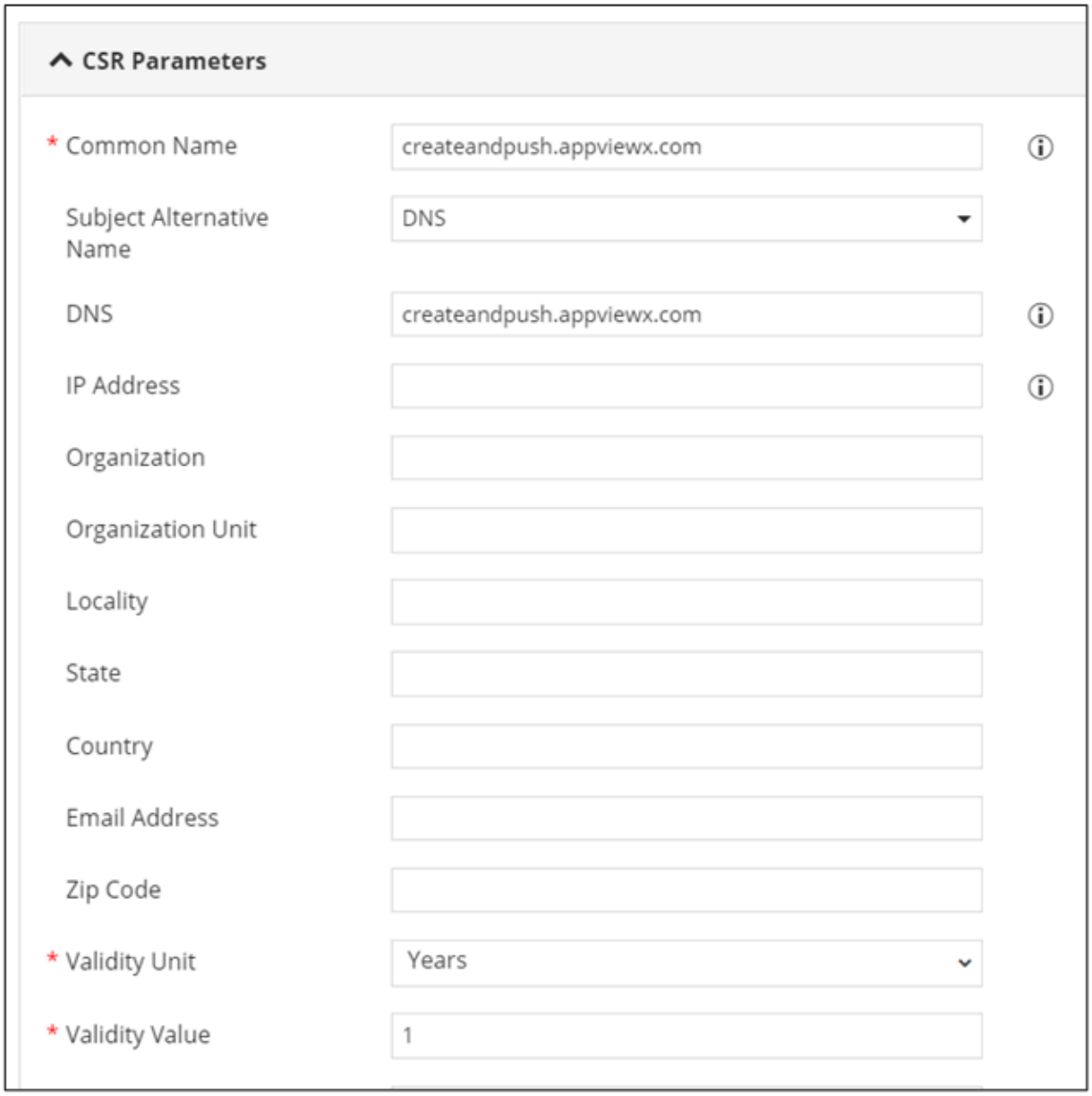
Field	Description
	• **Manual:** If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. • **Policy Based:** If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**. • **Upload CSR:** If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters.  **Note: Manual** is the default selection.
All Asterisk (*) marked fields are mandatory.	

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Policy Based**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under **CSR Parameters**, enter the field information as shown.

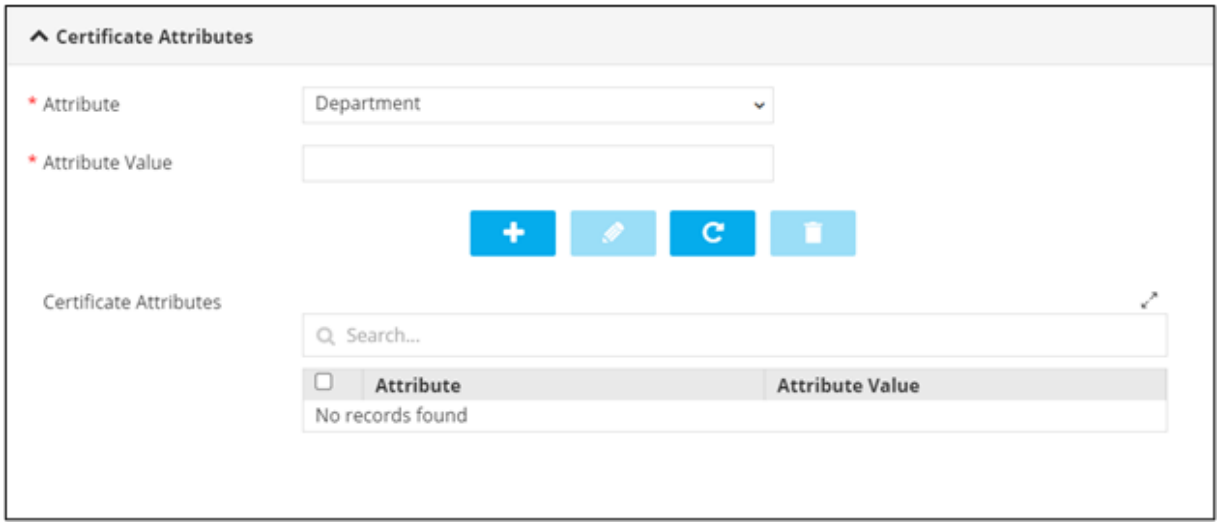


The following table describes the field information in the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.

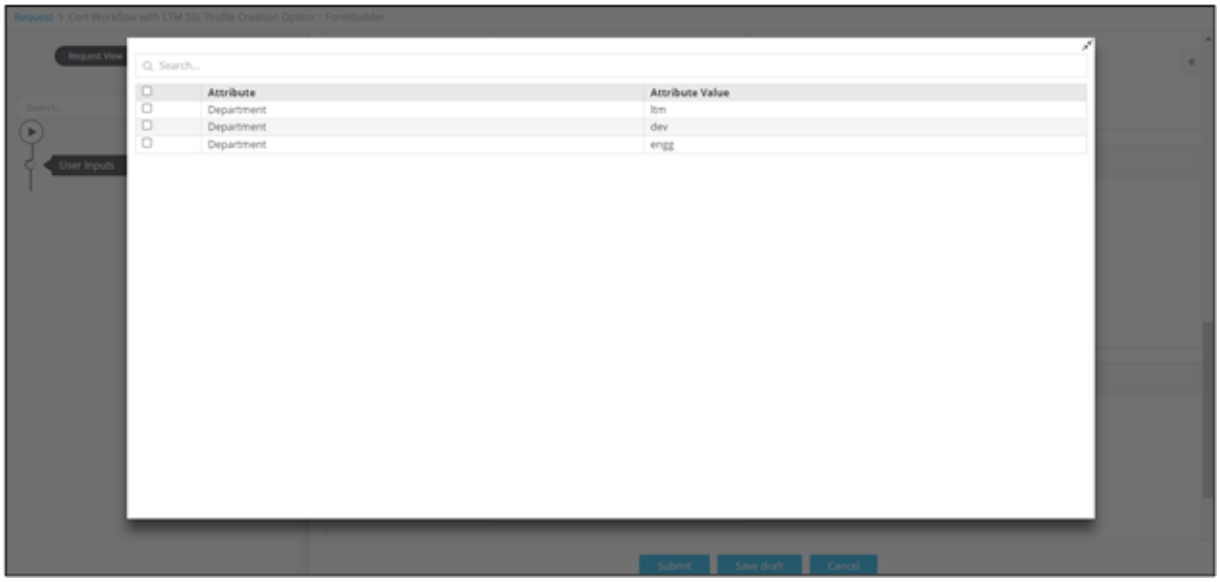
Field	Description
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select 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. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

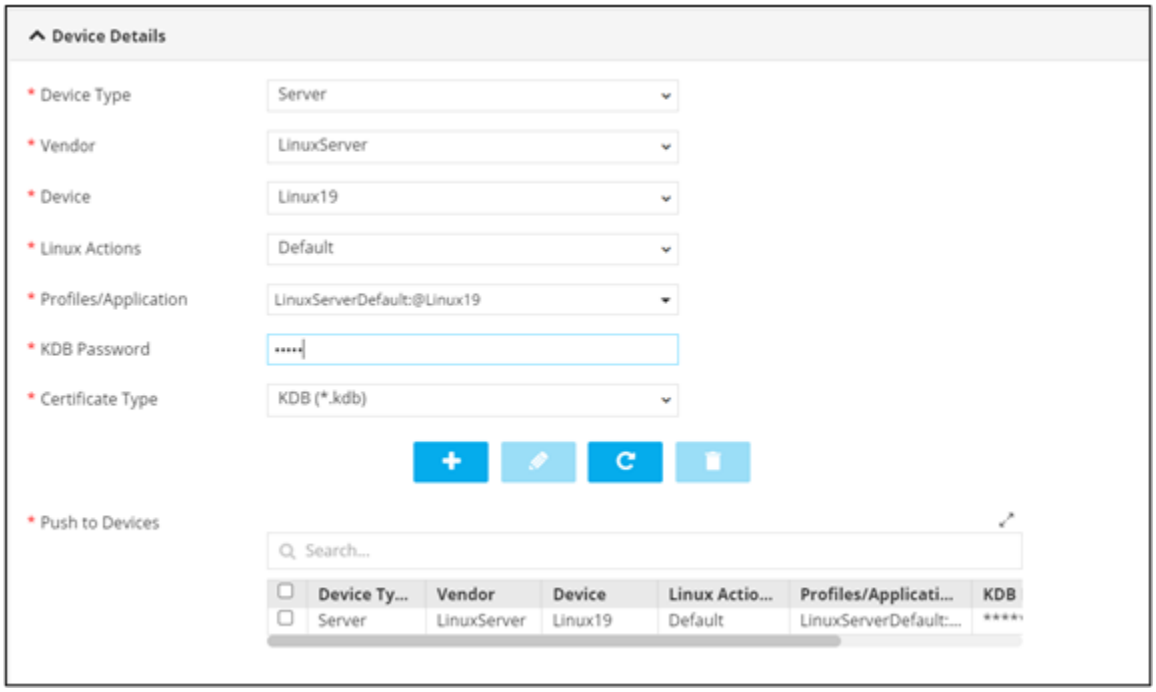


4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .
6. Enter the new value for the attribute in the **Value** field and click again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click .

8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



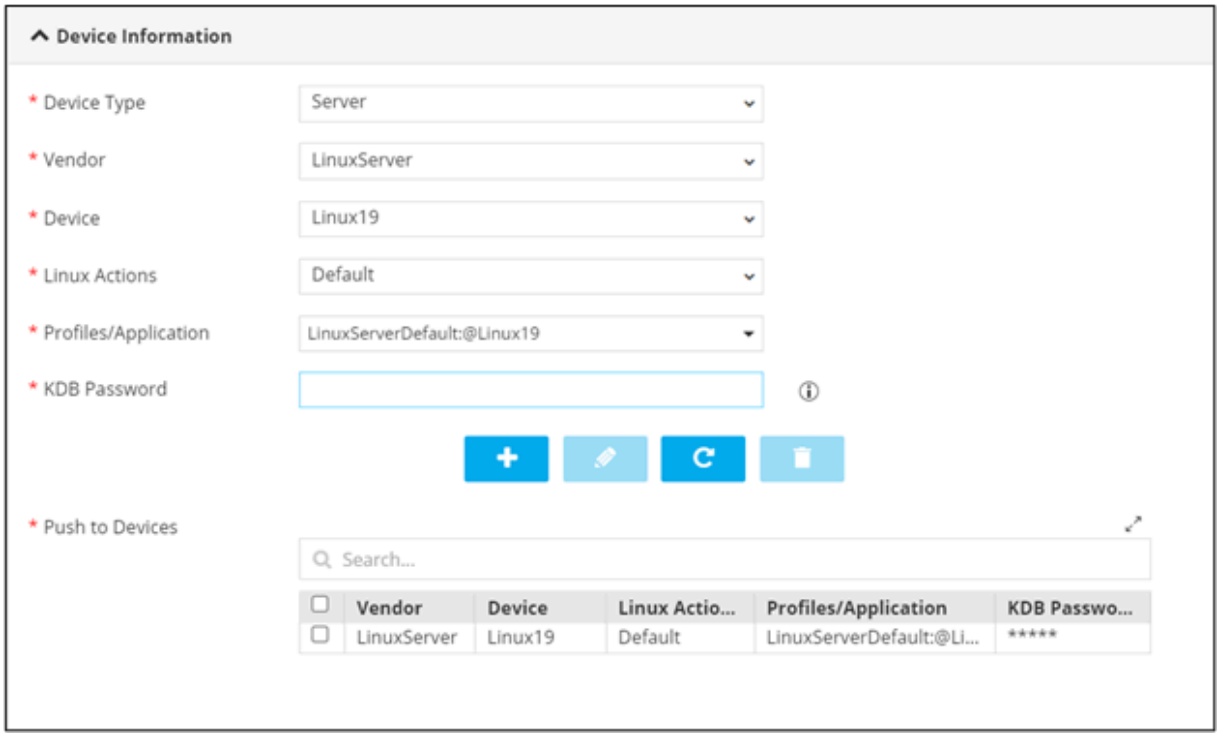
9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Device Details** section, select the field information as shown.



The following table describes the field information in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

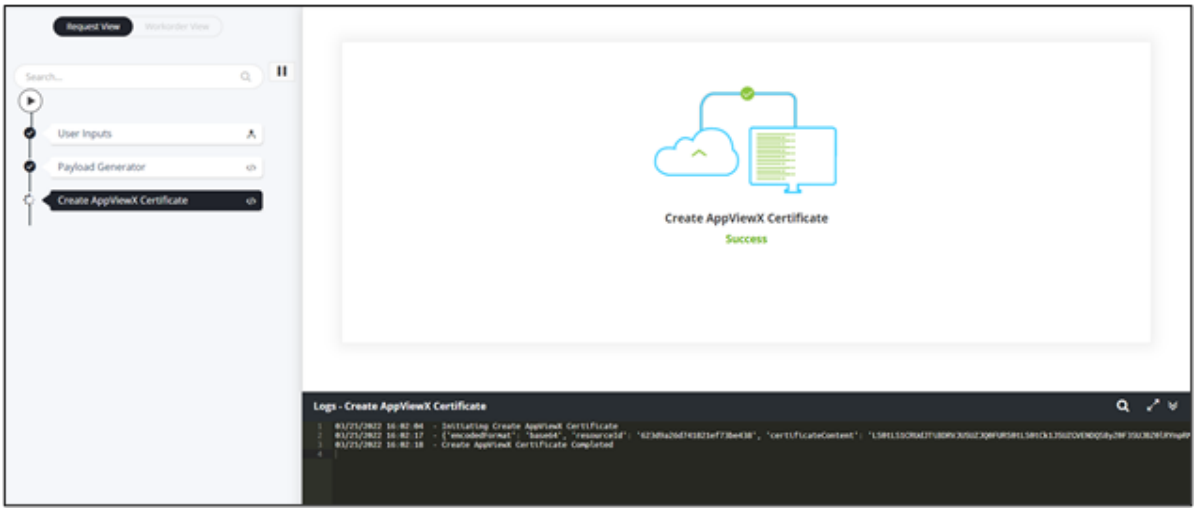
11. To add the selected profile/application to the grid, click  .
    The **Profile/Application** is added to the **Push to Devices** grid.



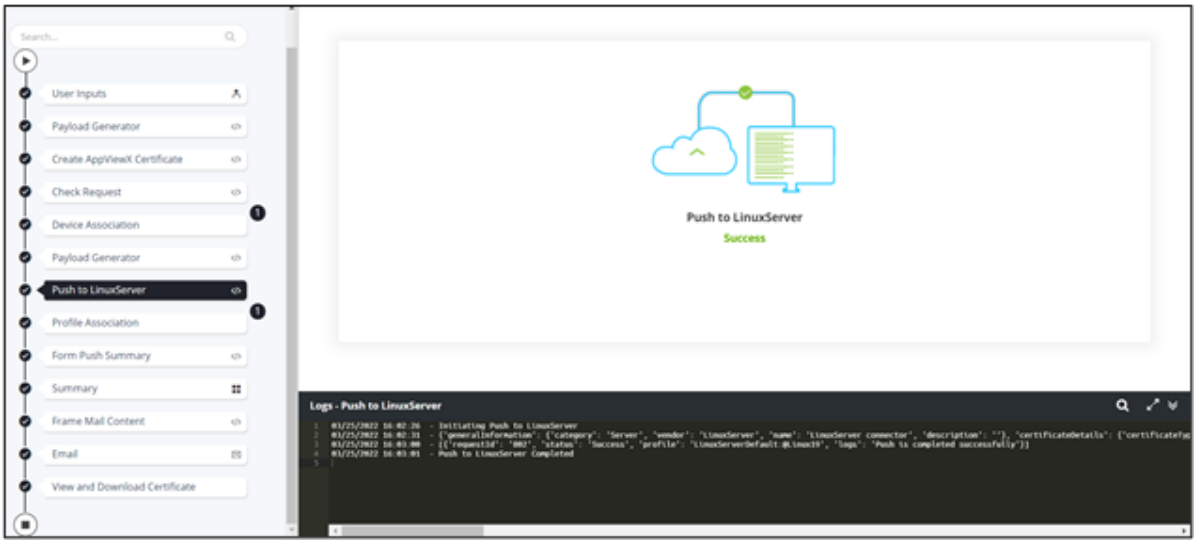
Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

12. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
13. Select a new device and click again to update the value.
14. To delete a profile/application, select the row to be deleted in the grid and click .
15. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
16. To search for a particular profile/application in the grid, type the keyword(s) in the search field.

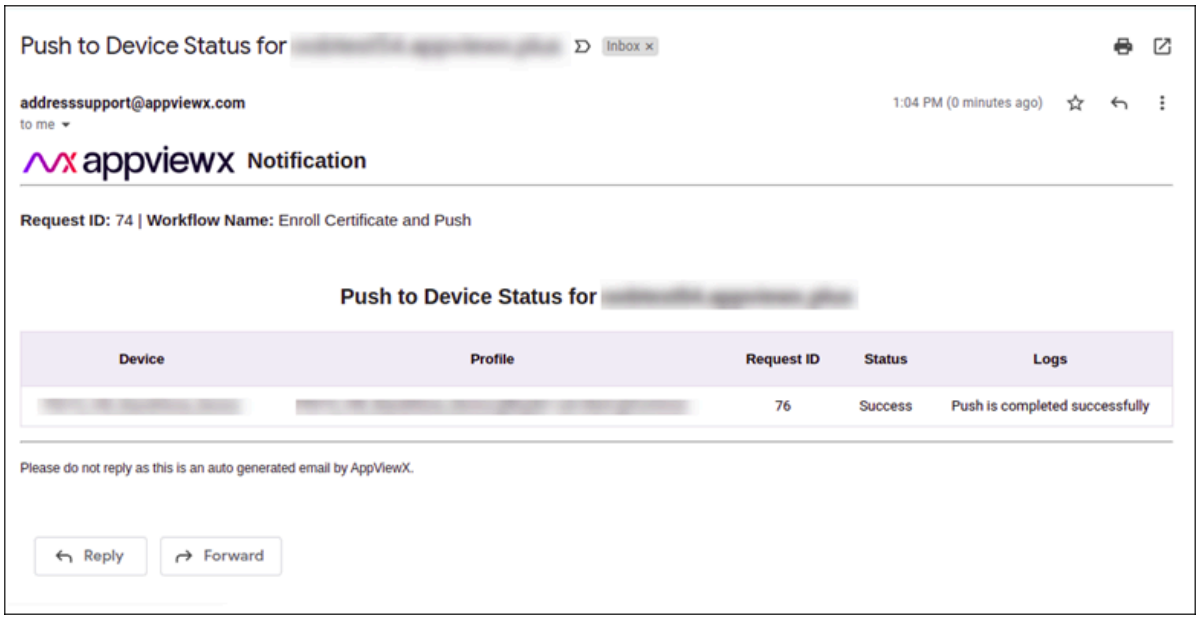
17. Click **Submit**.
    - Certificate created successfully.



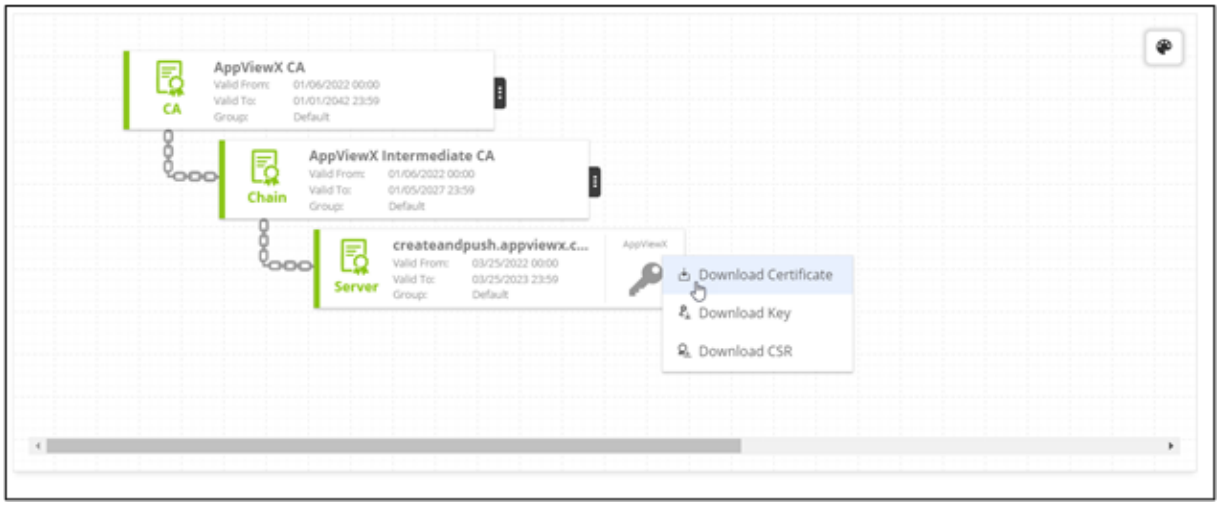
    - Certificate pushed to Linux server successfully.



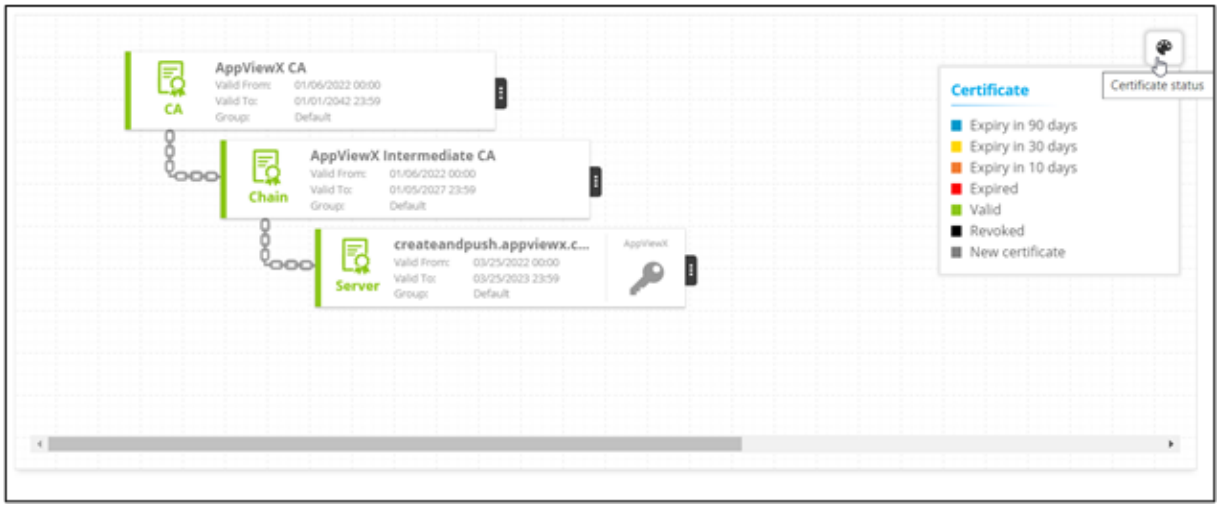
    - Email notification received.



18. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



19. Hover your mouse over  to view the **Certificate status**.

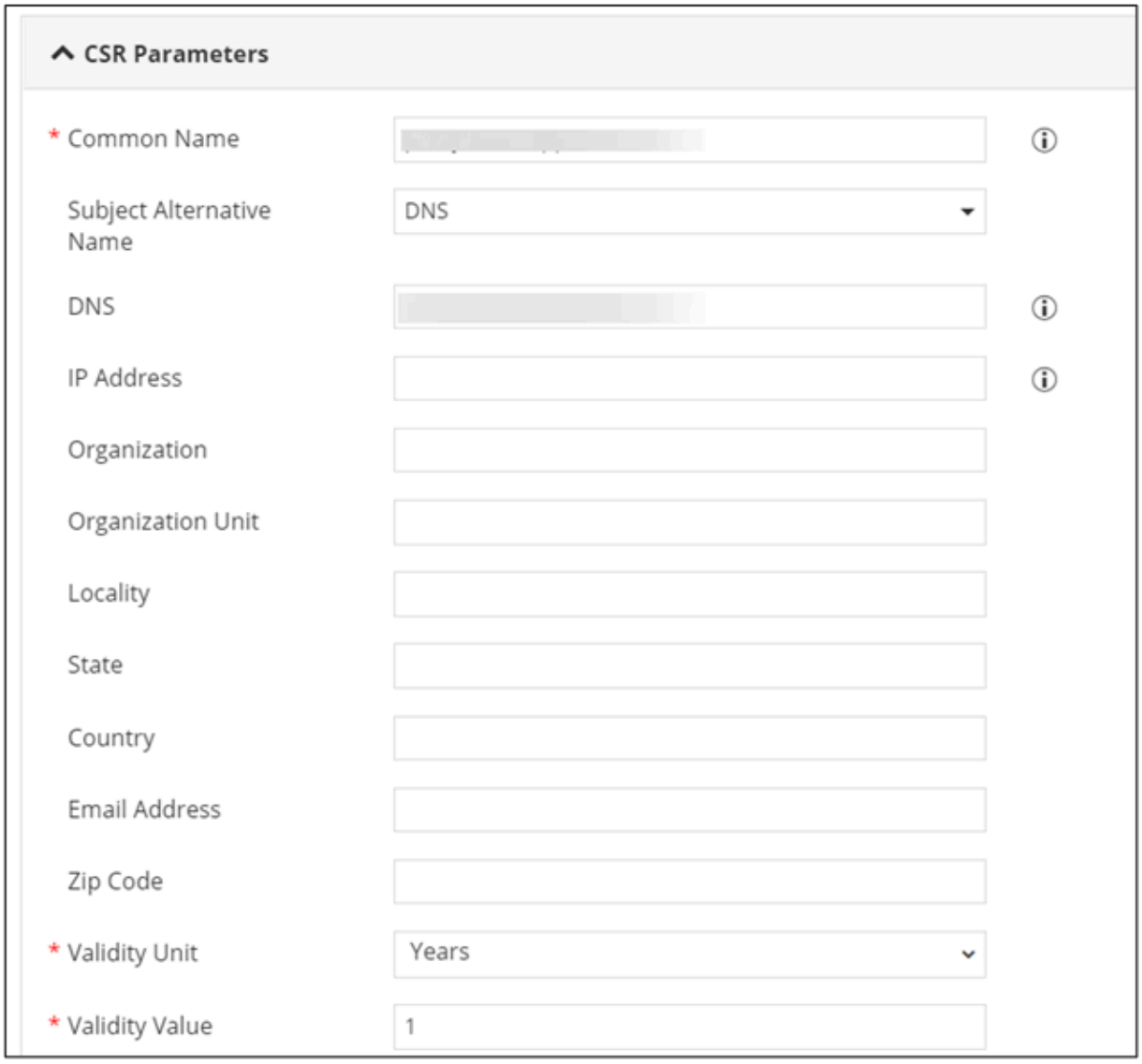


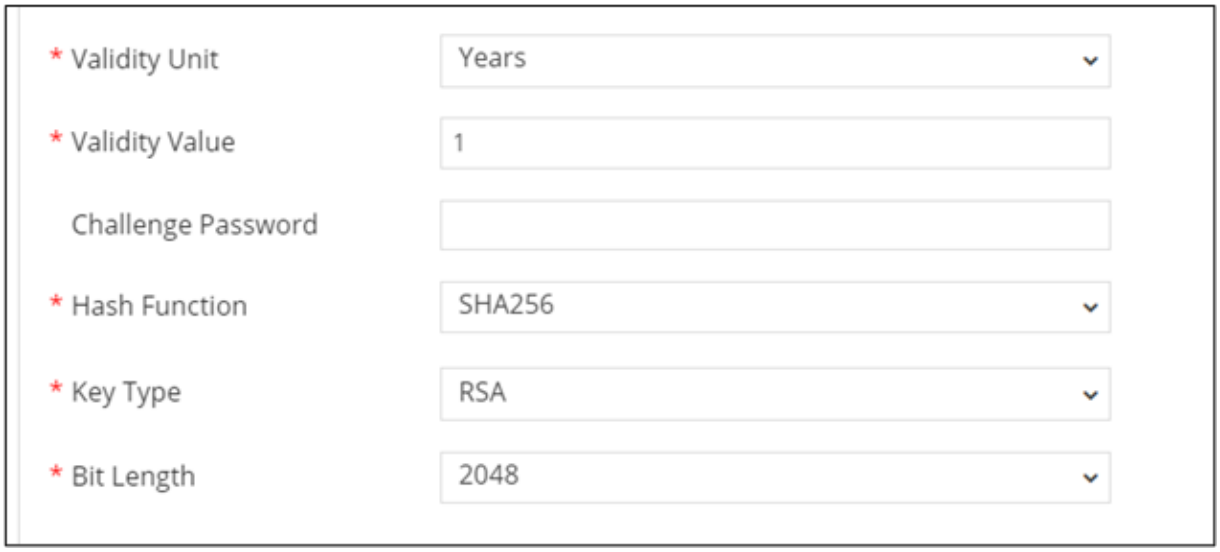
Policy Based

After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter the field information as shown.

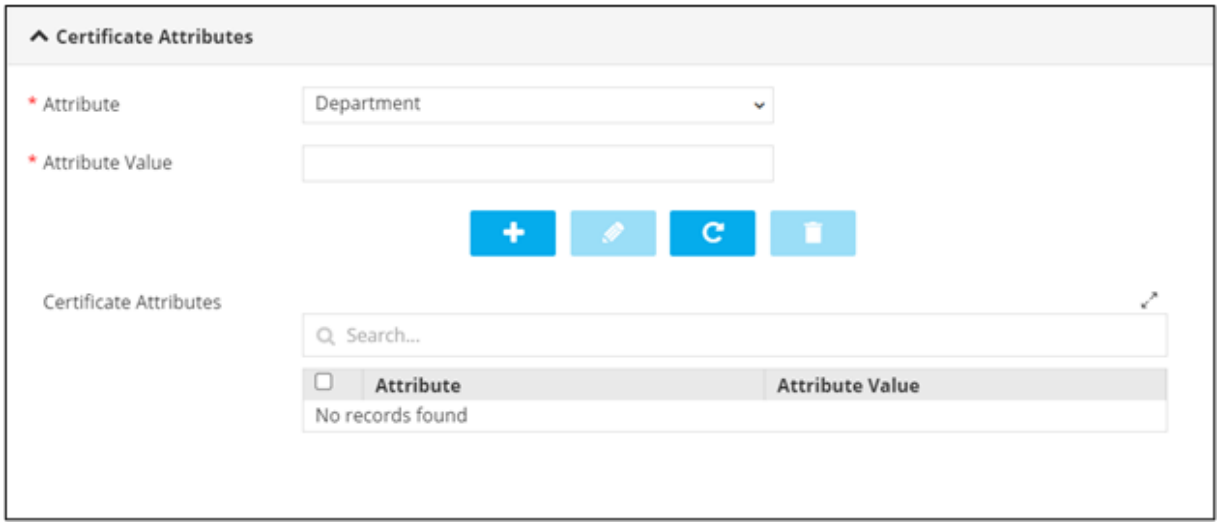
> **Note:** Some **CSR Parameters** will be auto-populated based on the policy associated with the **Certificate Group**.





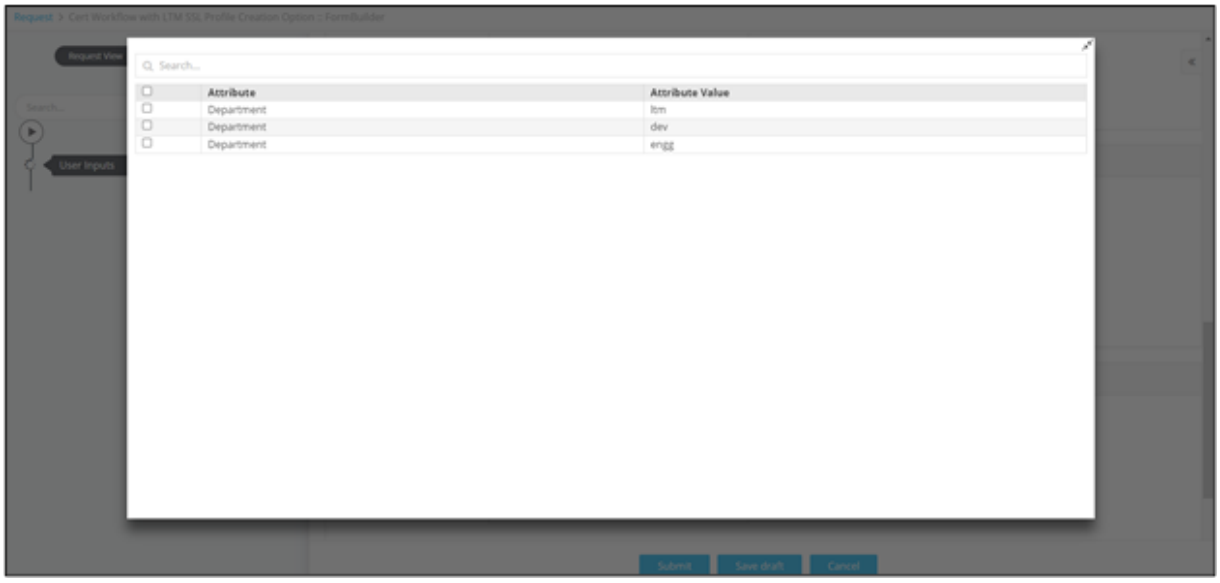
Note: For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

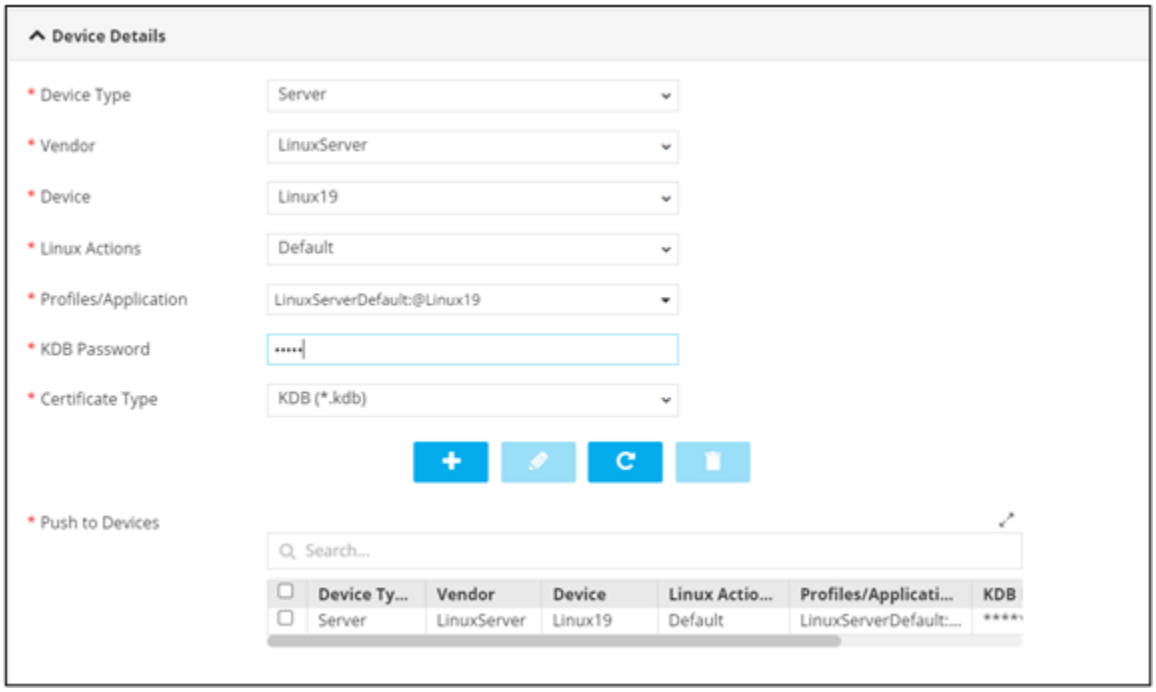


4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .
6. Enter the new value for the attribute in the **Value** field and click again to update the value.

7. To delete a certificate attribute, select the attribute in the grid and click  .
8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



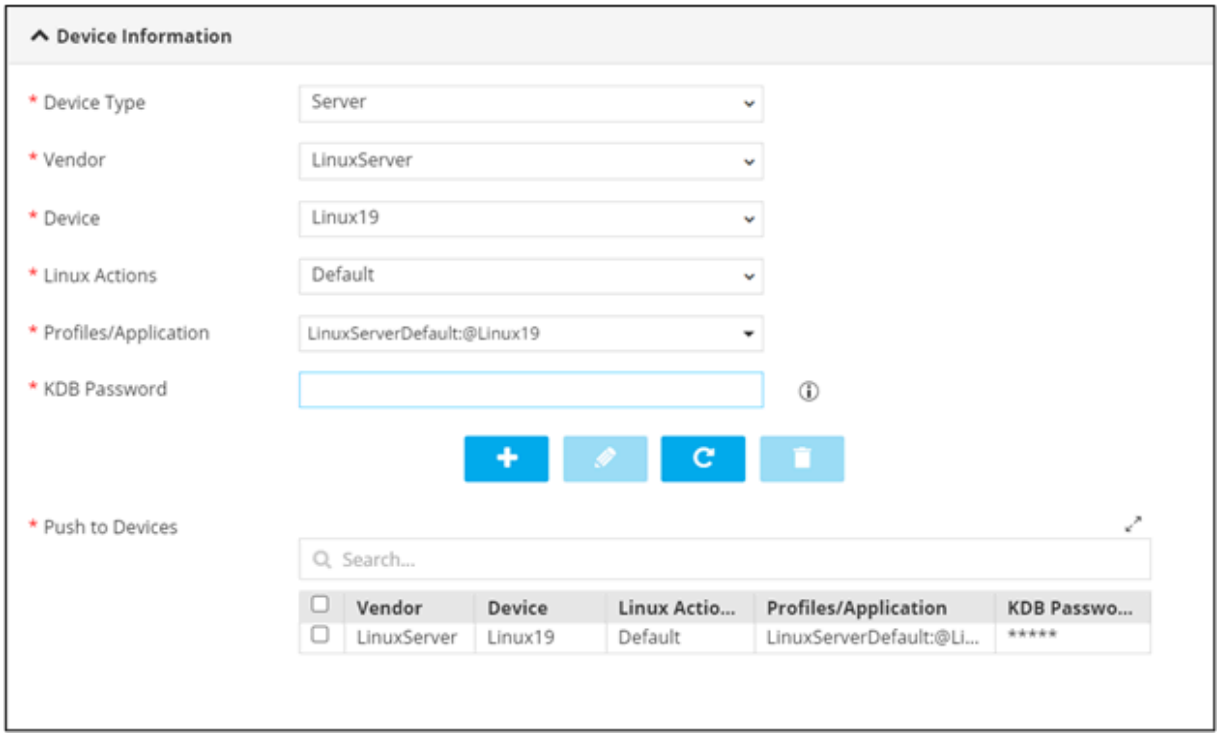
9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Device Details** section, select the field information as shown.



The following table describes the field information in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

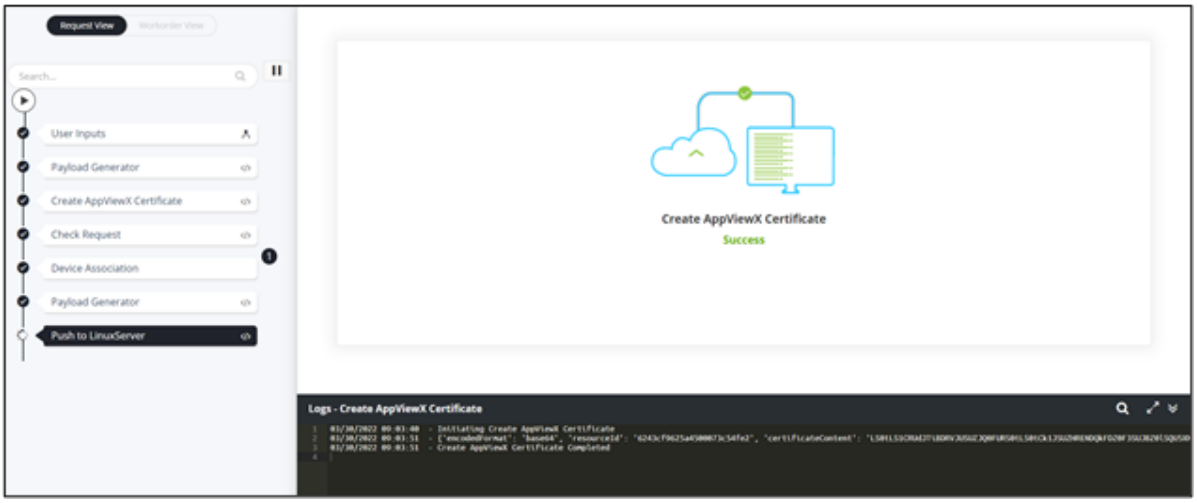
11. To add the selected profile/application to the grid, click  .
    The **Profile/Application** is added to the **Push to Devices** grid.



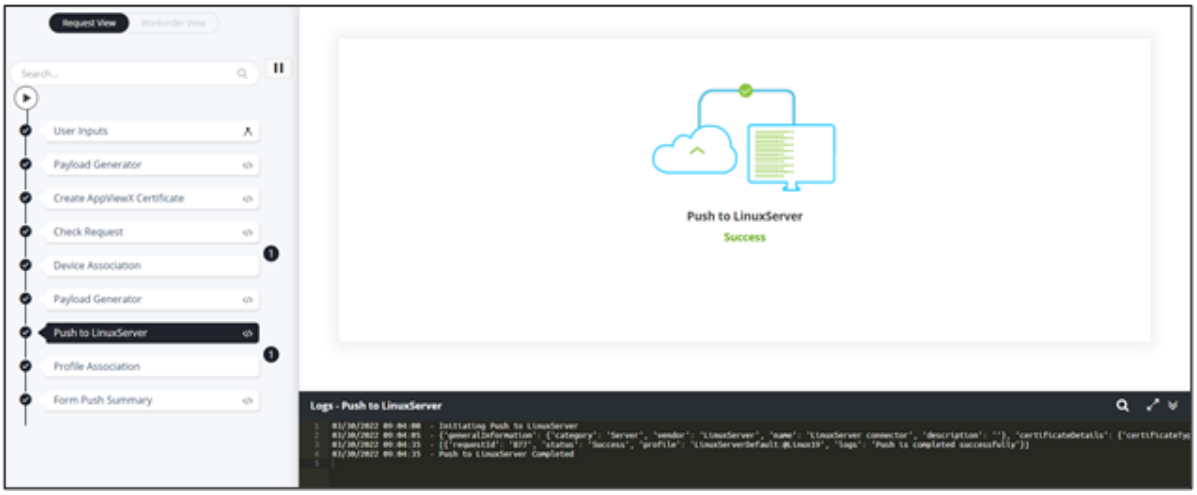
Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

12. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
13. Select a new device and click again to update the value.
14. To delete a profile/application, select the row to be deleted in the grid and click .
15. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
16. To search for a particular profile/application in the grid, type the keyword(s) in the search field.

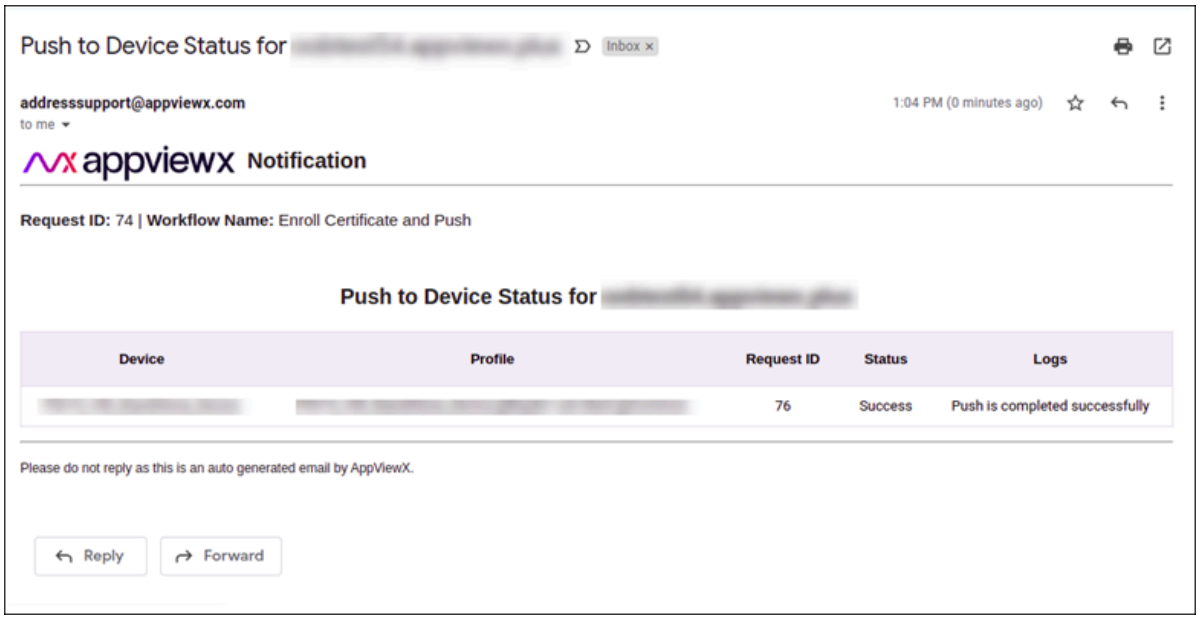
17. Click **Submit**.
    - Certificate created successfully.



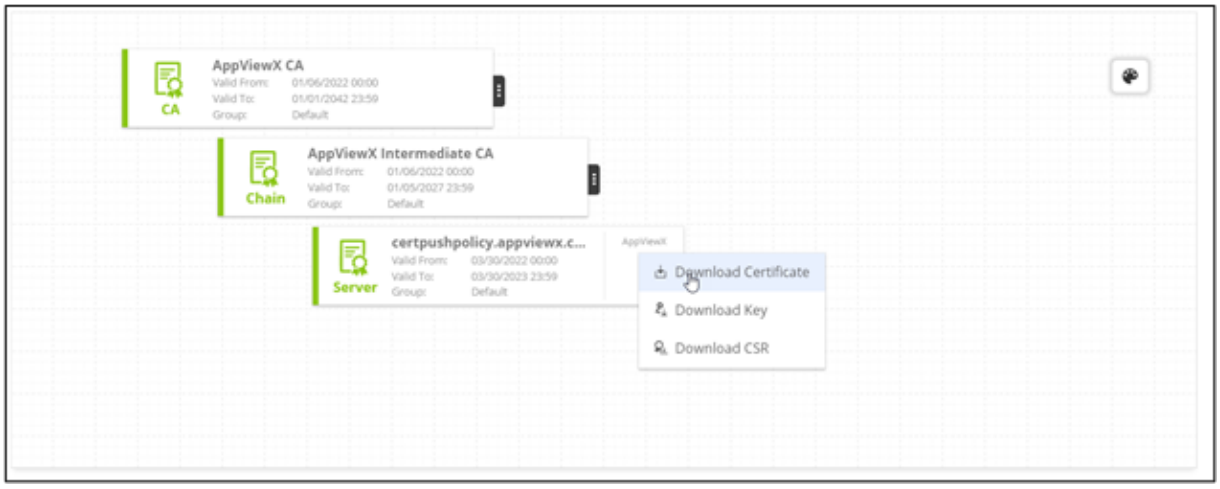
    - Certificate pushed to Linux server successfully.



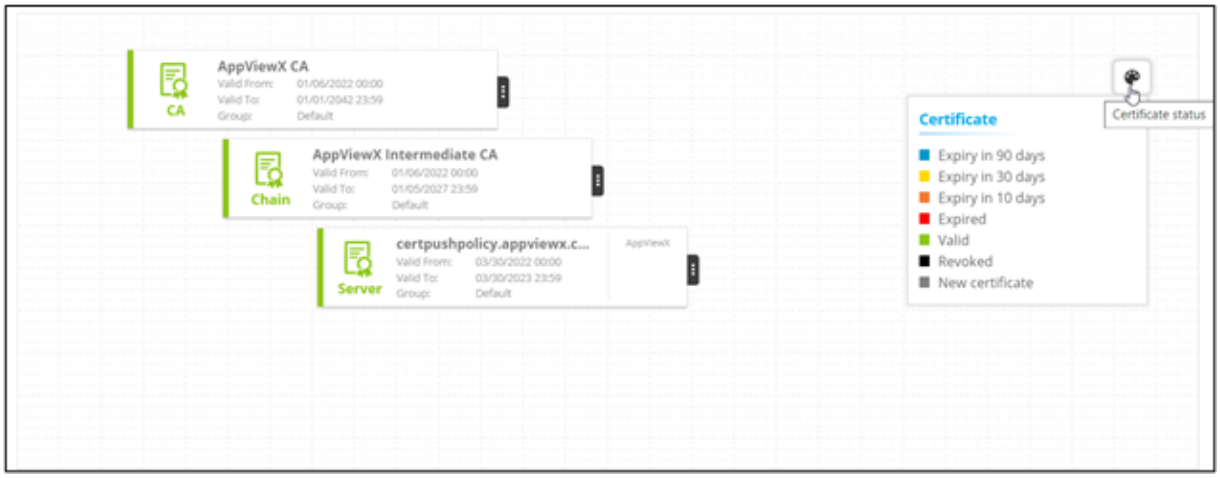
    - Email notification received.



18. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



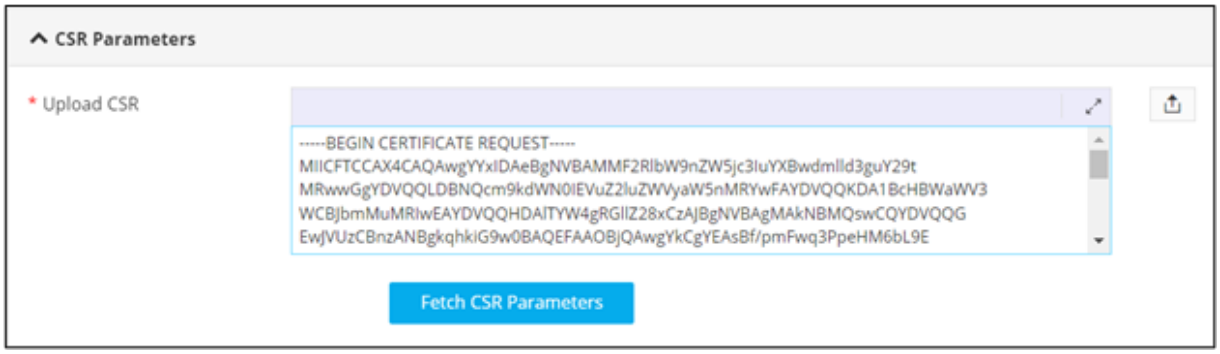
19. Hover your mouse over  to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

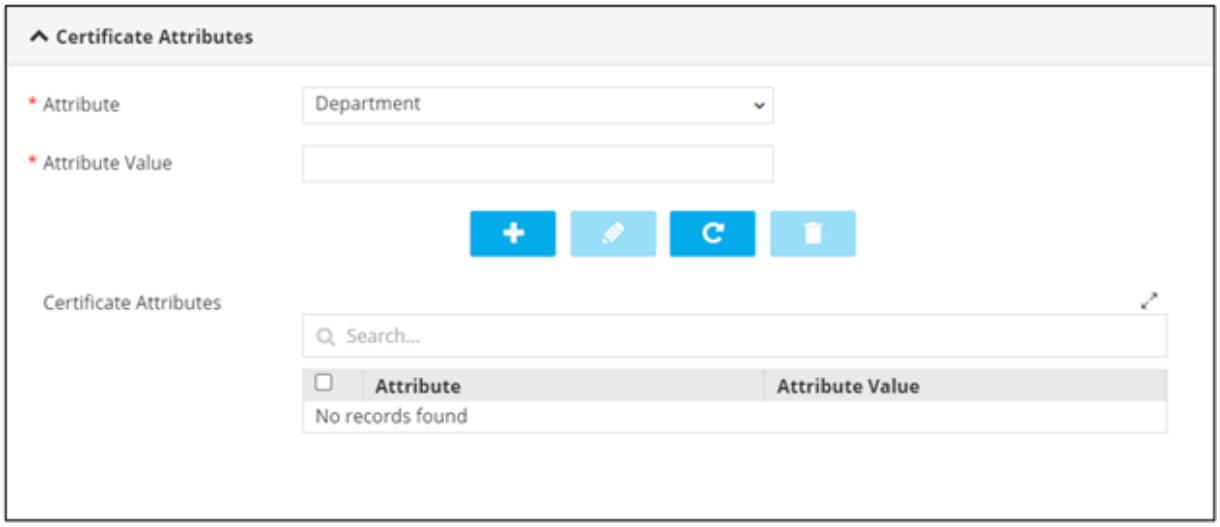
1. Under the **CSR Parameters** section, to **Upload CSR**, click .



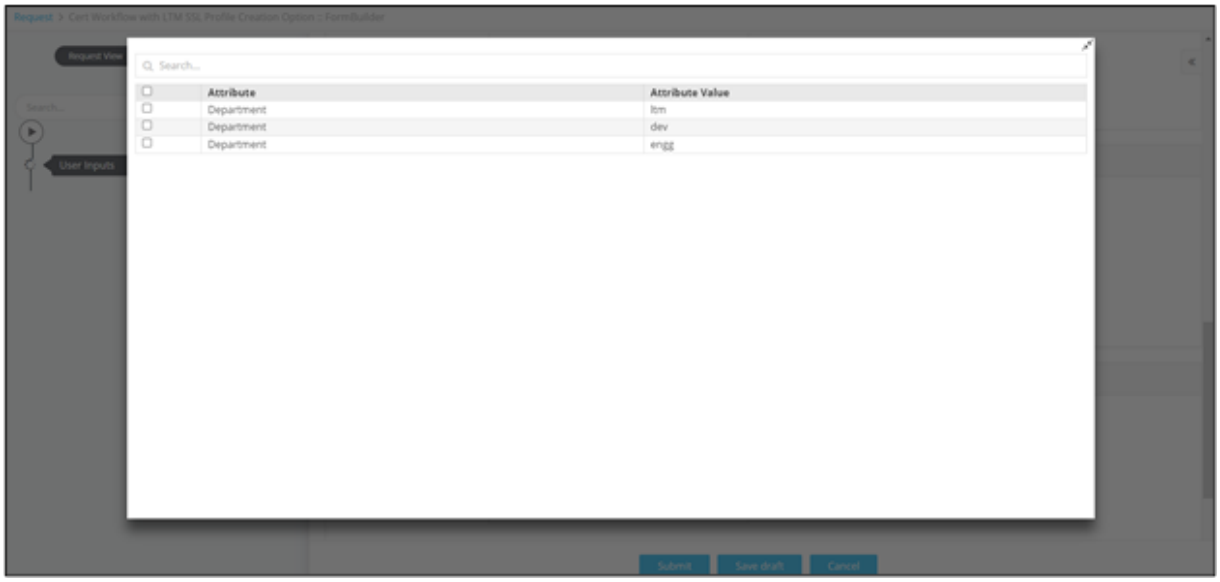
2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Policy Based section.

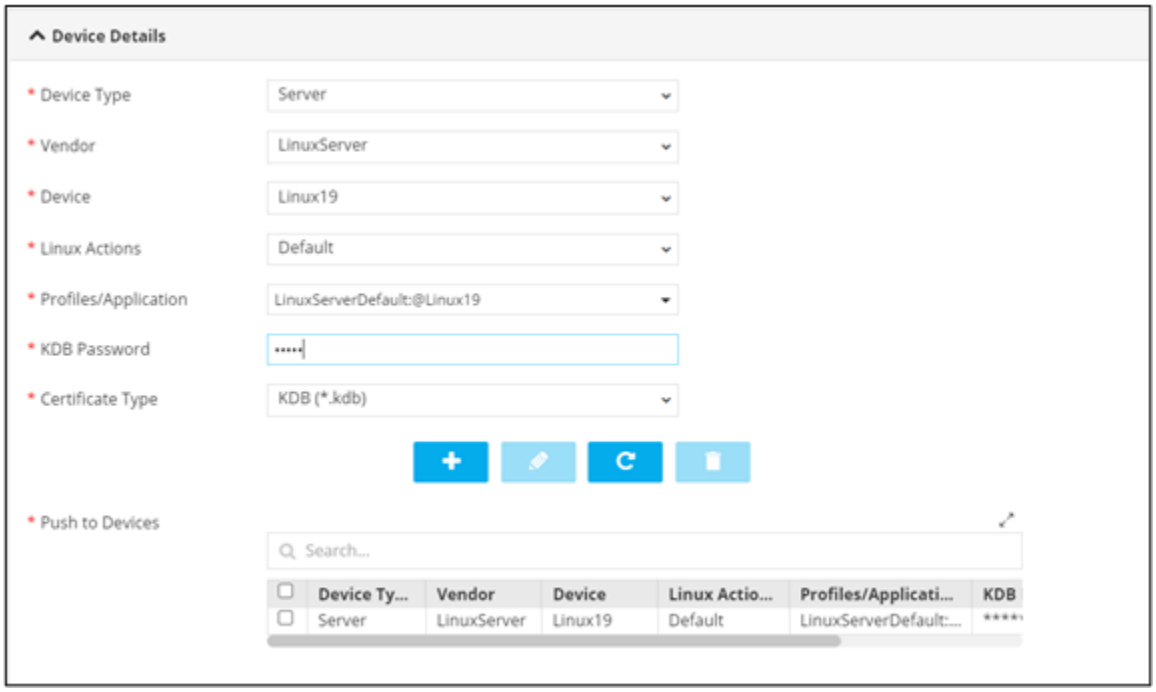
3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



5. To add this attribute to the **Certificate Attributes** grid, click .
6. To edit the value of a particular attribute, select the attribute in the grid and click .
7. Enter the new value for the attribute in the **Value** field and click again to update the value.
8. To delete a certificate attribute, select the attribute in the grid and click .
9. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



10. To search for a particular attribute in the grid, type the keyword(s) in the search field.
11. Under the **Device Details** section, select the field information as shown.

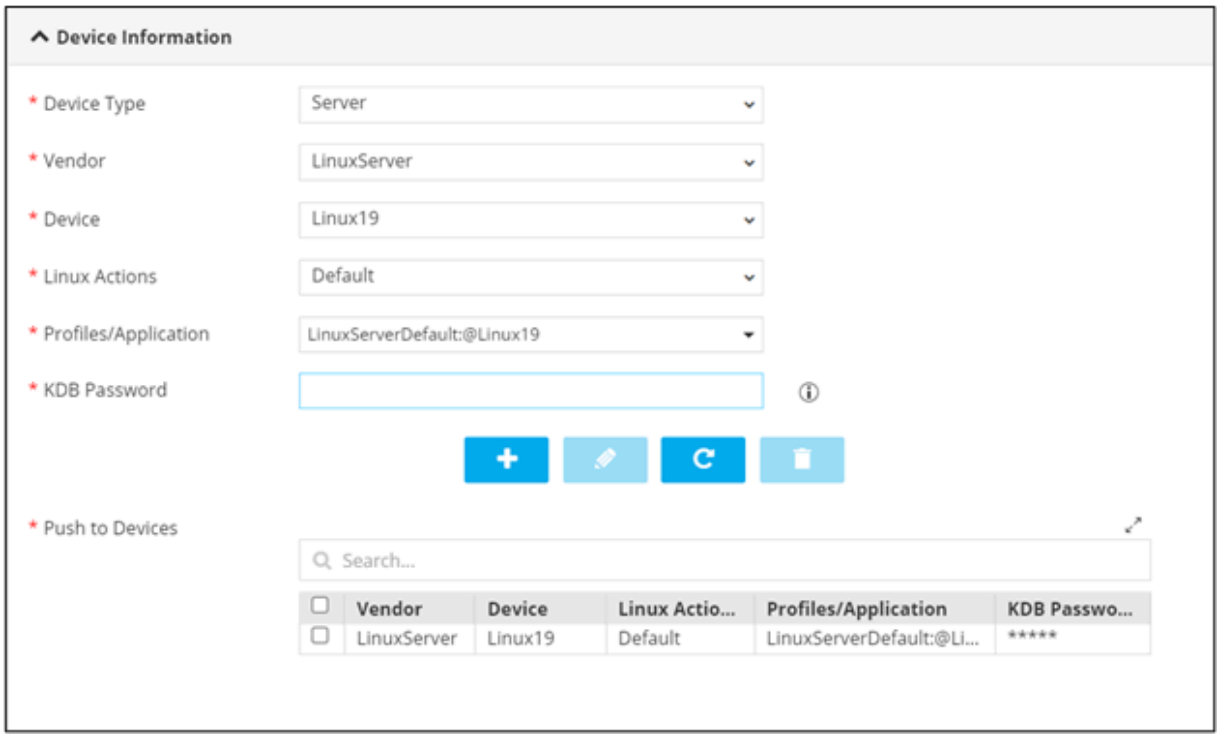


The following table describes the field information in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown.

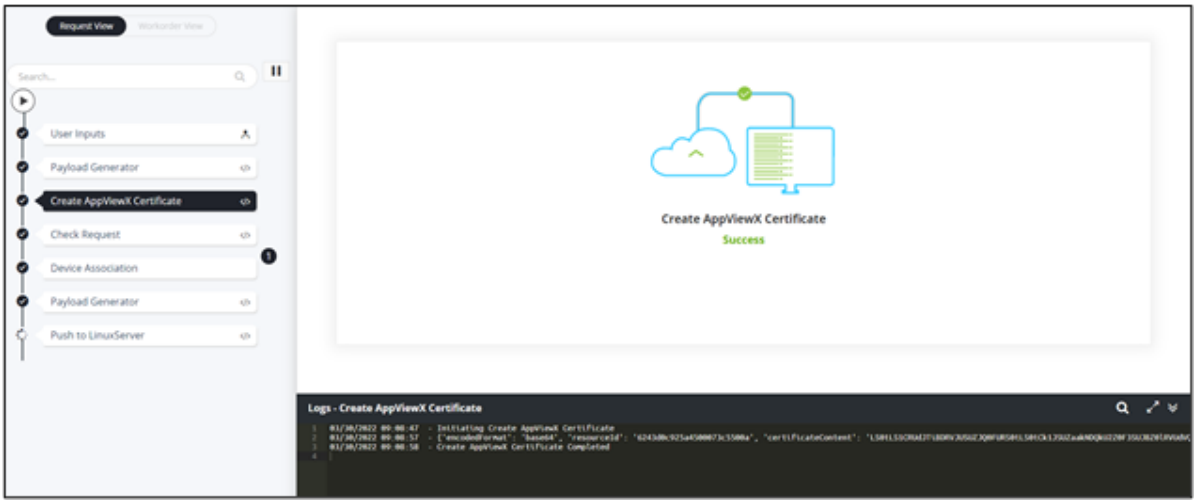
Field	Description
	Note: The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

12. To add the selected profile/application to the grid, click +.
    The **Profile/Application** is added to the **Push to Devices** grid.

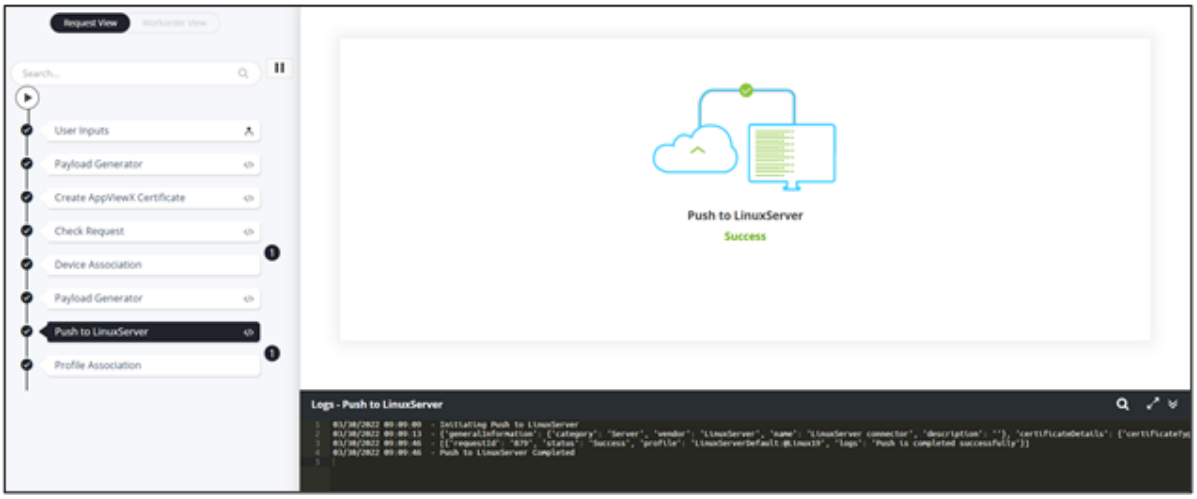


Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

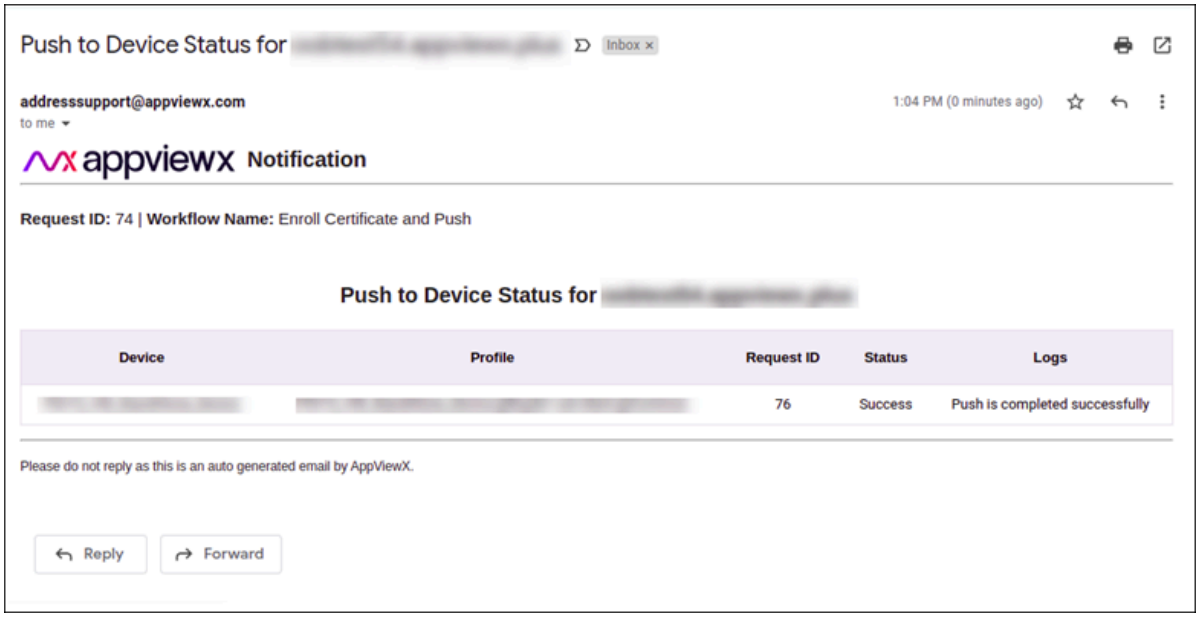
13. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click  .
14. Select a new device and click  again to update the value.
15. To maximize the **Push to Devices** grid, from the top right corner of the grid, click  .
16. To delete a profile/application, select the row to be deleted in the grid and click  .
17. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
18. Click **Submit**.
    - Certificate created successfully.



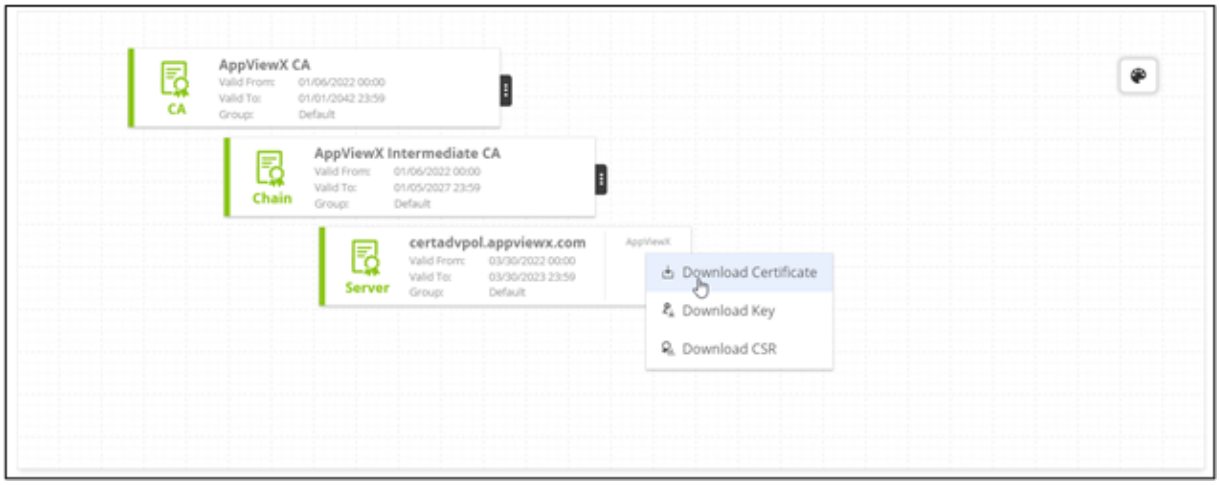
    - Certificate pushed to Linux server successfully.



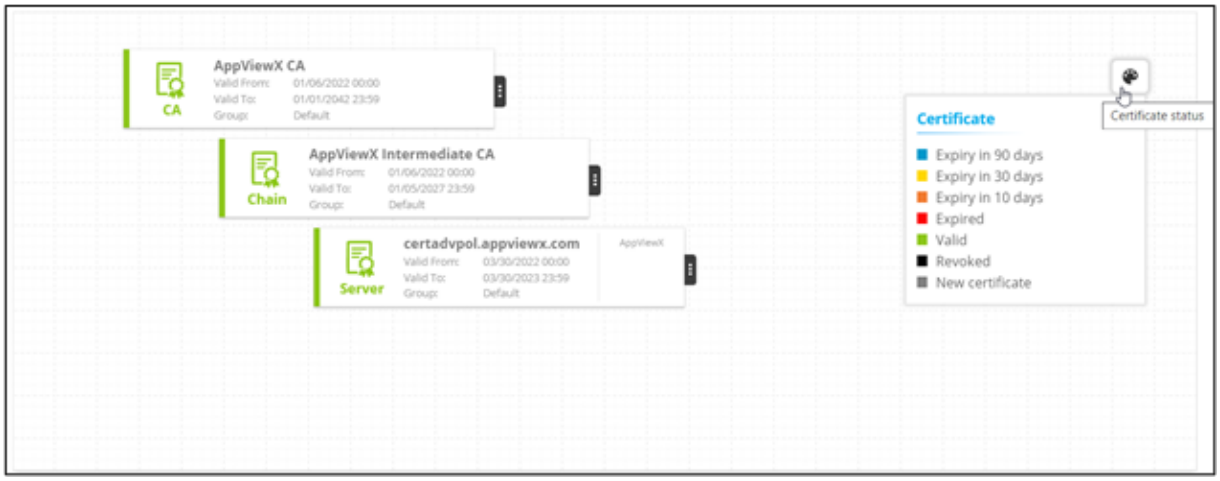
- Email notification received.



19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



20. Hover your mouse over  to view the **Certificate status**.



Chapter 7: Renew Certificate Workflows

Overview

This section lists and describes the workflows that can be used to renew and regenerate certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Renewal with Incident Automation.

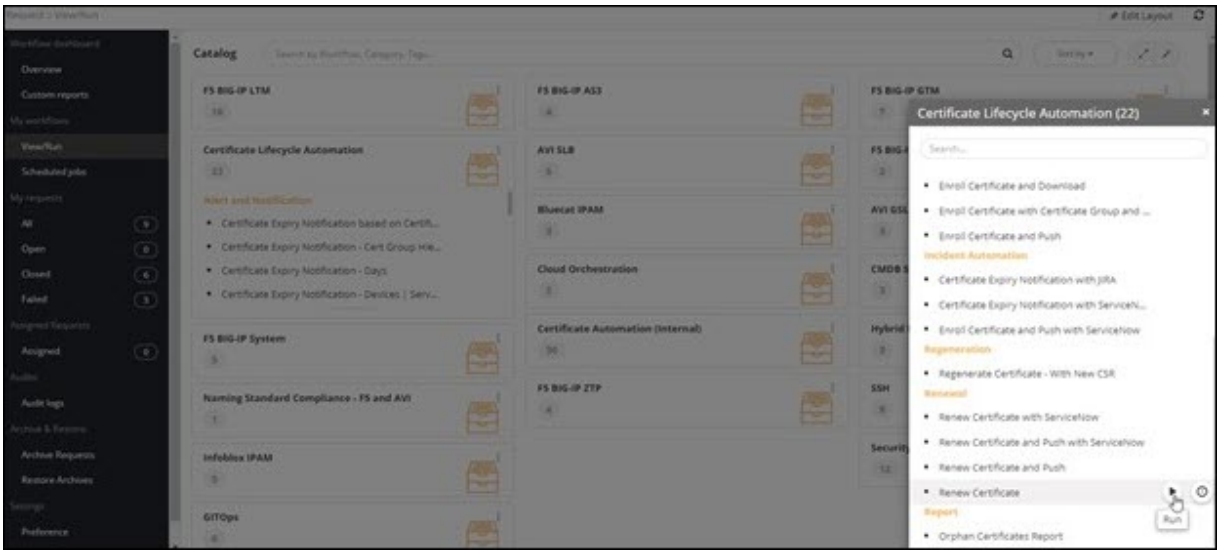
Renew Certificate

This workflow allows you to renew a certificate based on the certificate group and certificate authority.

To trigger this workflow:

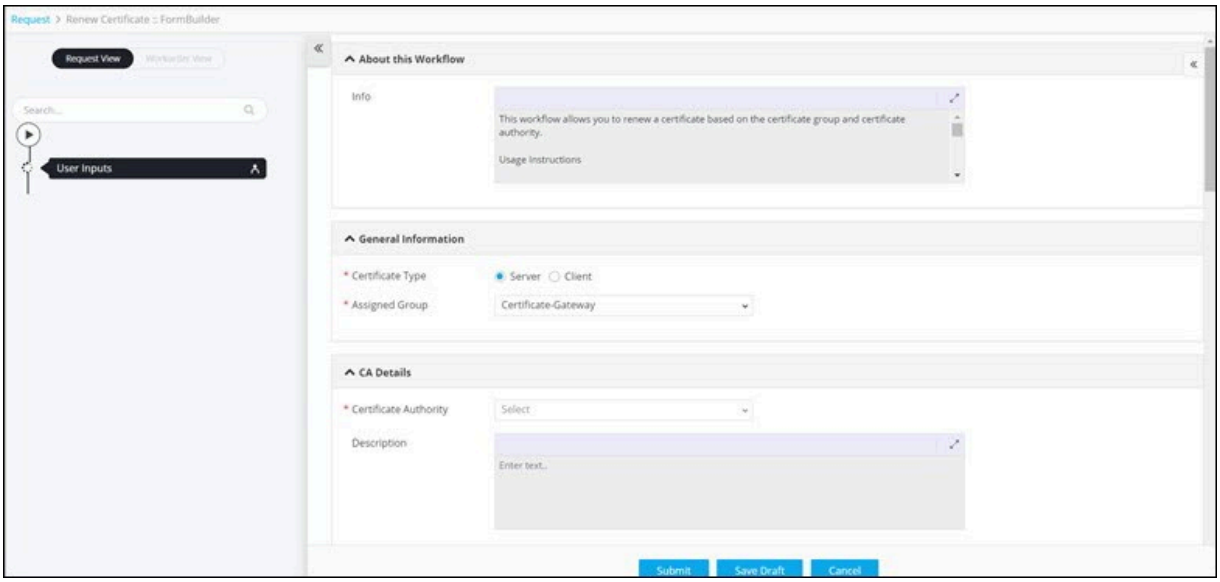
1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate** workflow and click .

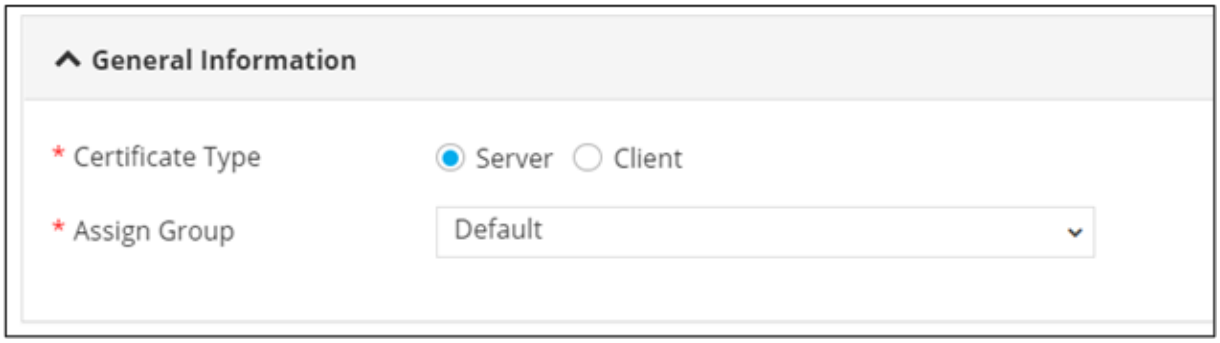


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.

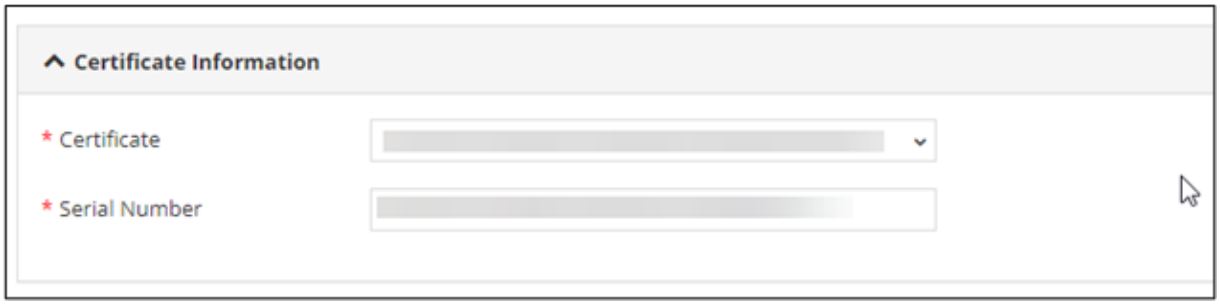


5. Under the **General Information** section, select the **Certificate Type** (mandatory).
6. Under the **General Information** section, select the **Assign Group** (mandatory).

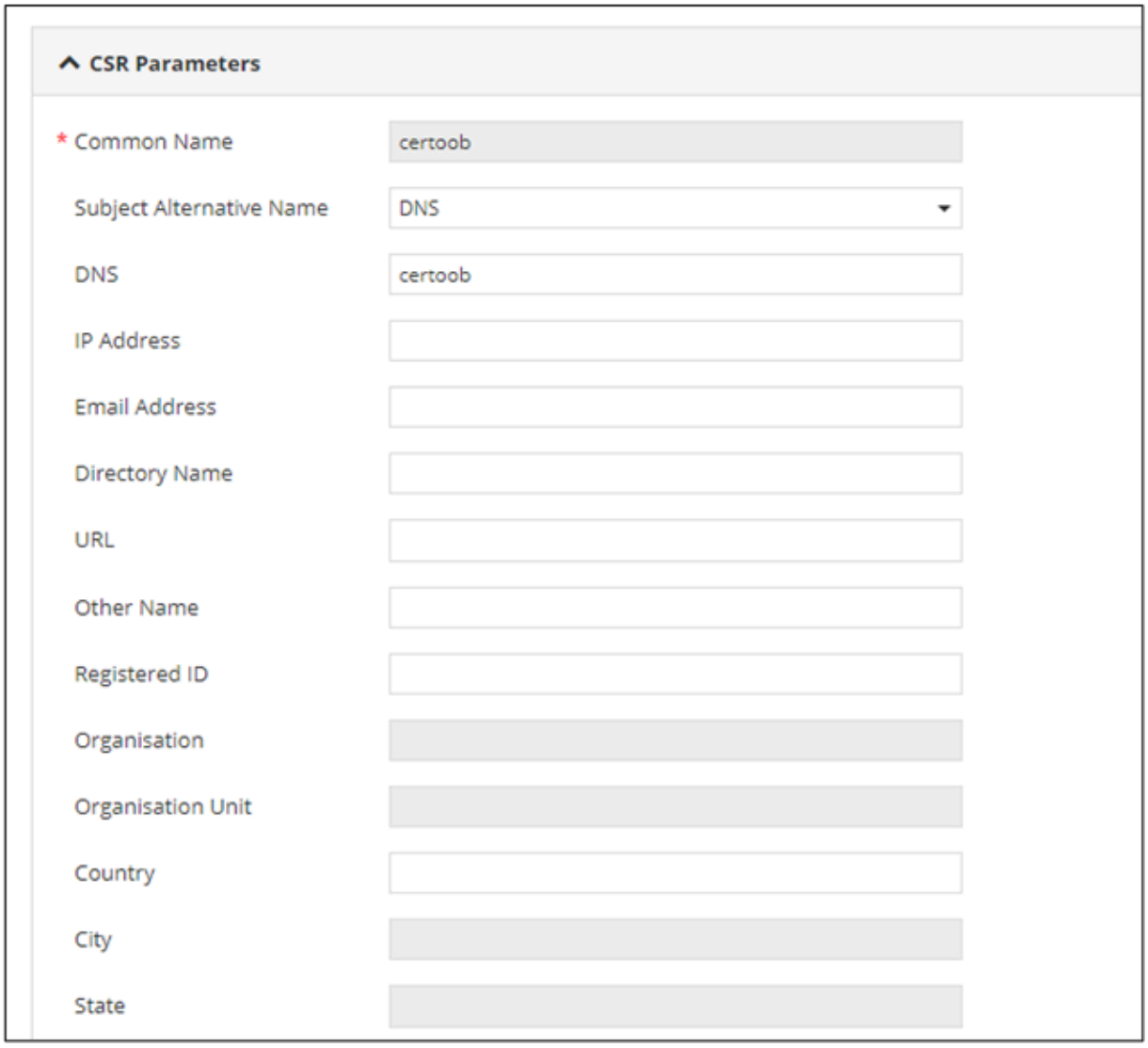


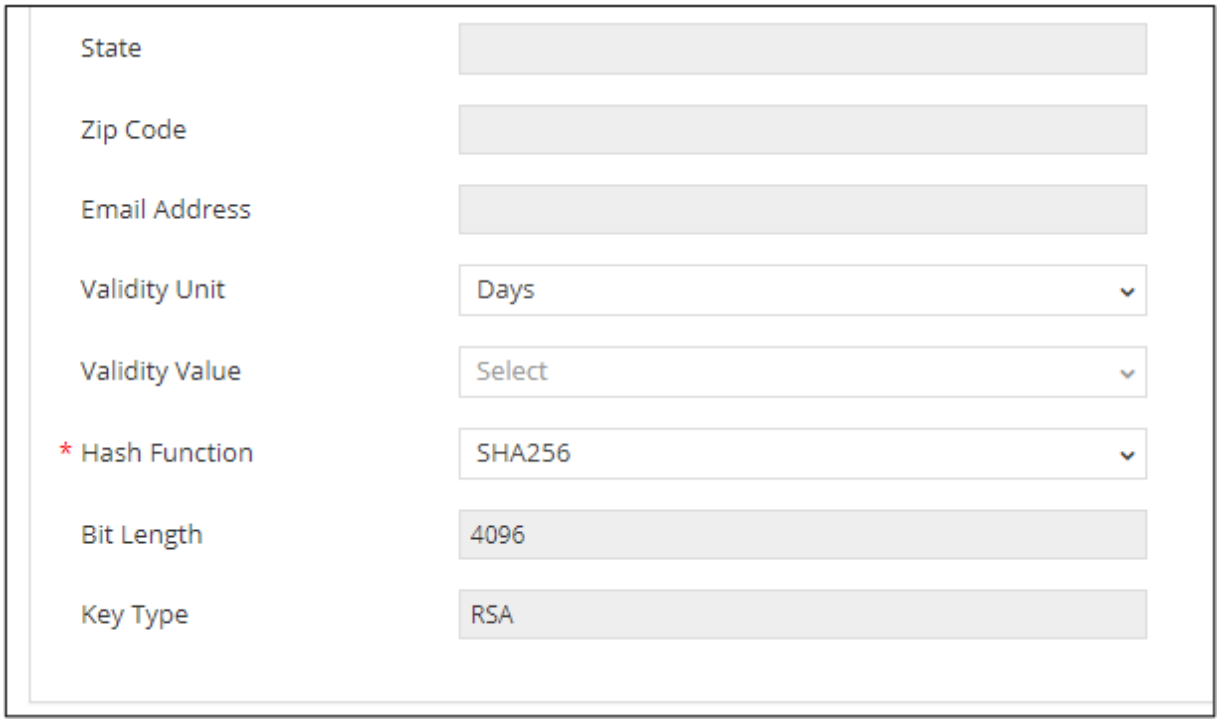
7. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
8. Under the **CA Details** section, add a description for the certificate being renewed (optional).

9. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.



10. Under the **CSR Parameters** section**,** enter or select the field information as shown.



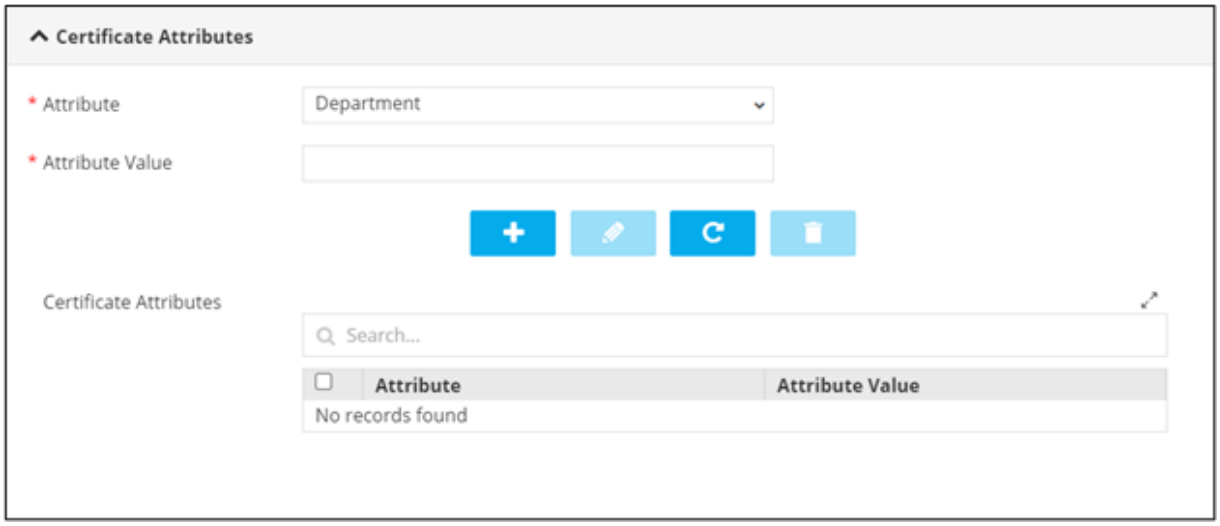


The following table describes the fields in the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

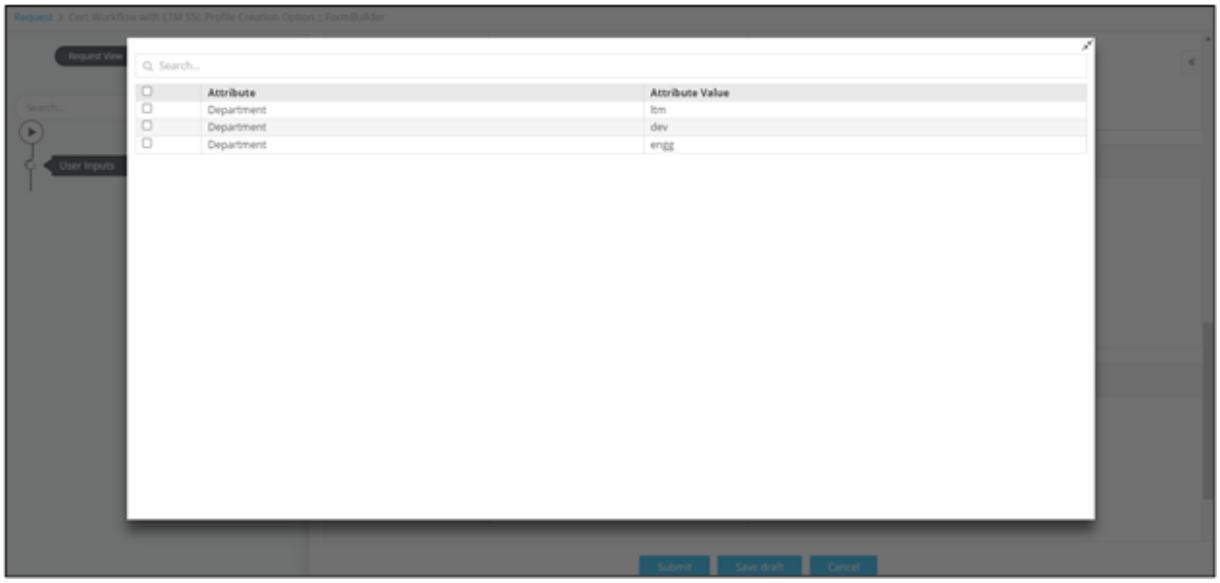
Field	Description
	Note: This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

11. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
12. Enter a value for the selected attribute.

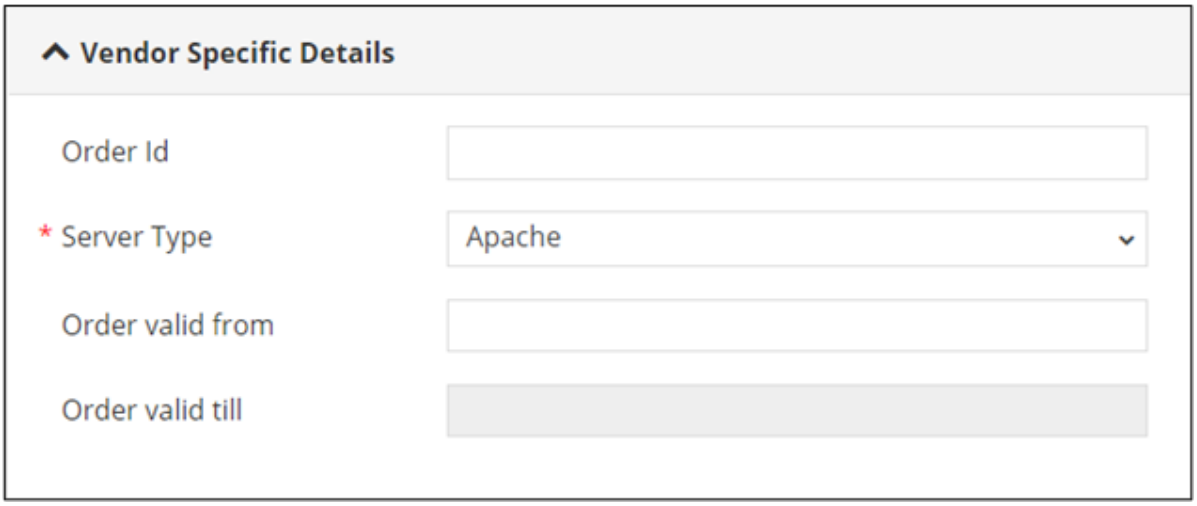


13. To add this attribute to the **Certificate Attributes** grid, click .
14. To edit the value of a particular attribute, select the attribute in the grid and click .

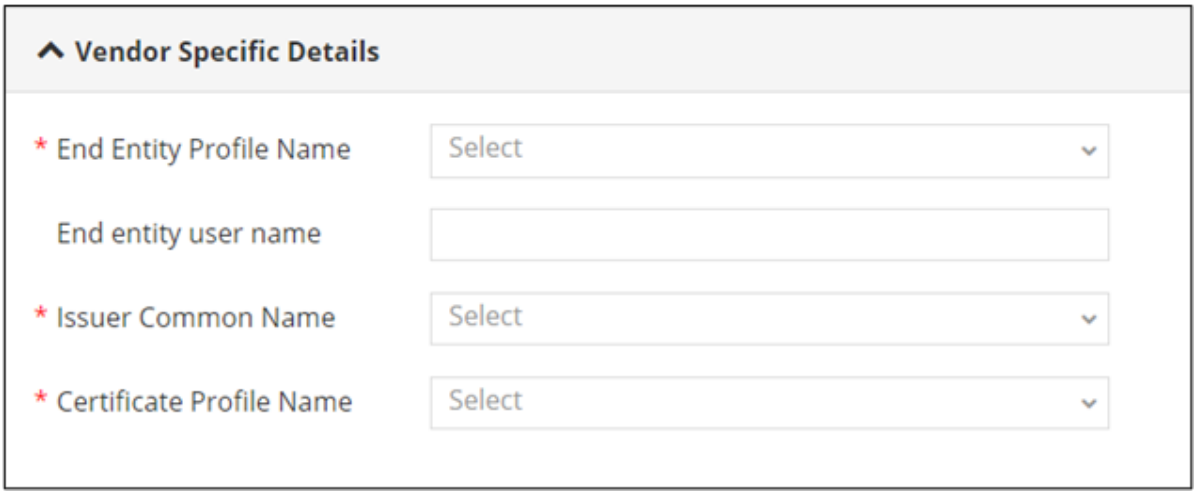
15. Enter the new value for the attribute in the **Value** field and click again to update the value.
16. To delete a certificate attribute, select the attribute in the grid and click .
17. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .



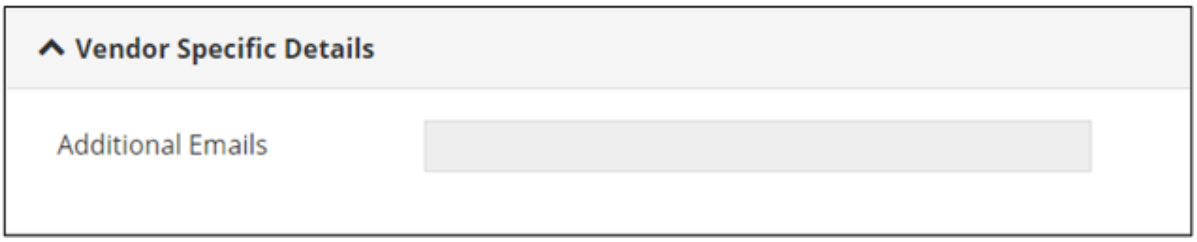
18. To search for a particular attribute in the grid, type the keyword(s) in the search field.
19. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.



    - When EJBCA is selected as CA.

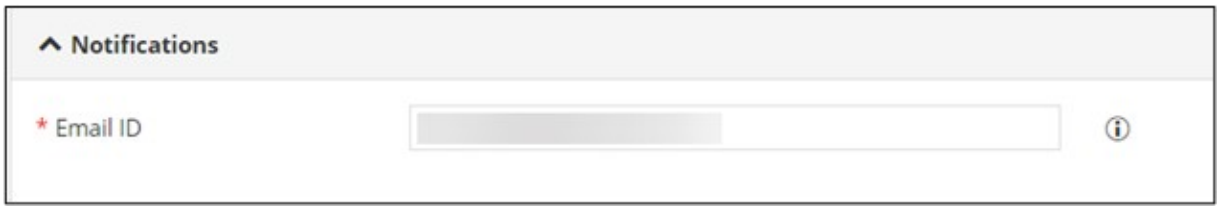


- When Entrust is selected as CA.



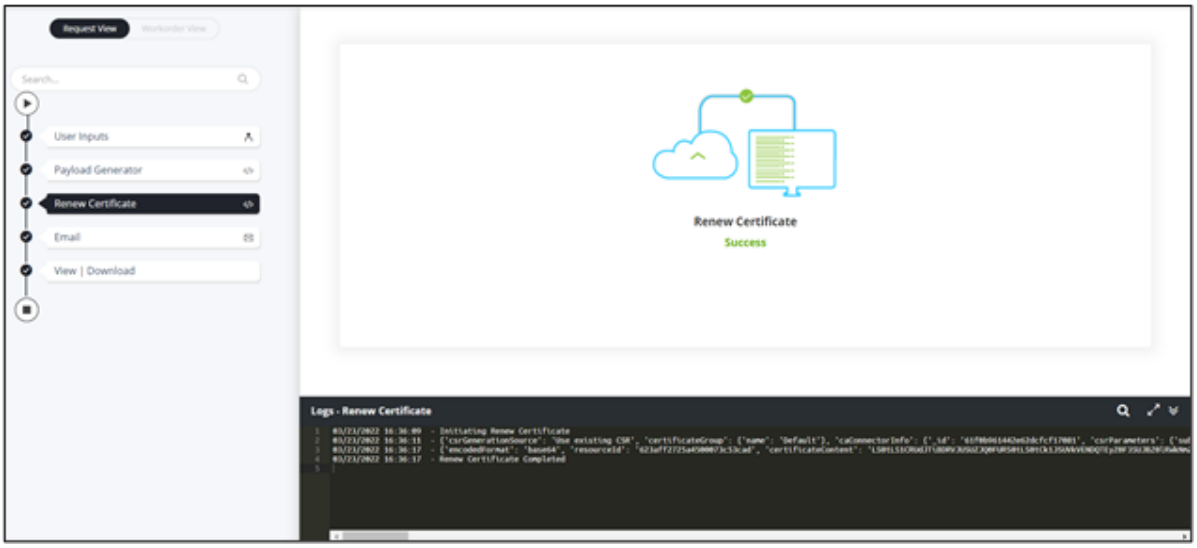
Note: The Vendor Specific Details section is displayed only when DigiCert, EJBCA, Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

20. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

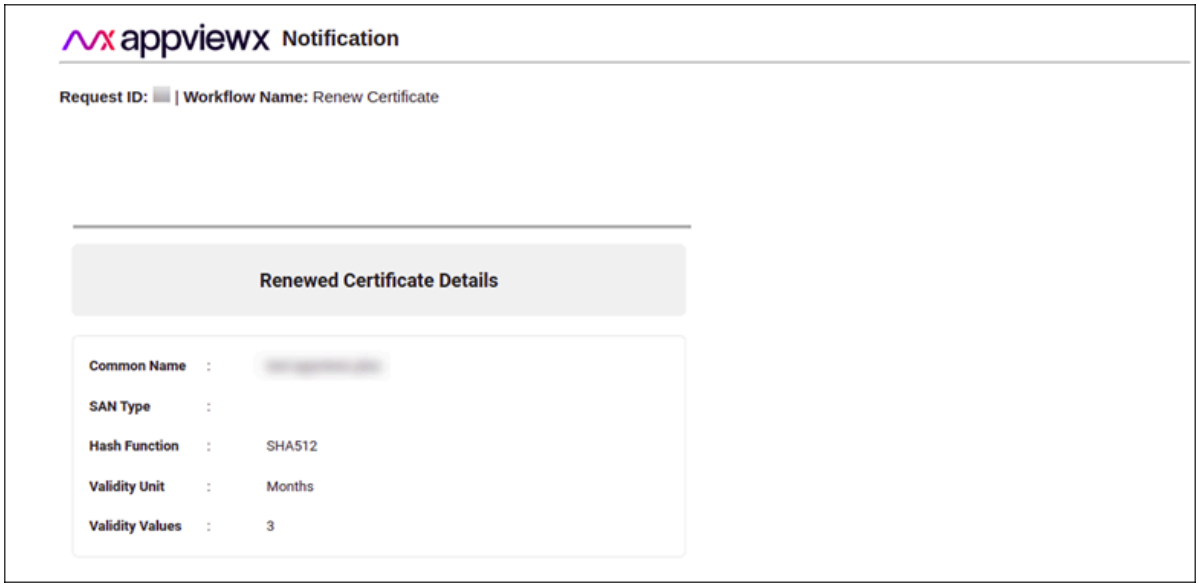


Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

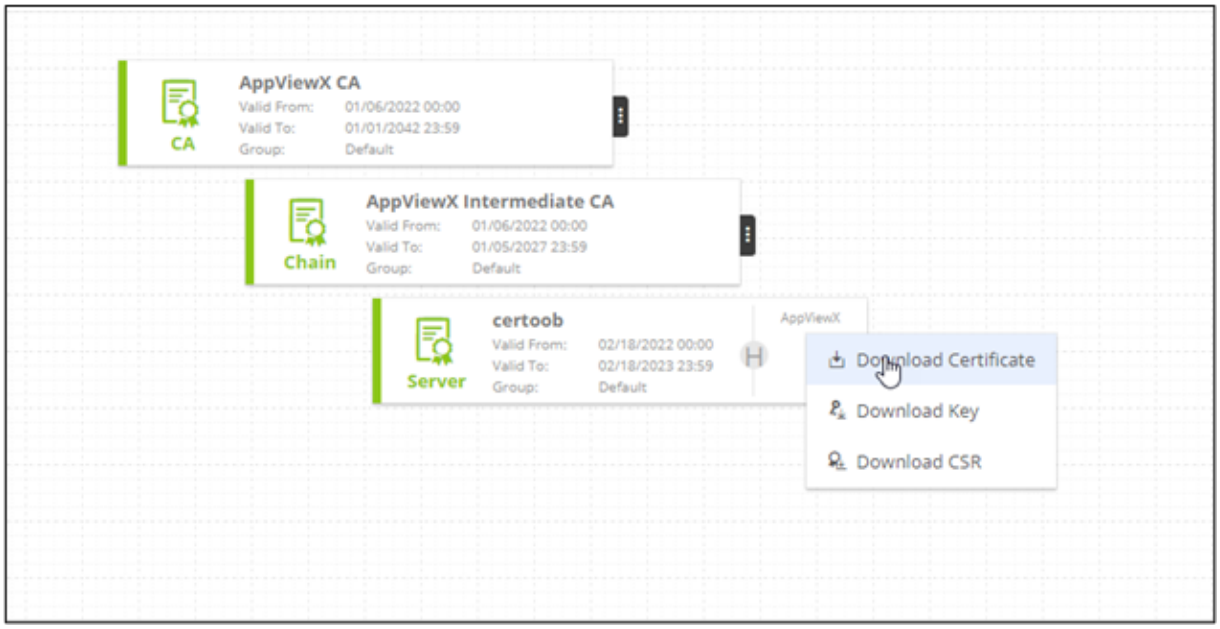
21. Click **Submit**.
    - Certificate renewed successfully.



    - Email notification received.



22. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



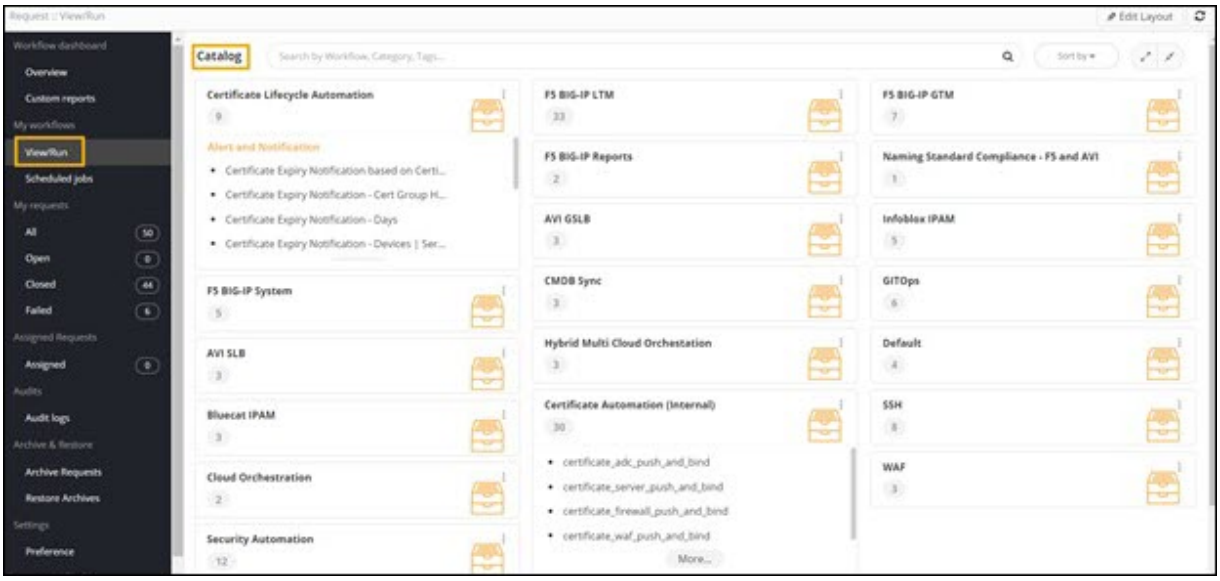
23. Hover your mouse over  to view the **Certificate status**.

Regenerate Certificate with New CSR

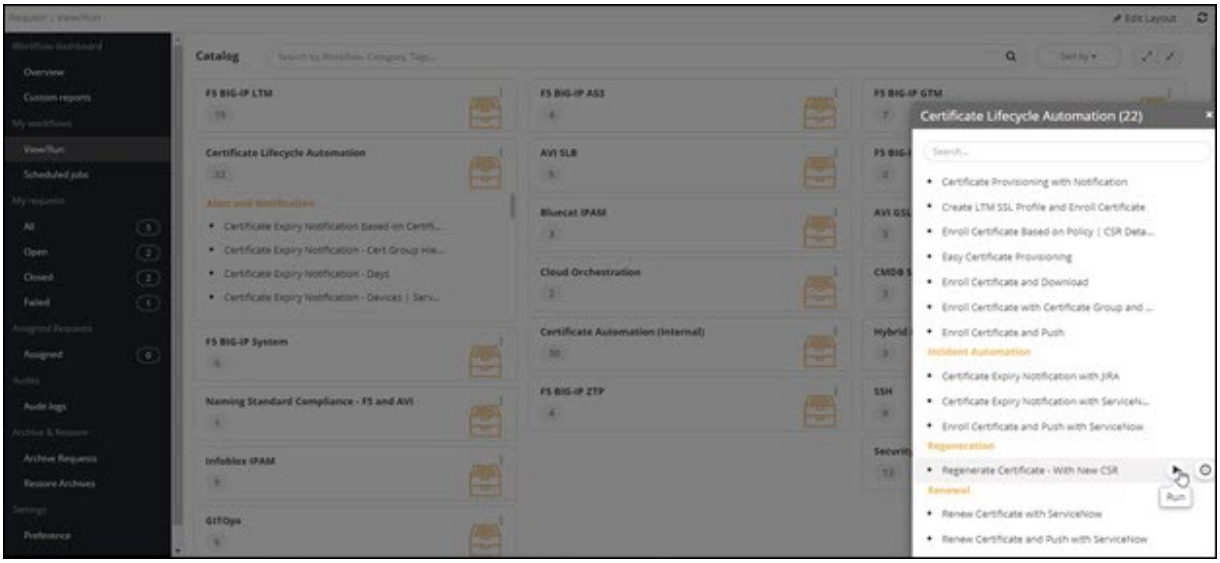
This workflow allows you to regenerate a certificate with a new CSR.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

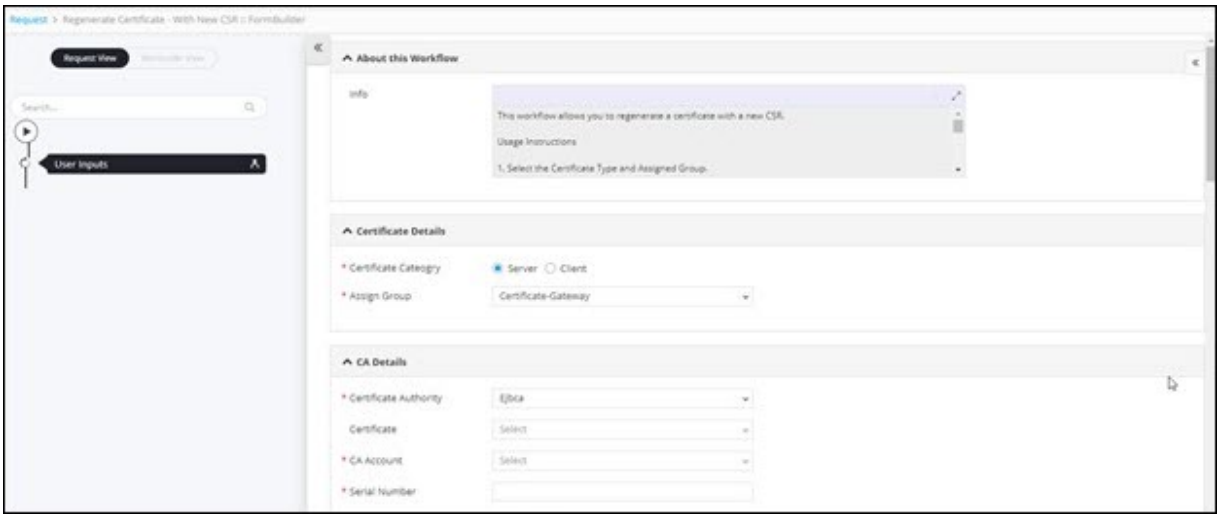


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Regenerate Certificate with New CSR** workflow and click .



Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **Certificate Details** section, select the **Certificate Type** (mandatory).
6. Under the **Certificate Details** section, select the **Assign Group** (mandatory).
7. Under the **CA Details** section, select the field information as shown:

   The following table describes the fields in the **CSR Parameters** section:

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown.

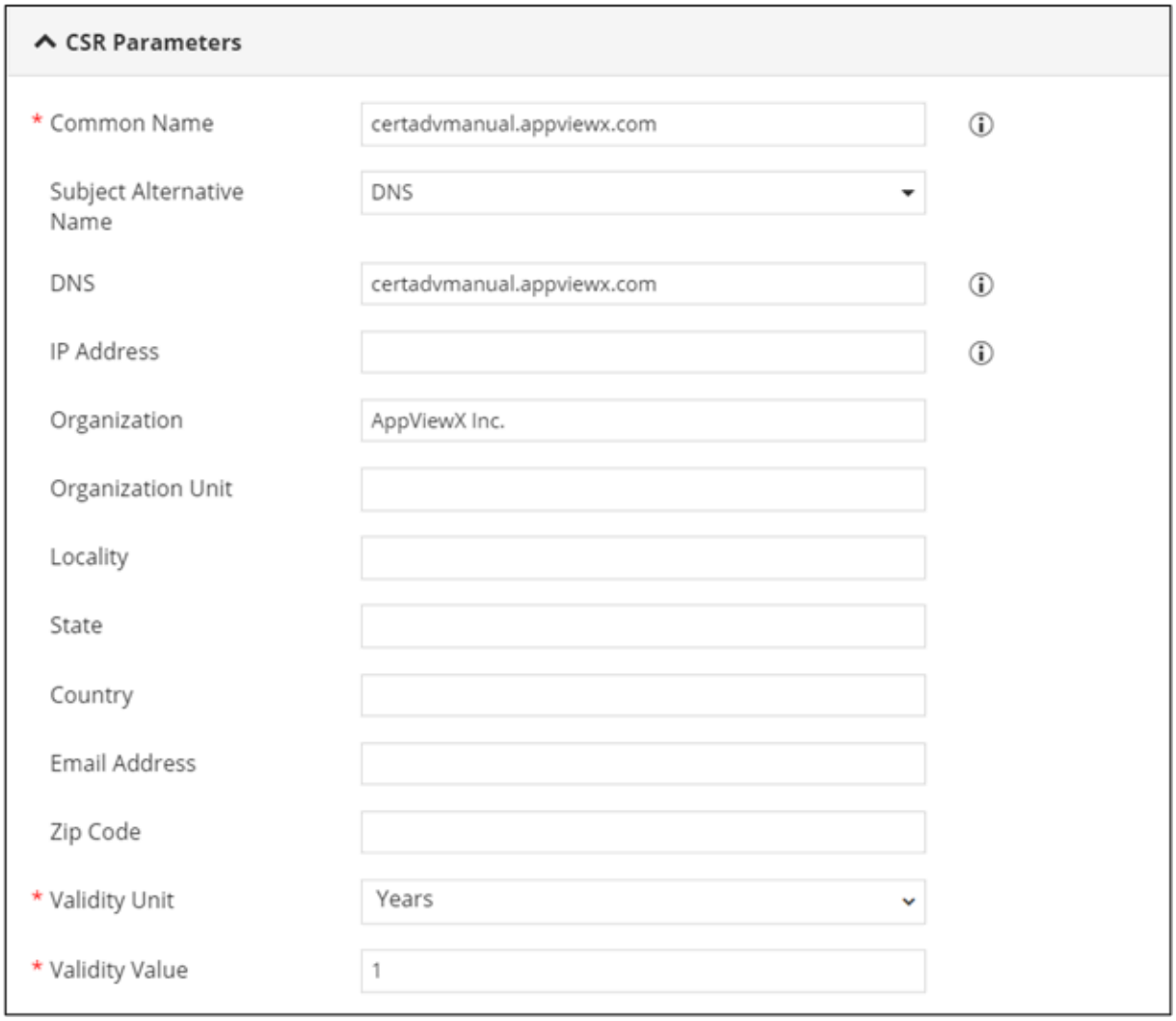
Field	Description
	Note: This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Provide a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter the field information as shown.

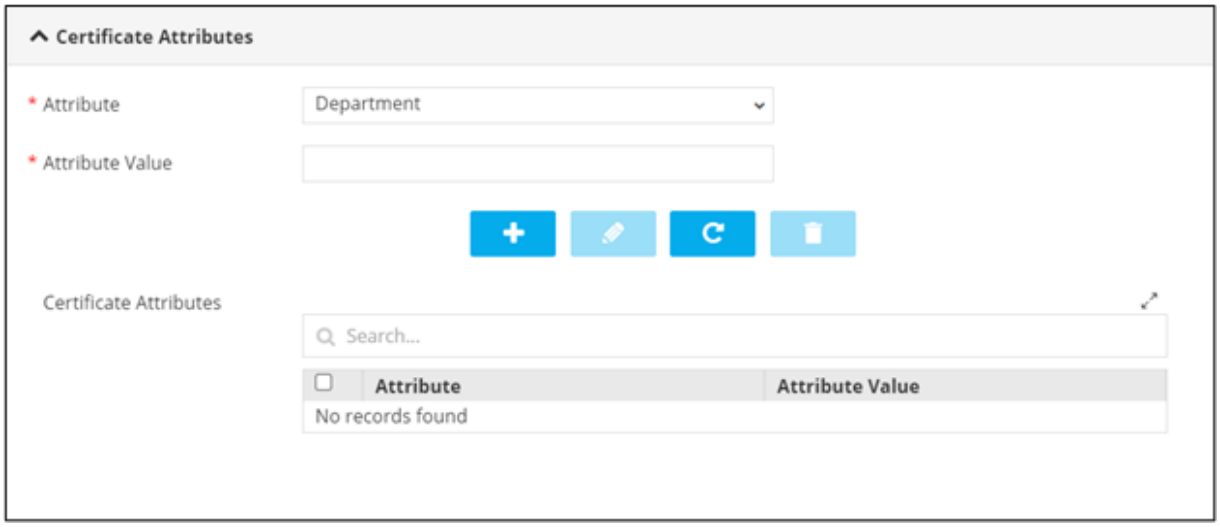


The following table describes the field information in the **CSR Parameters** section:

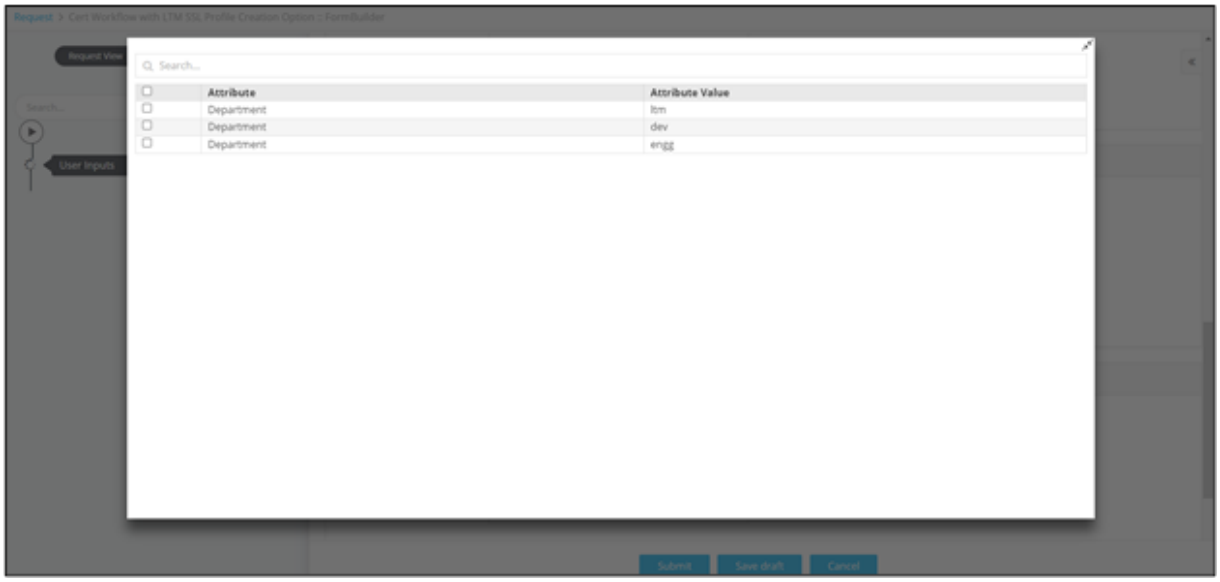
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name** • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.

Field	Description
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***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.  **Note:** This field will be populated based on the selected **Key Type**.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

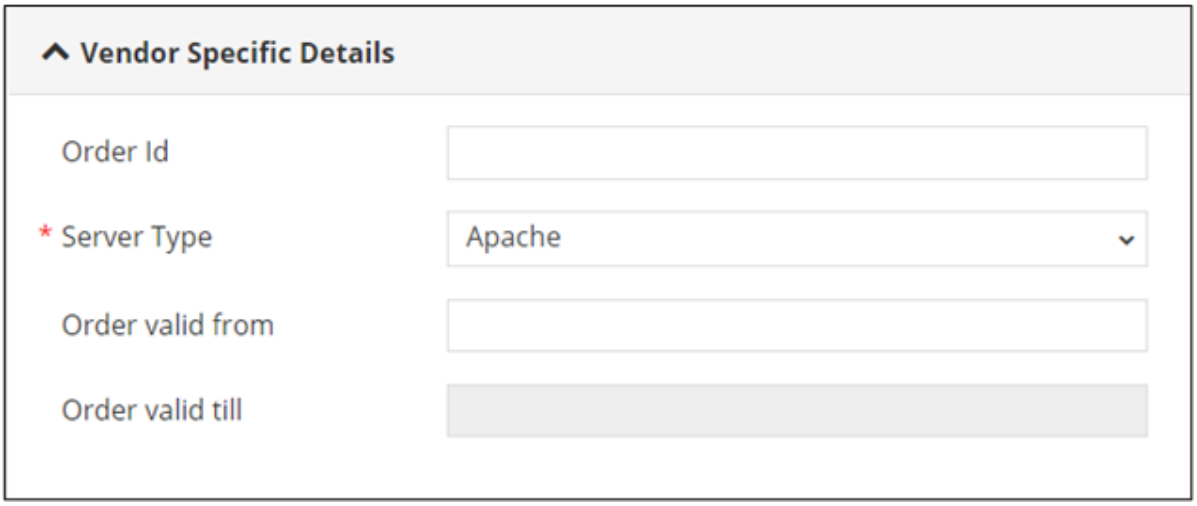


4. To add this attribute to the **Certificate Attributes** grid, click .
5. To edit the value of a particular attribute, select the attribute in the grid and click .
6. Enter the new value for the attribute in the **Value** field and click again to update the value.
7. To delete a certificate attribute, select the attribute in the grid and click .
8. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .

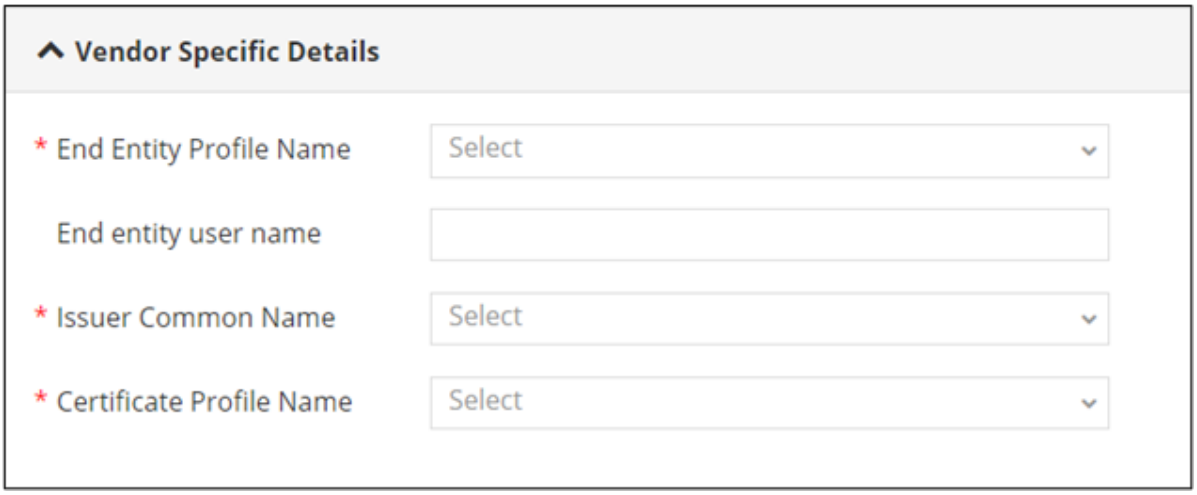


9. To search for a particular attribute in the grid, type the keyword(s) in the search field.
10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

• When Digicert is selected as CA.



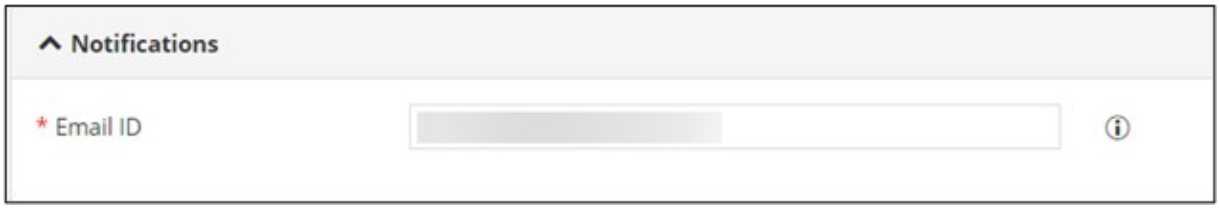
• When EJBCA is selected as CA.



• When Microsoft Enterprise is selected as CA.

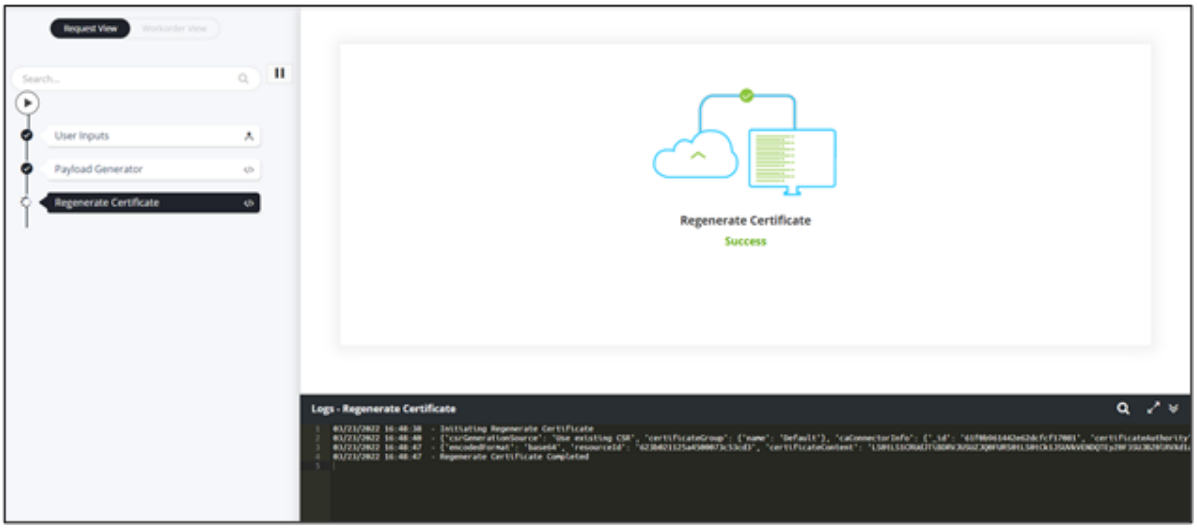
Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

11. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

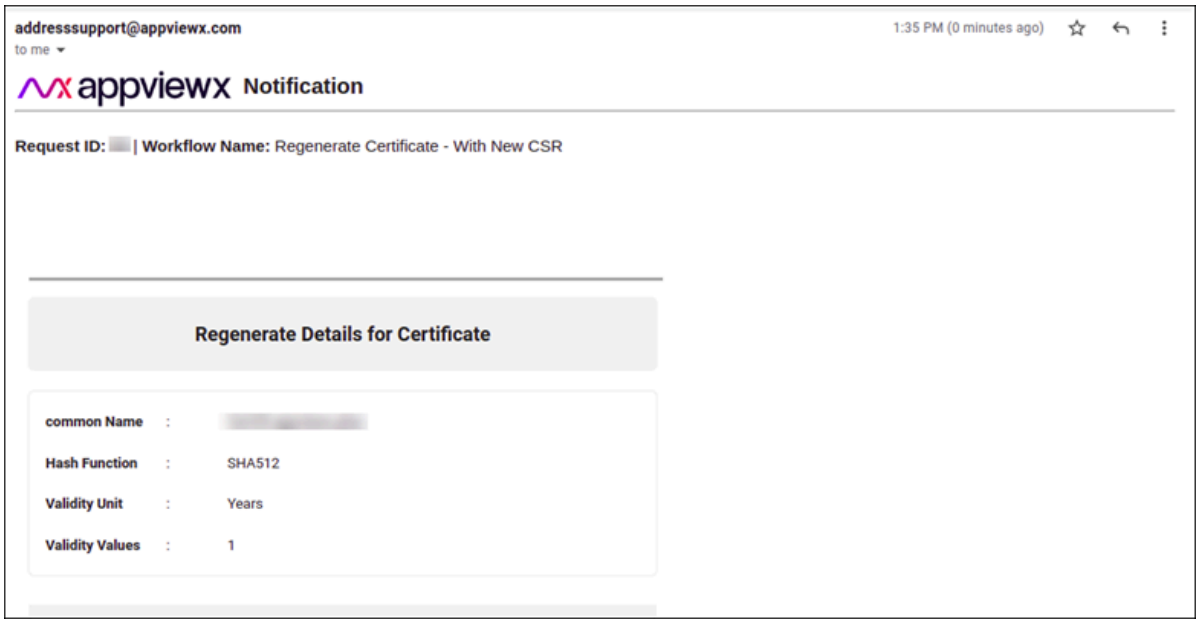


Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

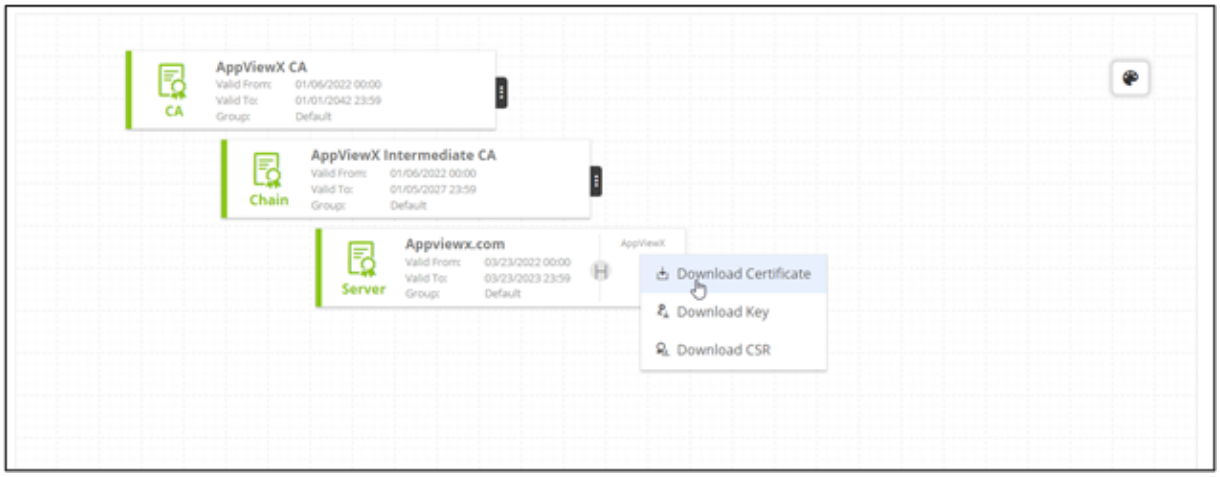
12. Click **Submit**.
    - Certificate regenerated successfully.



    - Email notification received.



13. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



14. Hover your mouse over  to view the **Certificate status**.

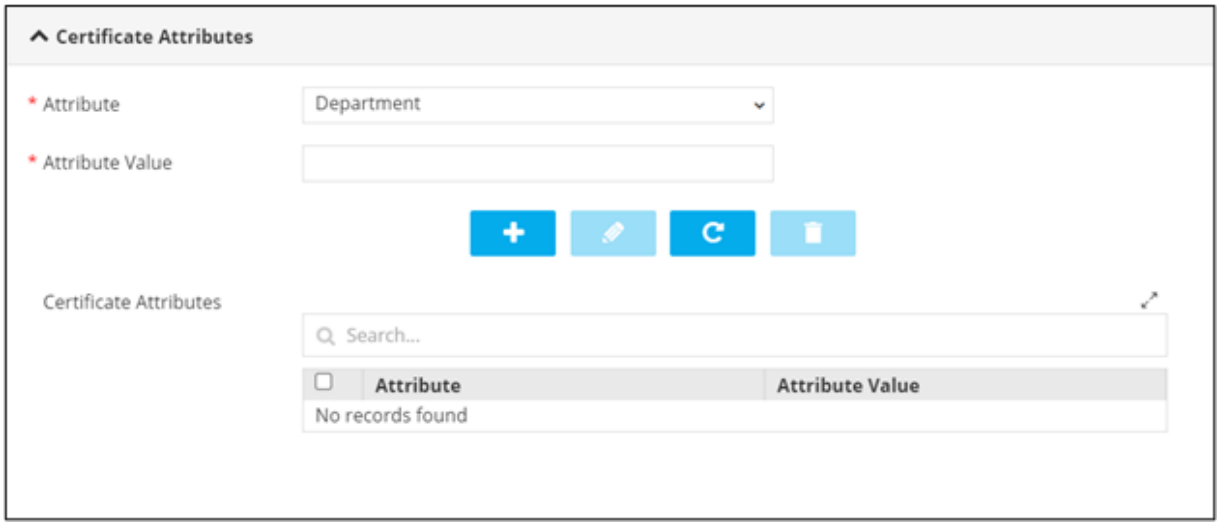
Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

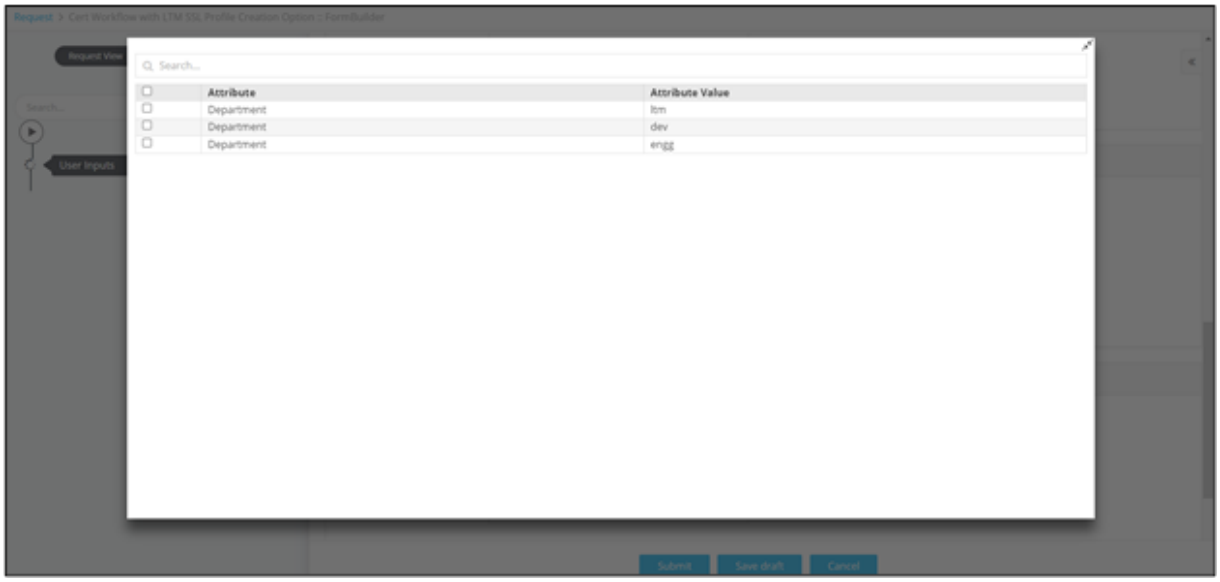
1. Under the **CSR Parameters** section, to **Upload CSR**, click .
2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

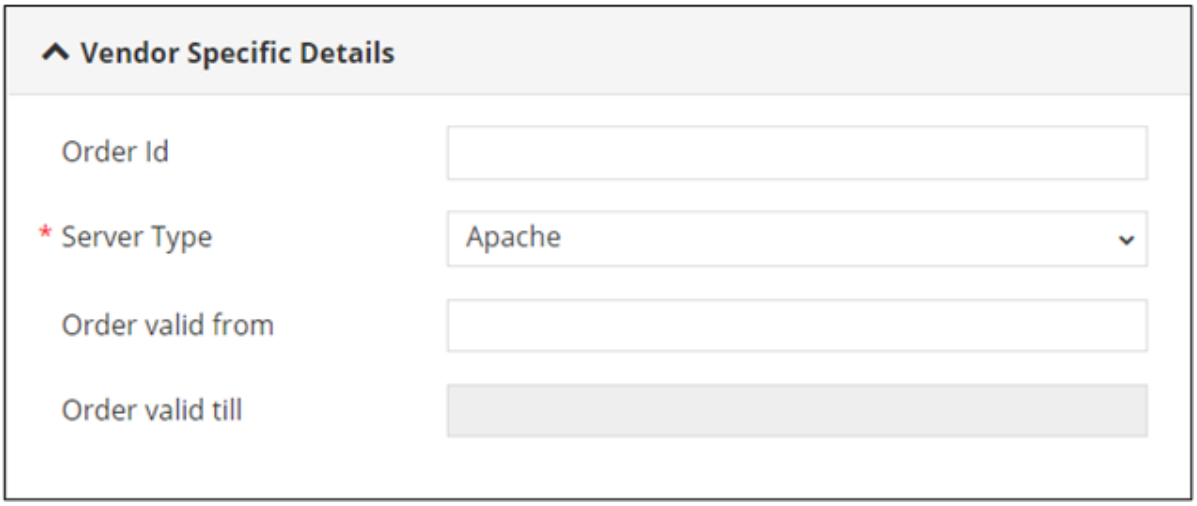
3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



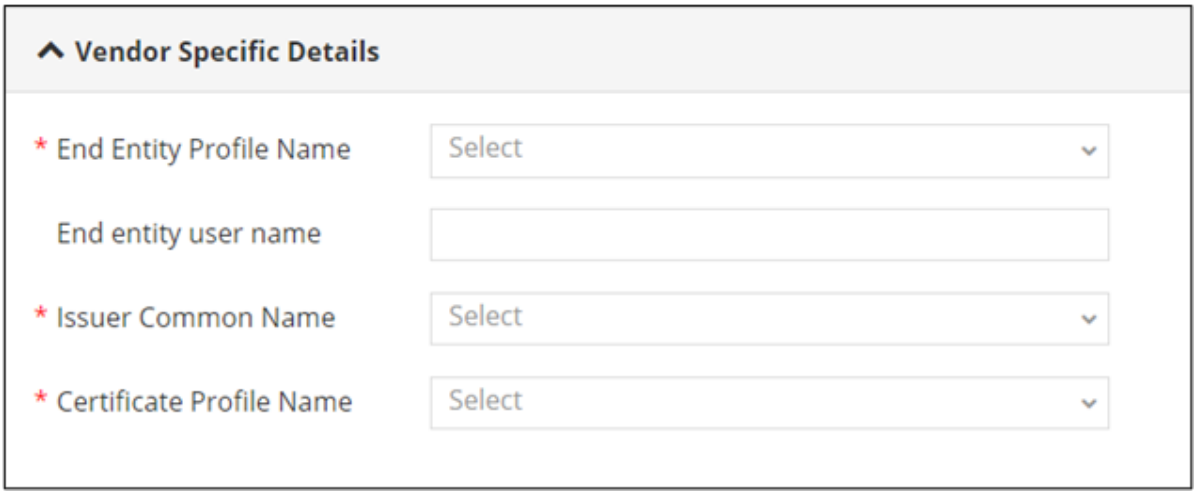
5. To add this attribute to the **Certificate Attributes** grid, click  .
6. To edit the value of a particular attribute, select the attribute in the grid and click  .
7. Enter the new value for the attribute in the **Value** field and click  again to update the value.
8. To delete a certificate attribute, select the attribute in the grid and click  .
9. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



10. To search for a particular attribute in the grid, type the keyword(s) in the search field.
11. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.



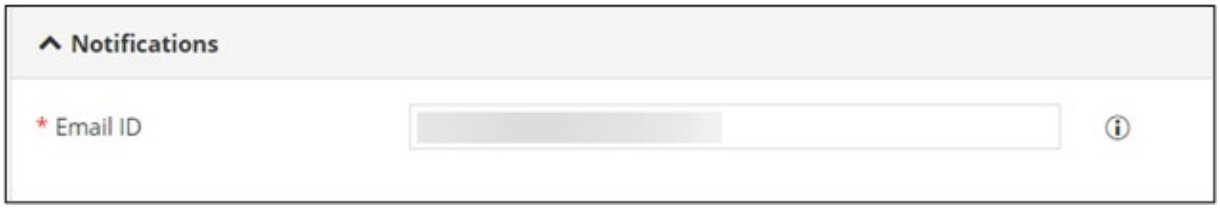
• When EJBCA is selected as CA.



• When Microsoft Enterprise is selected as CA.

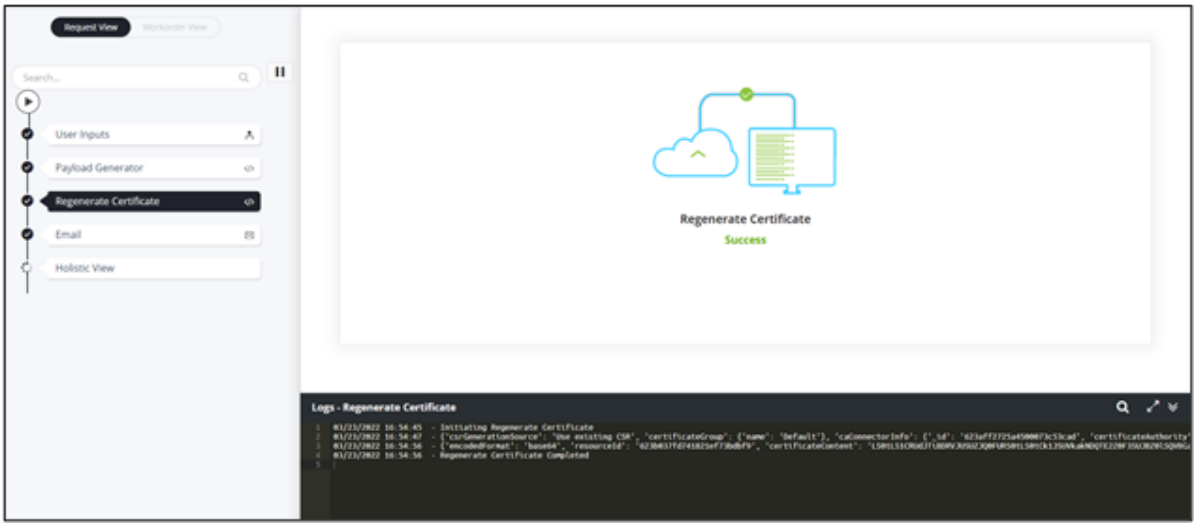
Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

12. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

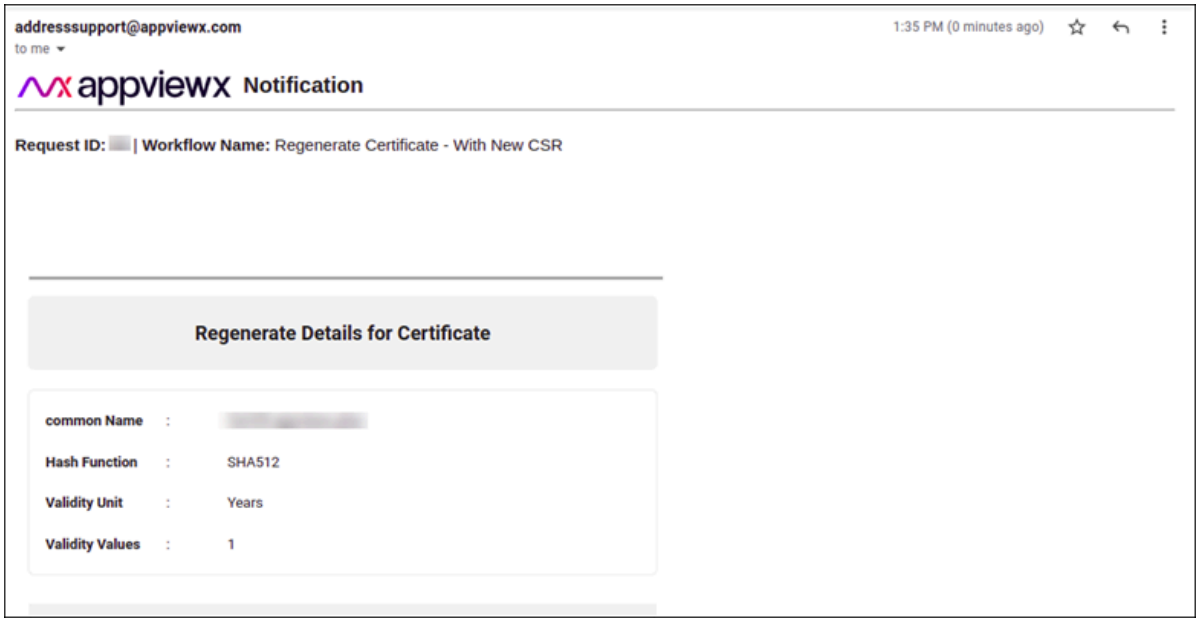


Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

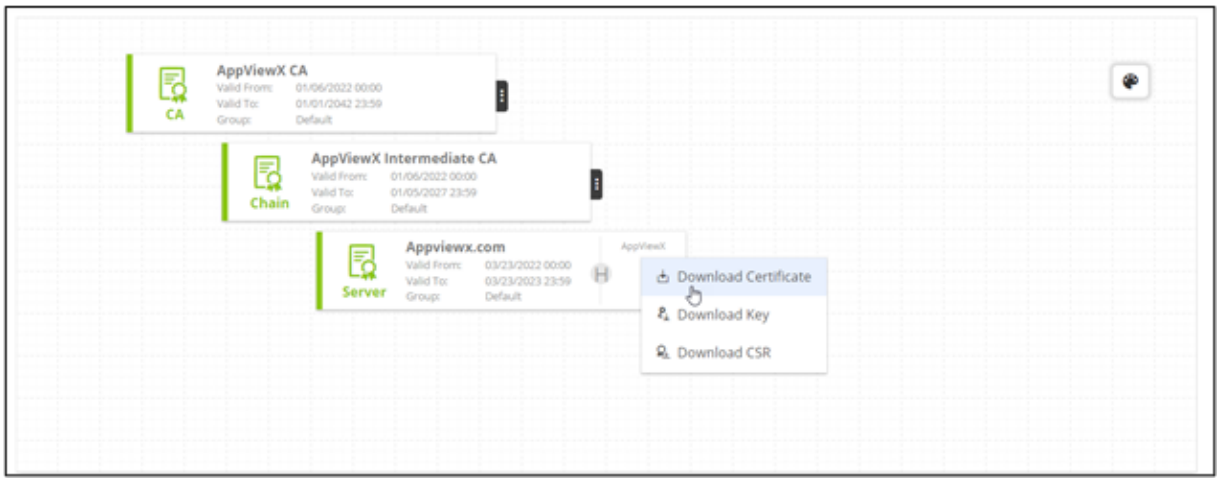
13. Click **Submit**.
    - Certificate regenerated successfully.



    - Email notification received.



14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



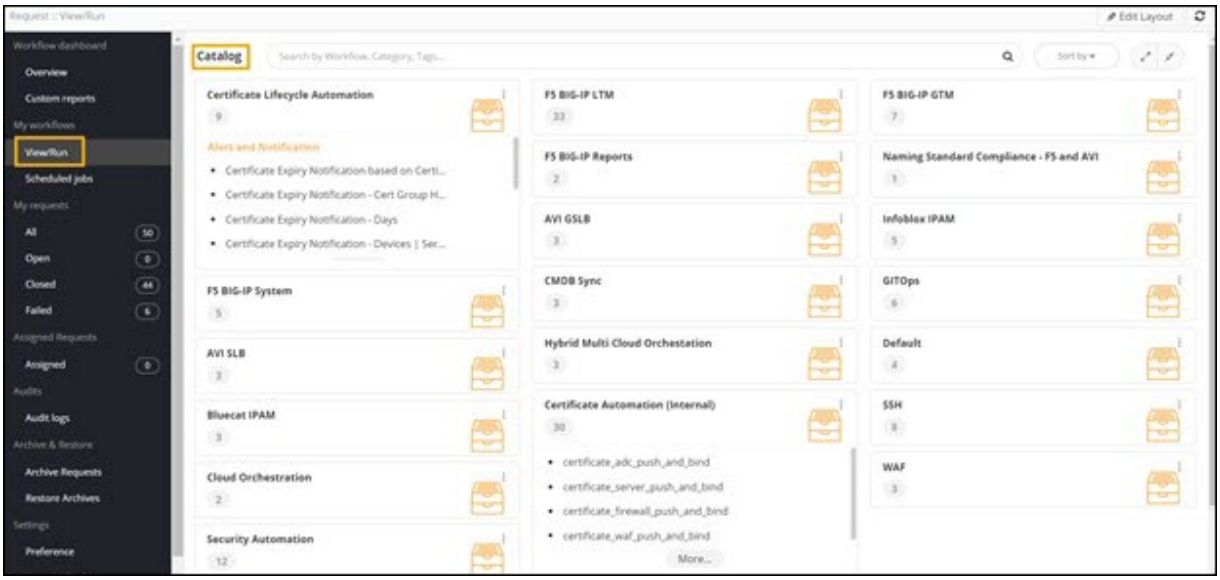
15. Hover your mouse over  to view the **Certificate status**.

Renew Certificate and Push

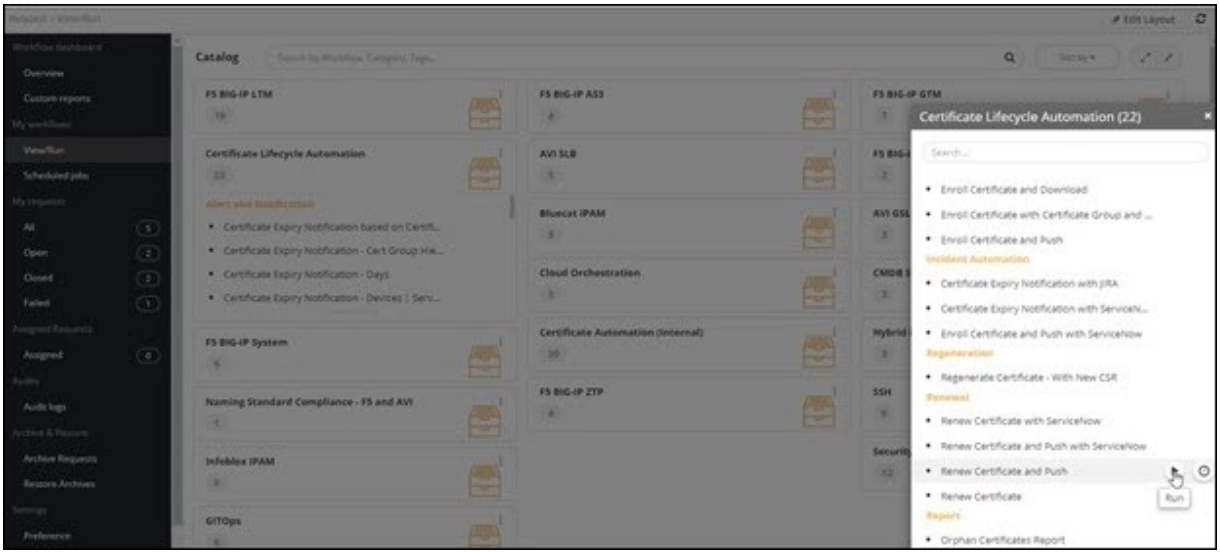
This workflow allows you to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

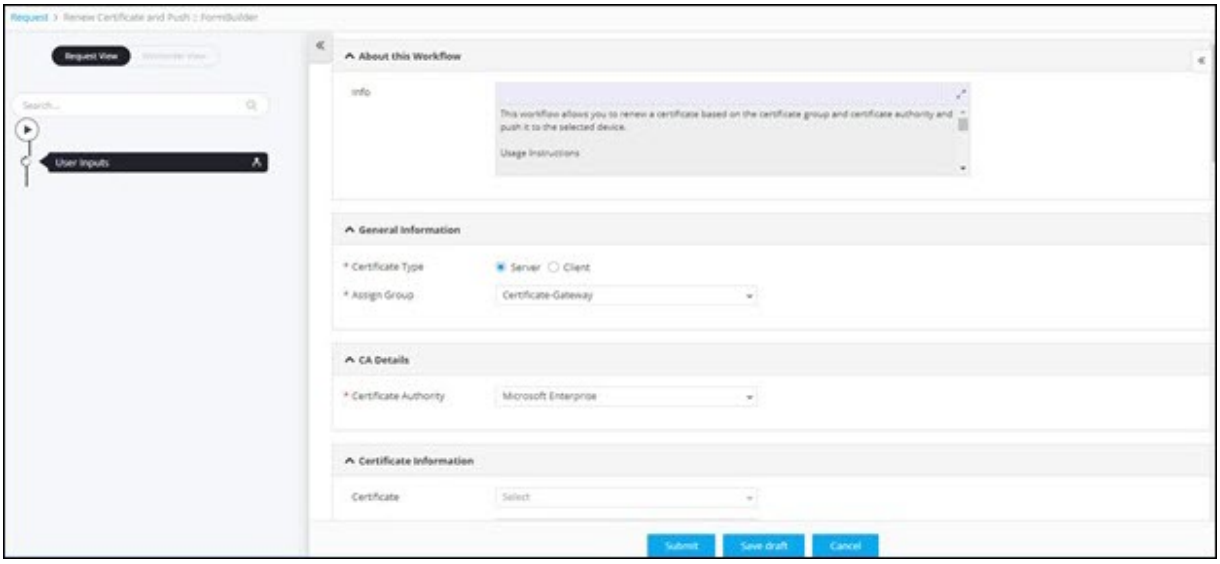


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push** workflow and click .

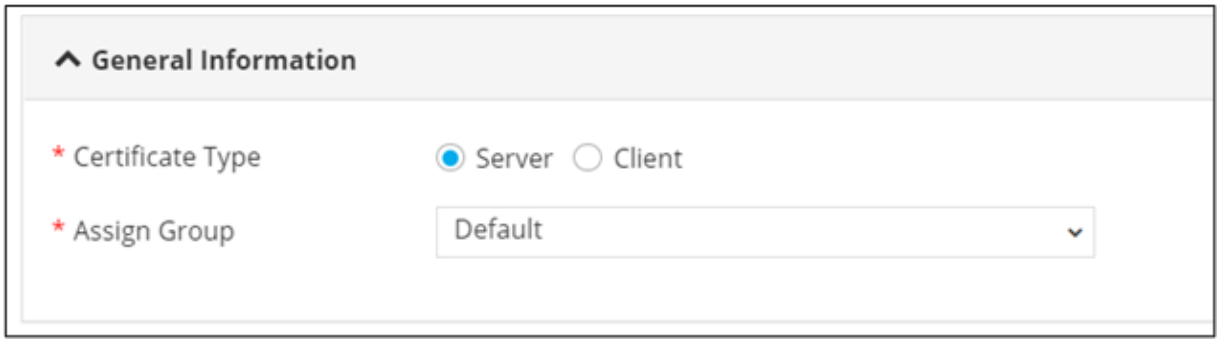


Tip: You can also search for the workflow by typing the workflow name in the search bar.

The workflow execution page is displayed with the workflow inputs requested at the first stage.



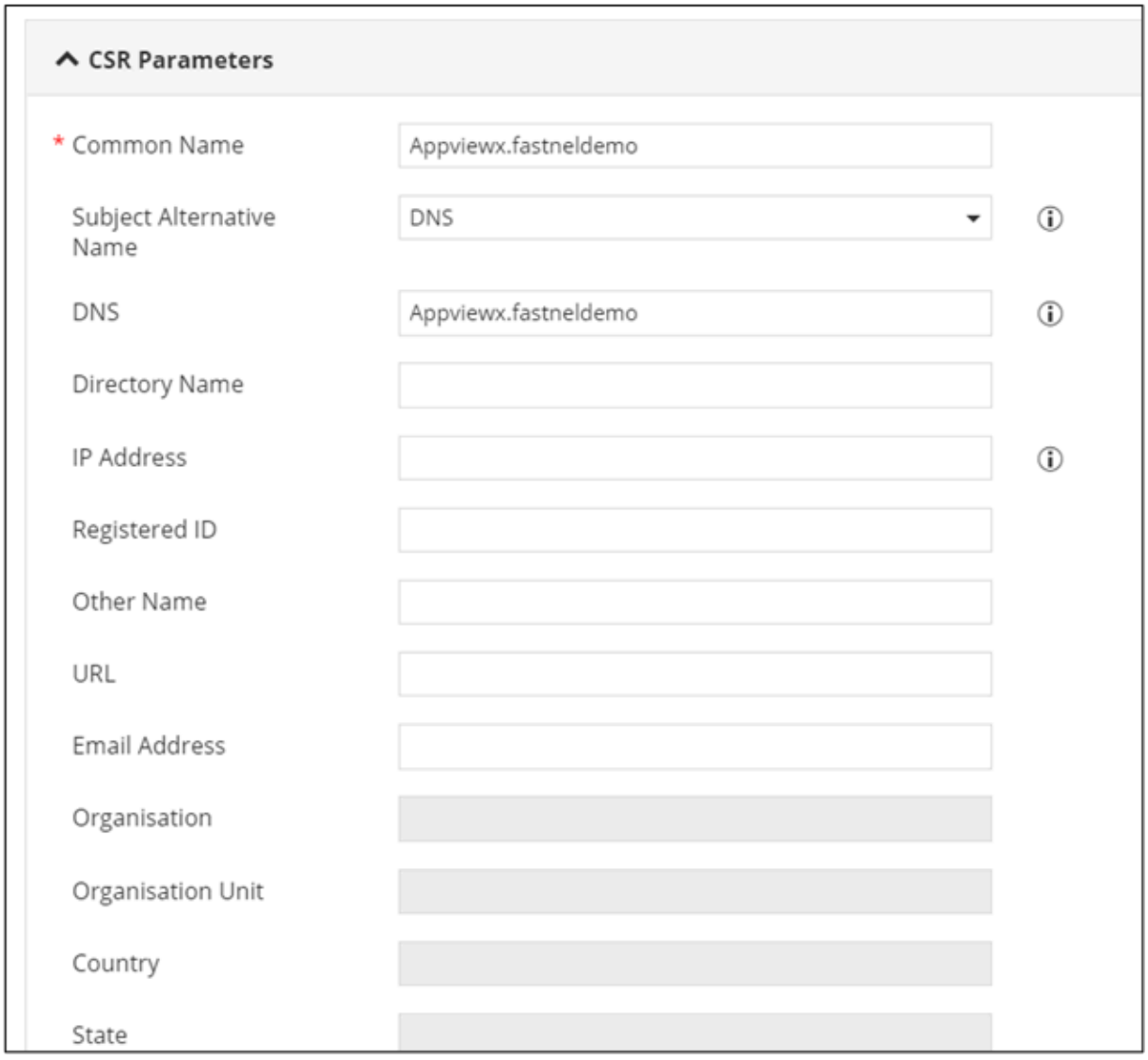
5. Under the **General Information** section, select the **Certificate Type** (mandatory).
6. Under the **General Information** section, select the **Assign Group** (mandatory).

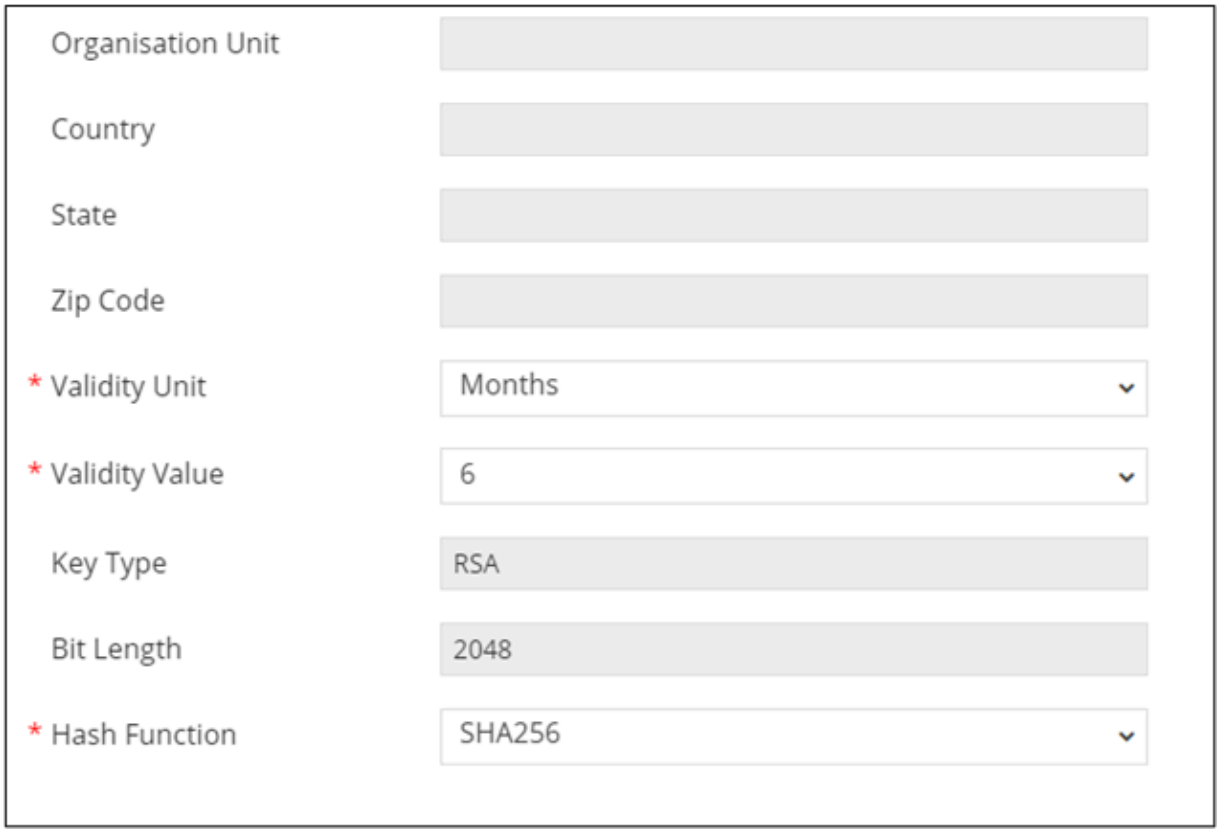


7. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
8. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory).

   The **Serial Number** and **CA Account** fields are populated based on the Certificate selected.

9. Under the **CSR Parameters** section**,** enter or select the field information as shown.





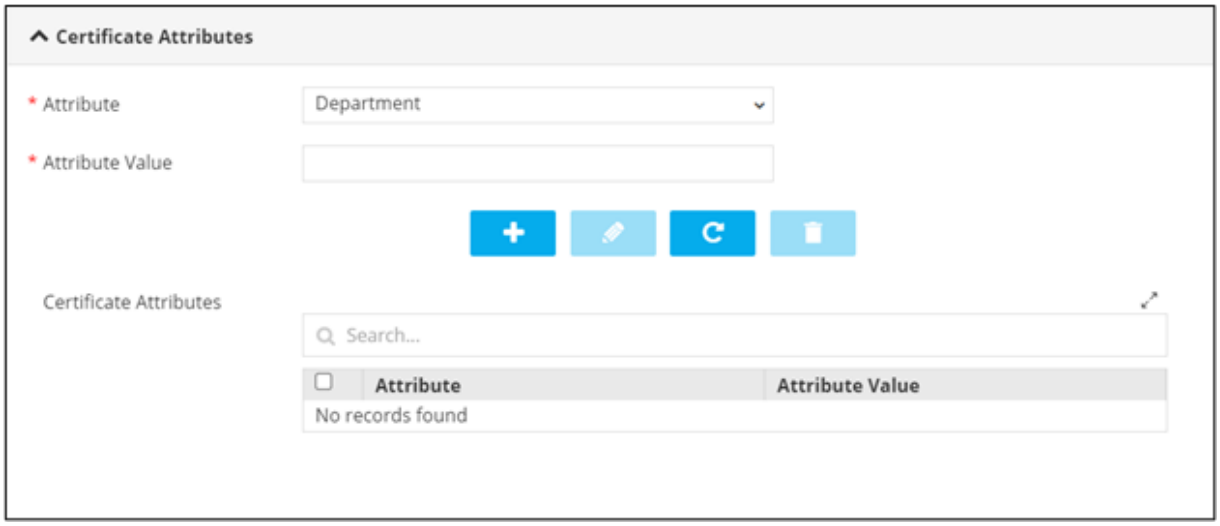
The following table describes the fields in the **CSR Parameters** section:

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name**

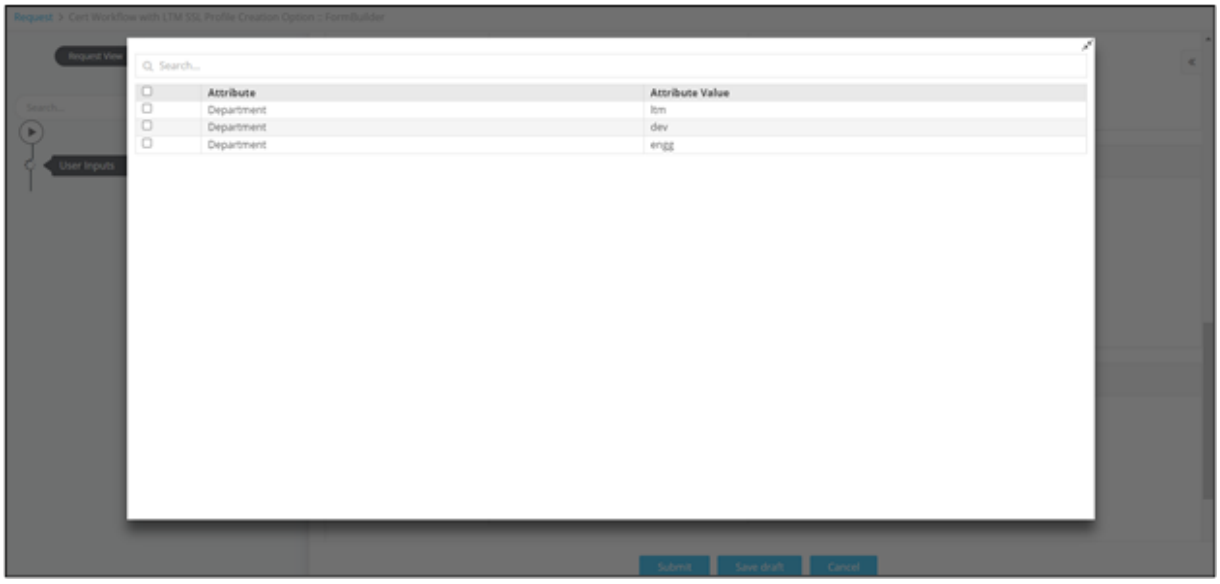
Field	Description
	• **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email Address	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Country	Enter the name of the country in which the organization is located.
State	Enter the name of the state in which the organization is located.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***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.  **Note:** This field will be populated based on the selected **Key Type**.

Field	Description
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

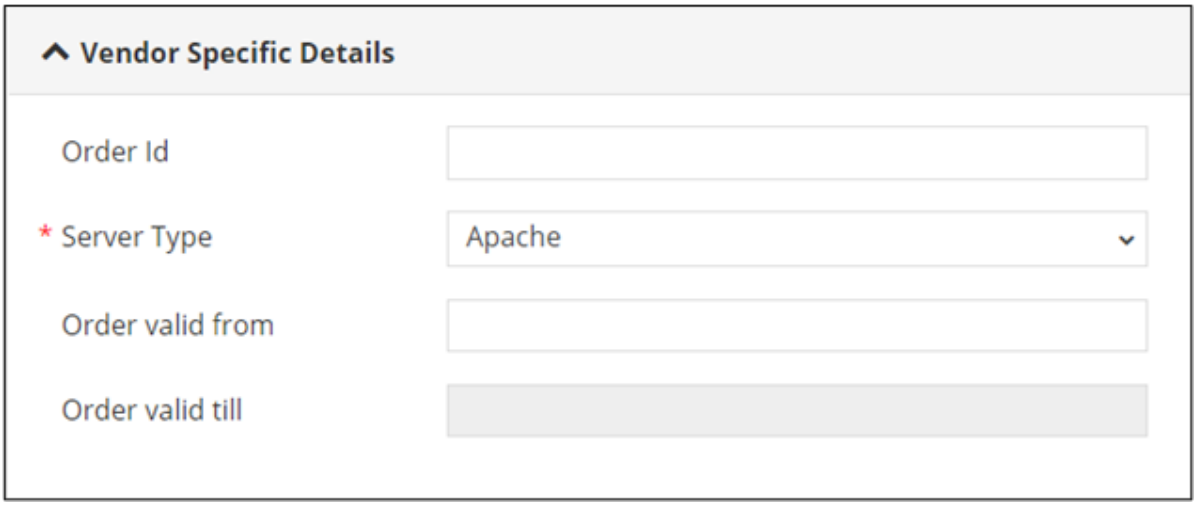
10. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
11. Enter a value for the selected attribute.



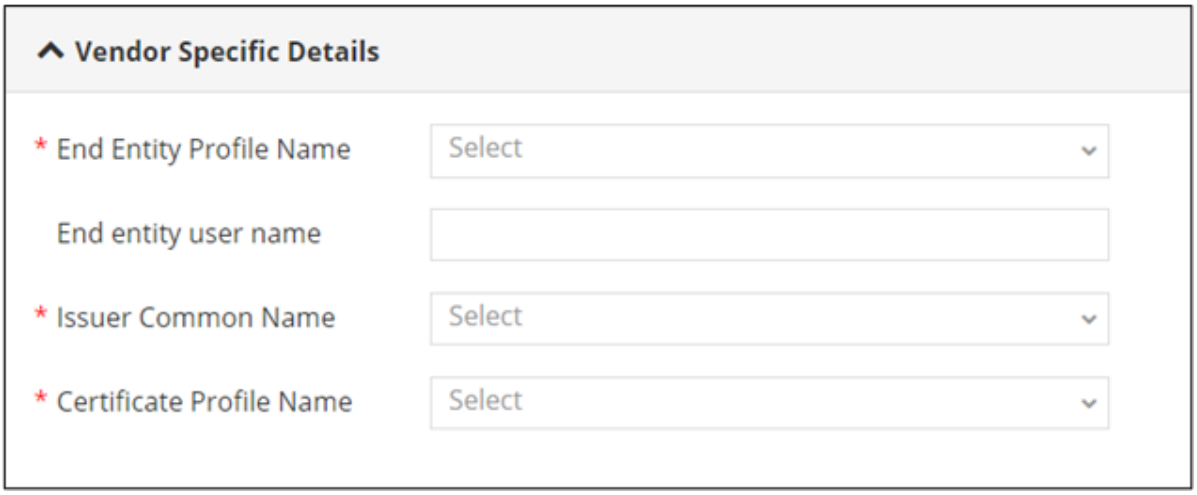
12. To add this attribute to the **Certificate Attributes** grid, click  .
13. To edit the value of a particular attribute, select the attribute in the grid and click  .
14. Enter the new value for the attribute in the **Value** field and click  again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click  .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



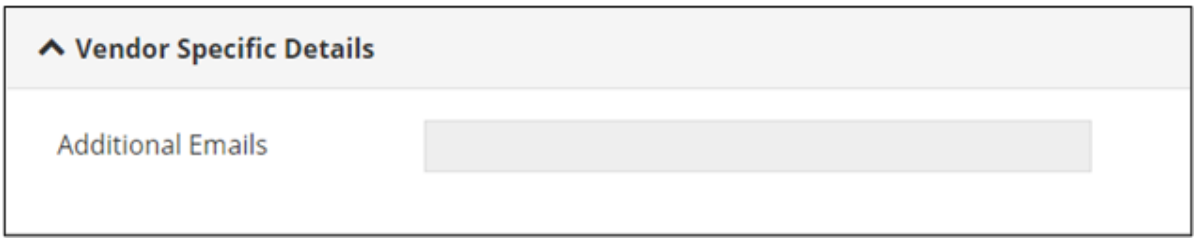
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
    - When Digicert is selected as CA.



    - When EJBCA is selected as CA.

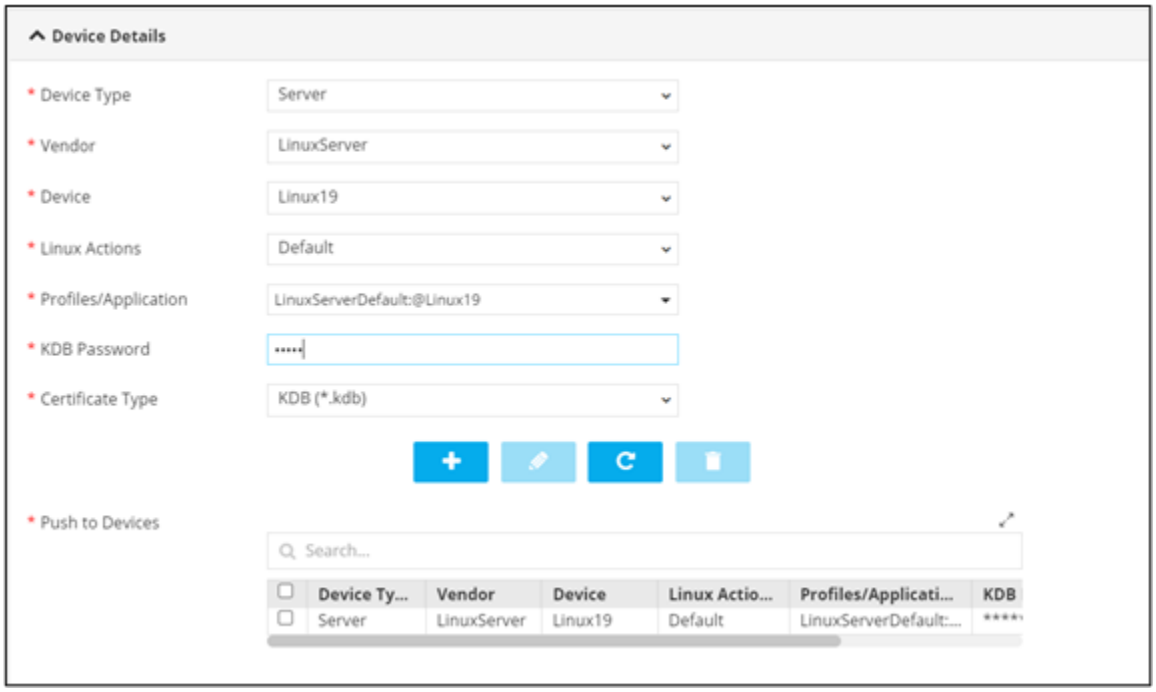


- When Entrust is selected as CA.



Note: The Vendor Specific Details section is displayed only when DigiCert, EJBCA, or Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

19. Under the **Device Details** section, select the field information as shown.



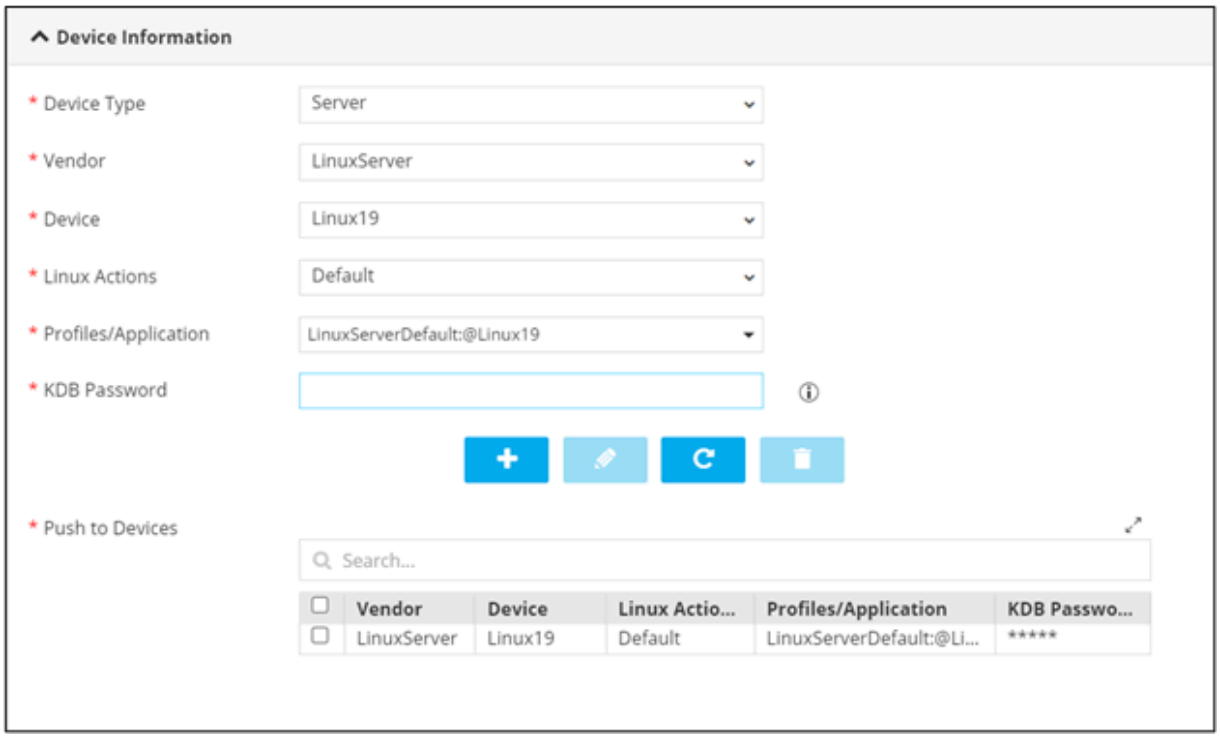
The following table describes the field information in the **Device Details** section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown.

Field	Description
	Note: The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

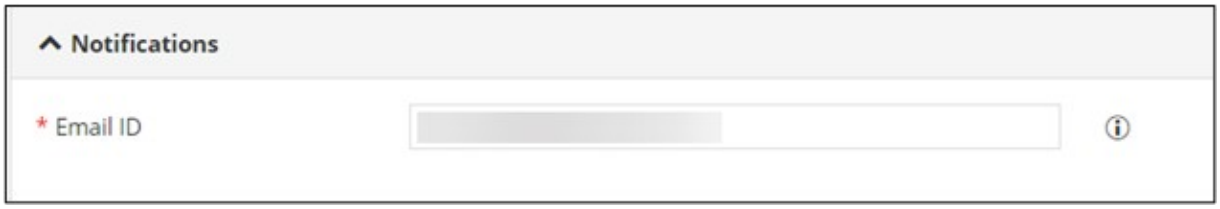
20. To add the selected profile/application to the grid, click +.

    The **Profile/Application** is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

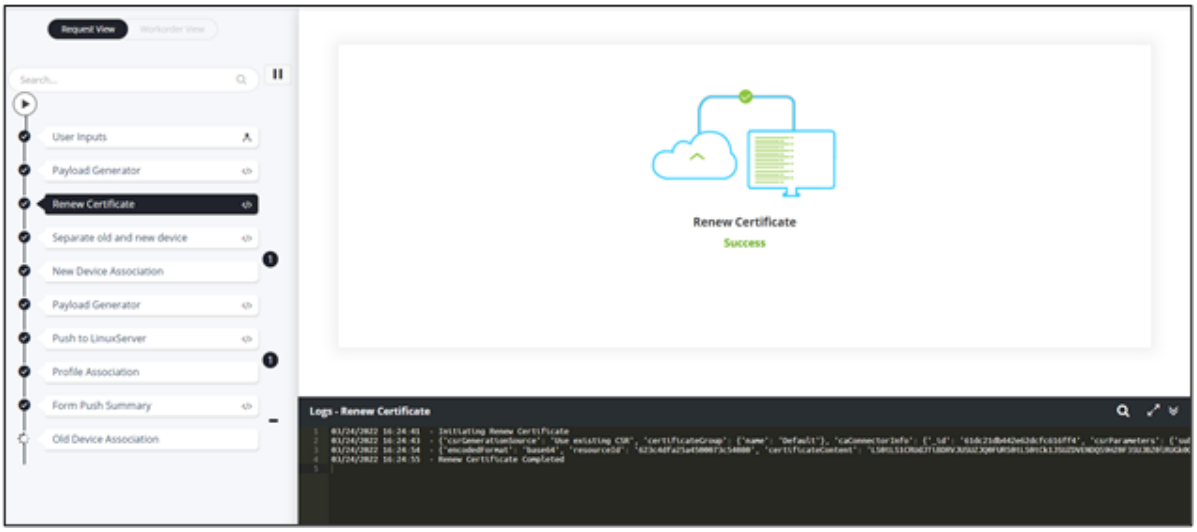
21. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
22. Select a new device and click again to update the value.
23. To delete a profile/application, select the row to be deleted in the grid and click .
24. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
25. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
26. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



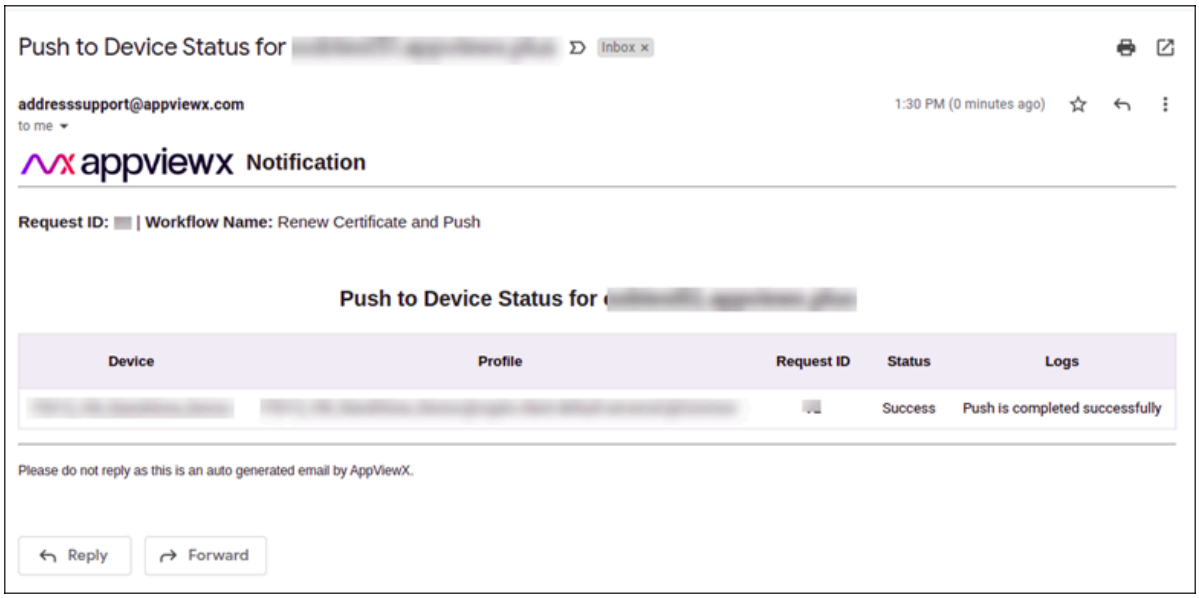
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

27. Click **Submit**.

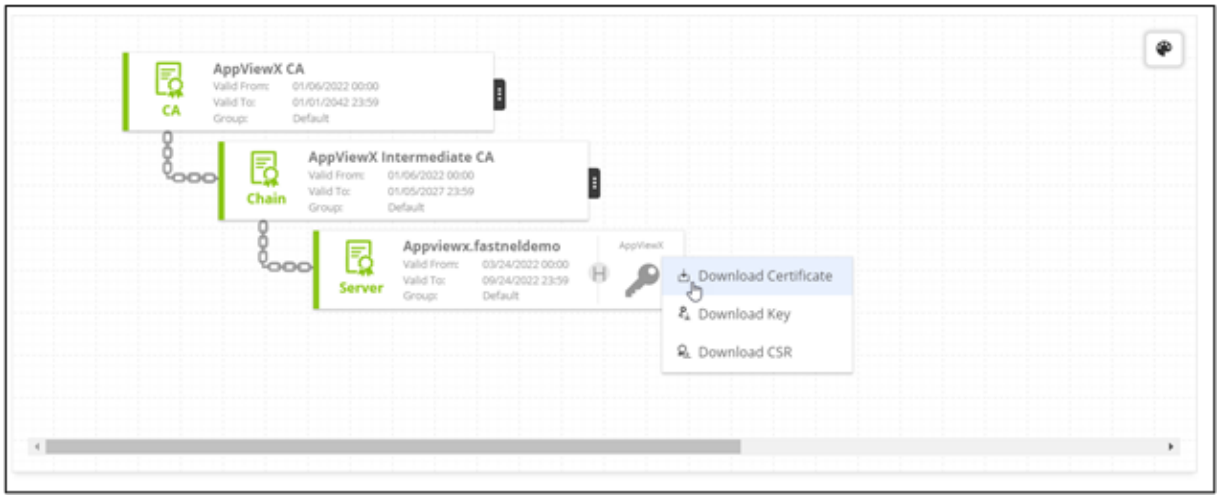
• Certificate renewed successfully.



• Email notification received.



28. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



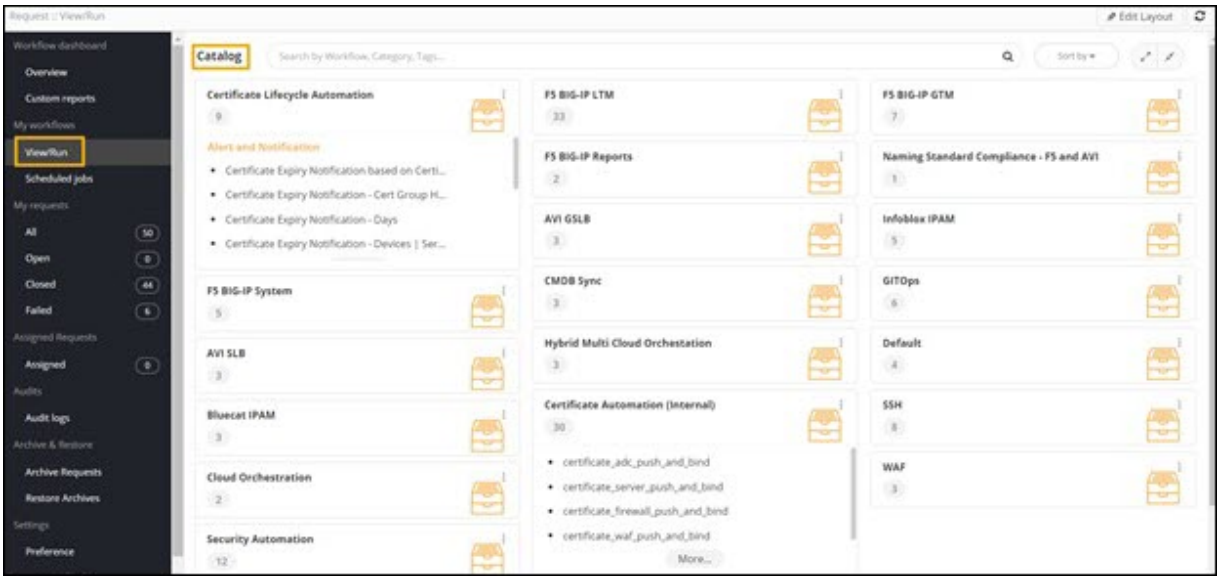
29. Hover your mouse over  to view the **Certificate status**.

Renew Certificate with ServiceNow

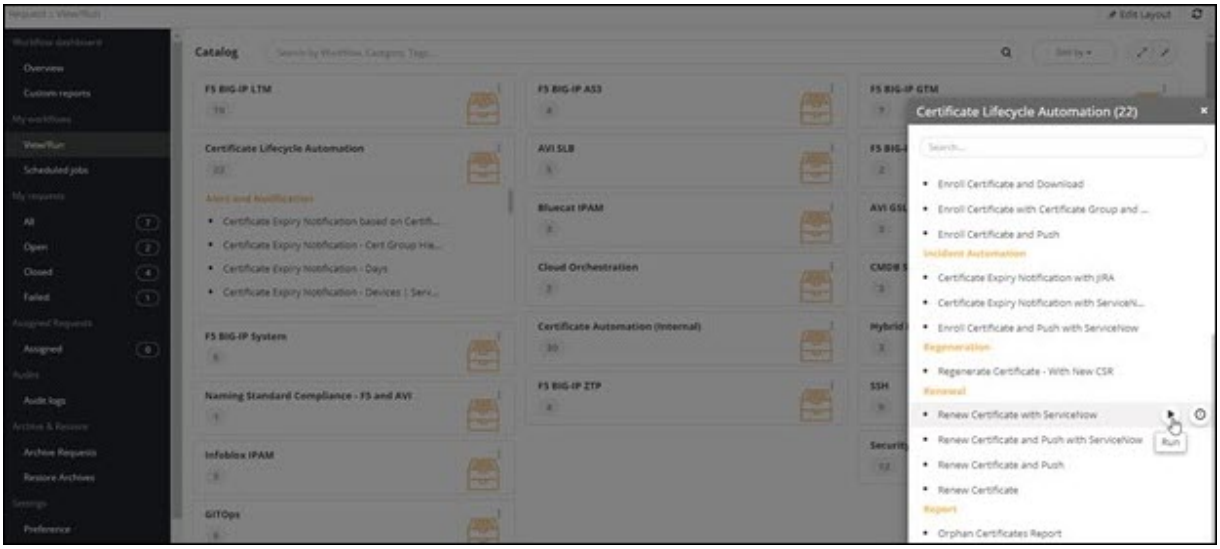
This workflow allows you to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

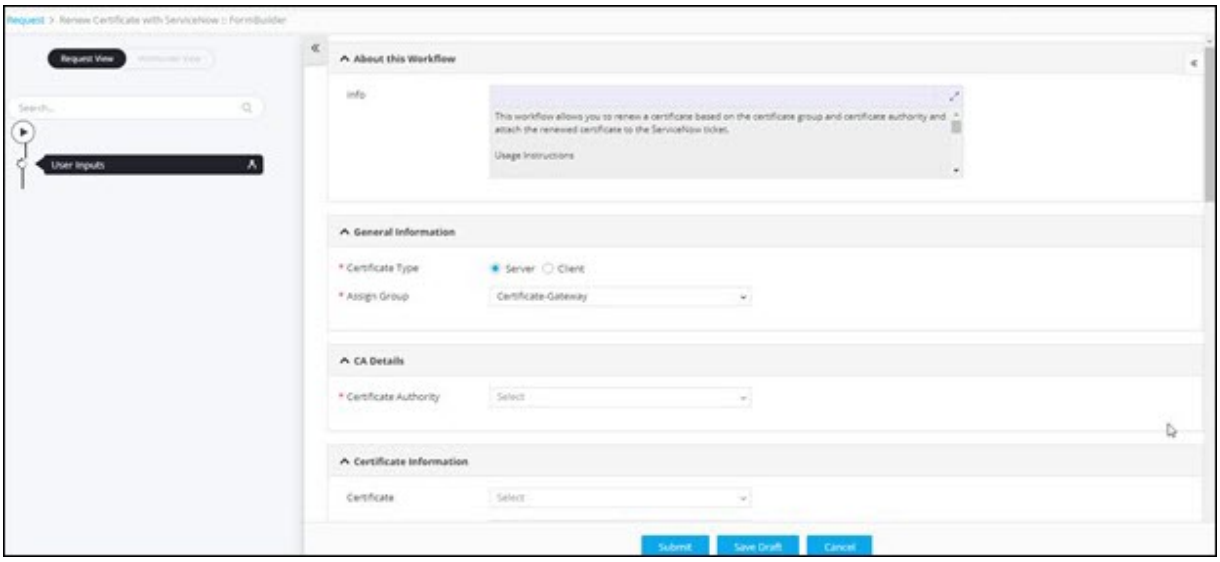


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate with ServiceNow** workflow and click .

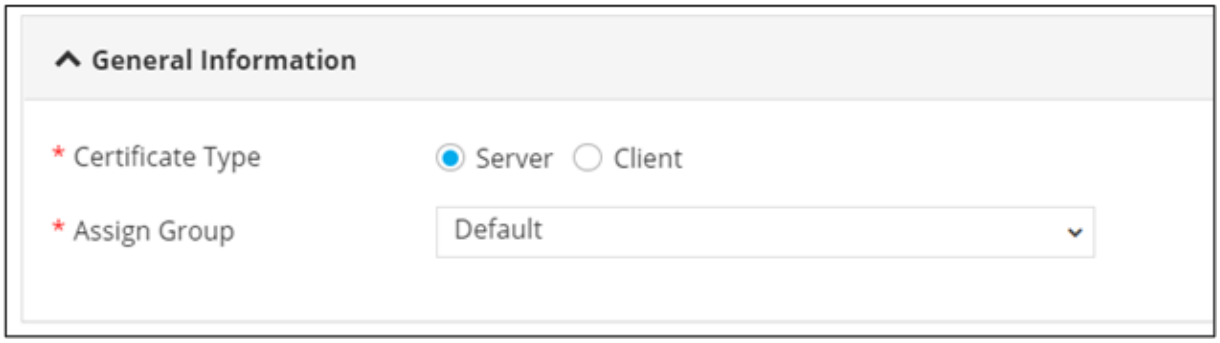


Tip: You can also search for the workflow by typing the workflow name in the search bar.

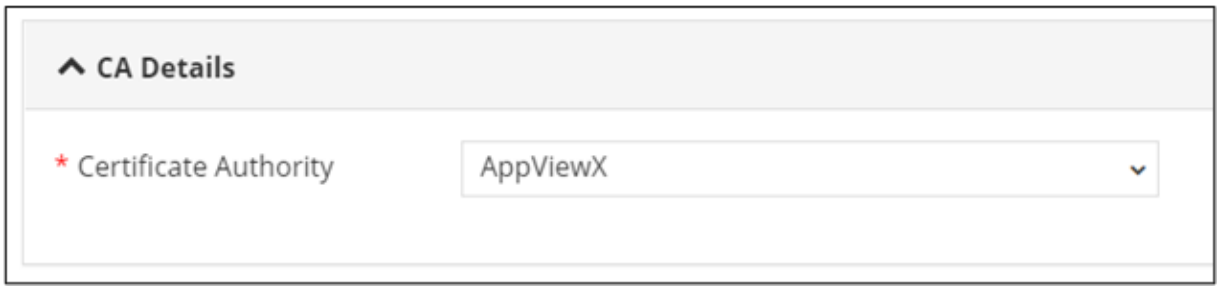
The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **General Information** section, select the **Certificate Type** (mandatory).
6. Under the **General Information** section, select the **Assign Group** (mandatory).

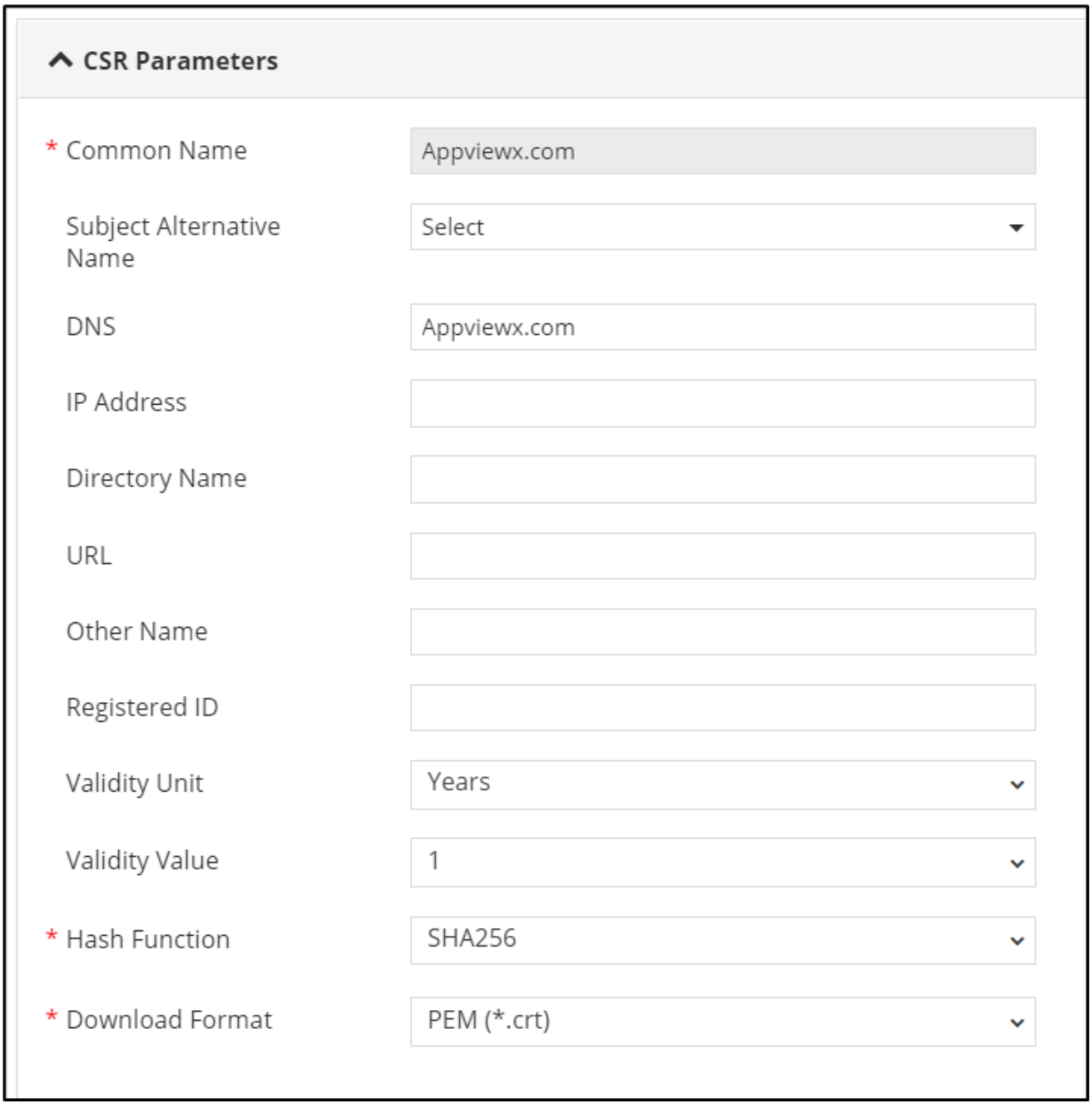


7. Under the **CA Details** section, select the **Certificate Authority** (mandatory).



8. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.

9. Under the **CSR Parameters** section**,** enter or select the field information as shown.

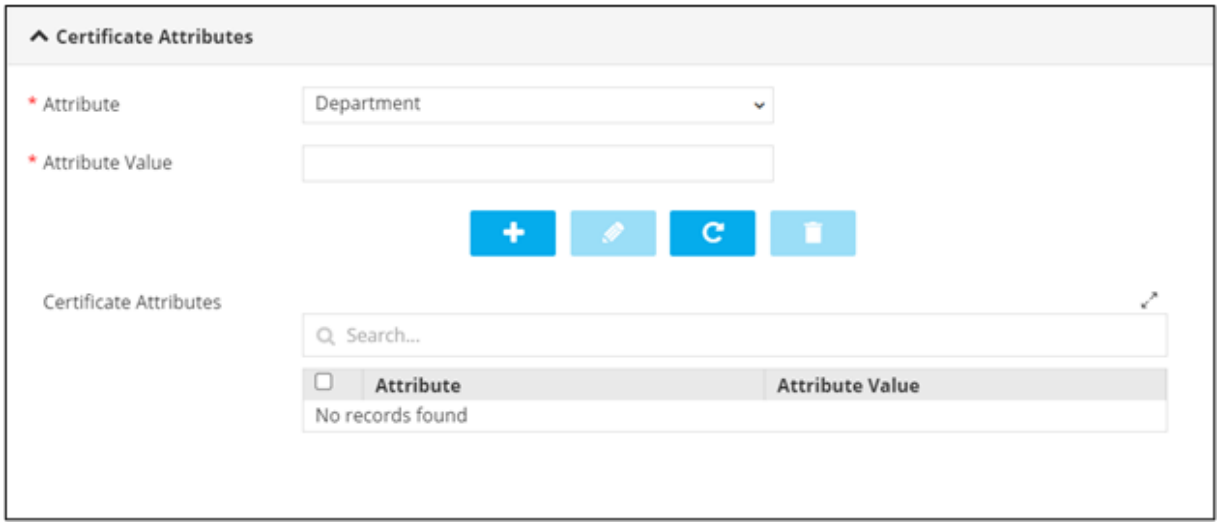


The following table describes the fields in the **CSR Parameters** section:

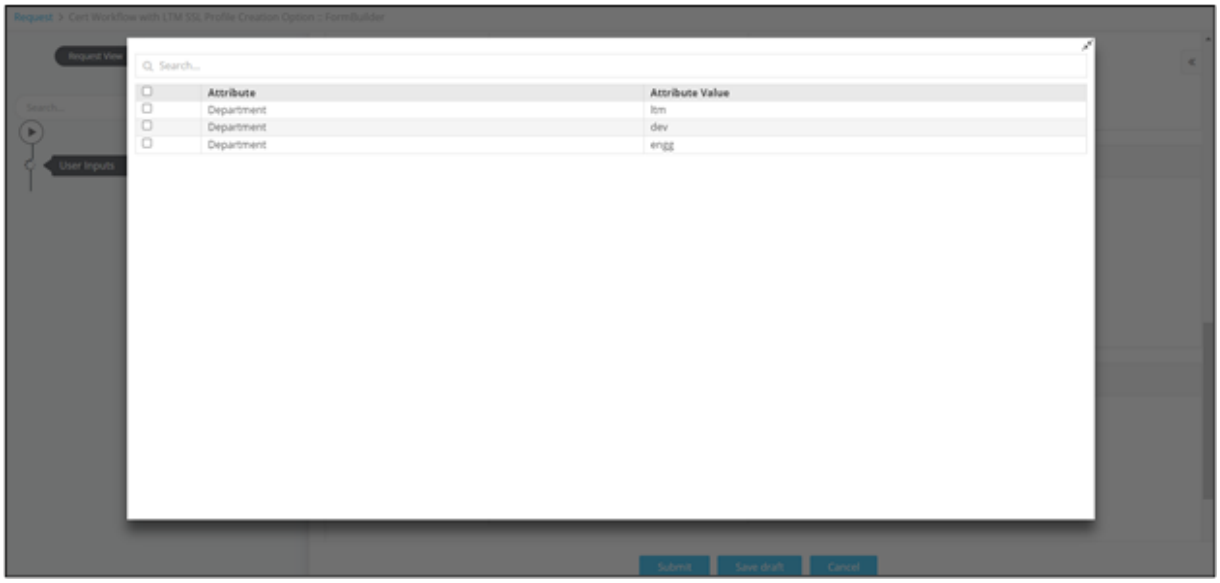
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID** • **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Validity Unit	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
Validity Value	Enter a **Validity Value** based on the selected validity unit.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.

Field	Description
***Download Format**	Select the format for downloading the certificate from the available options.
All asterisk (*) marked fields are mandatory.	

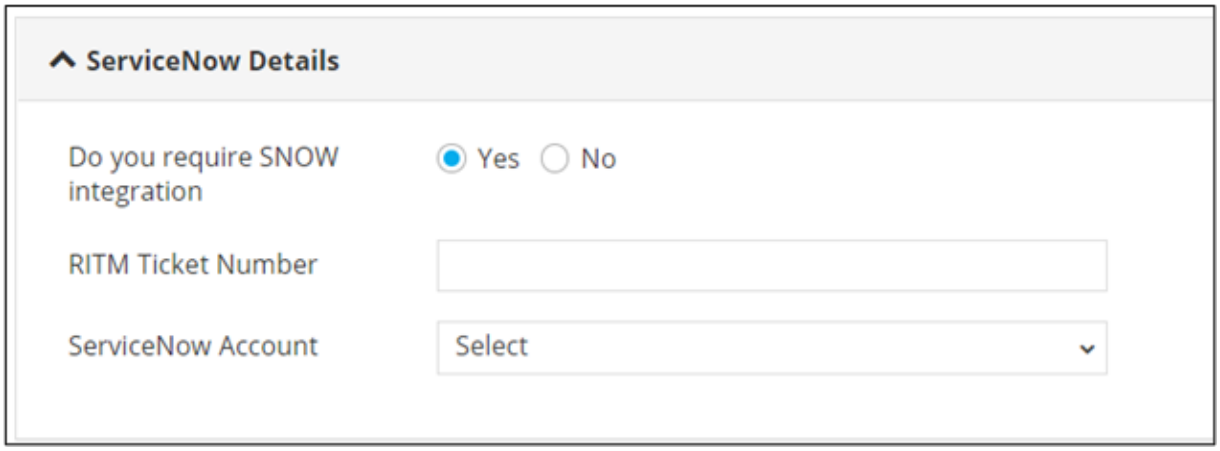
10. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
11. Enter a value for the selected attribute.



12. To add this attribute to the **Certificate Attributes** grid, click  .
13. To edit the value of a particular attribute, select the attribute in the grid and click  .
14. Enter the new value for the attribute in the **Value** field and click  again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click  .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Under the **ServiceNow Details** section, enter or select the required field information.

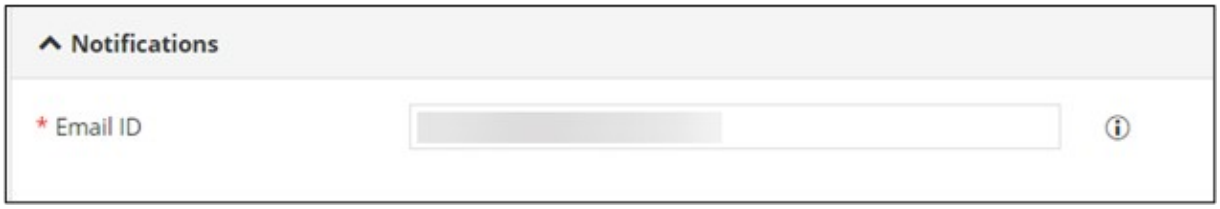


The following table describes the field information in the **ServiceNow Details** section:

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached.

Field	Description
	Note: This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

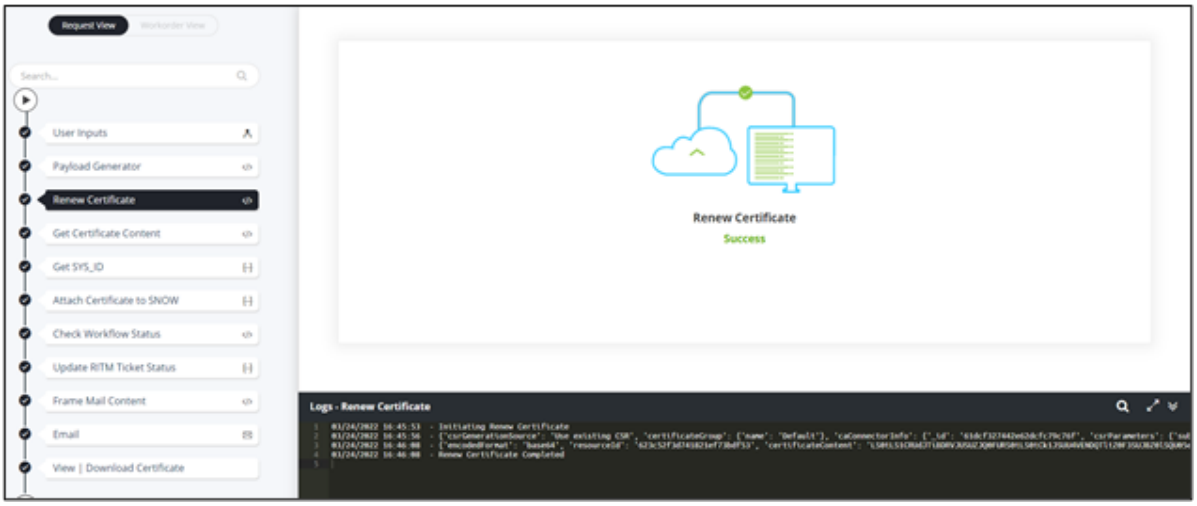
19. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



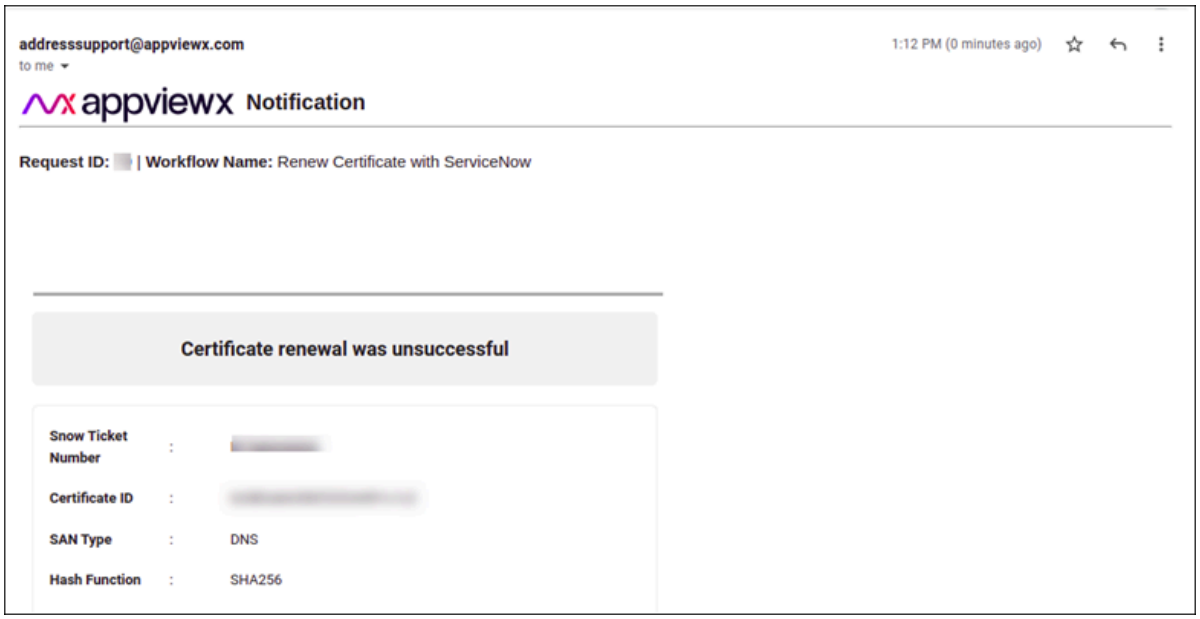
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

20. Click **Submit**.

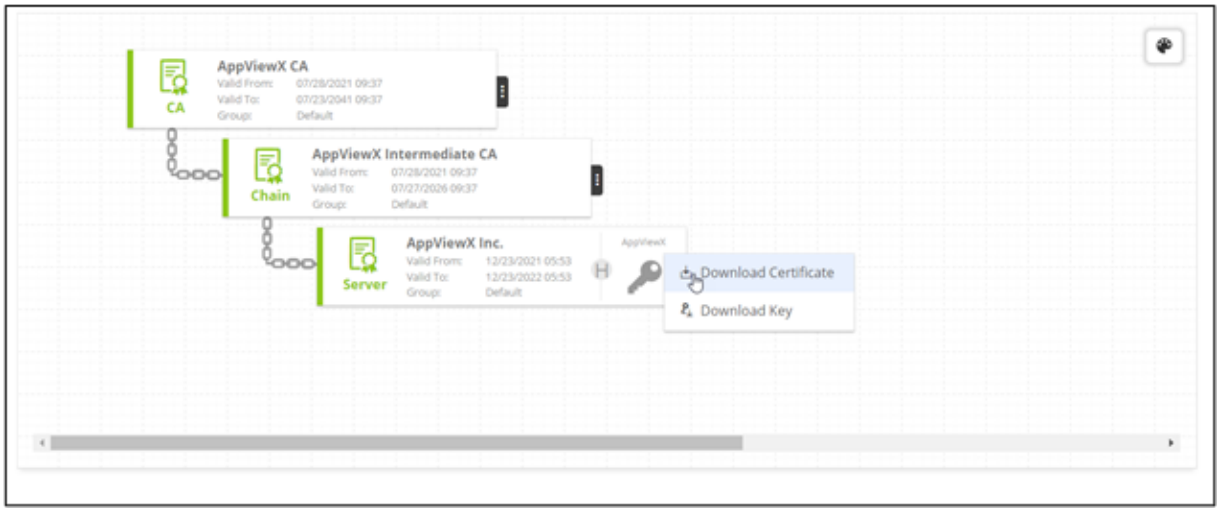
- Certificate renewed successfully.



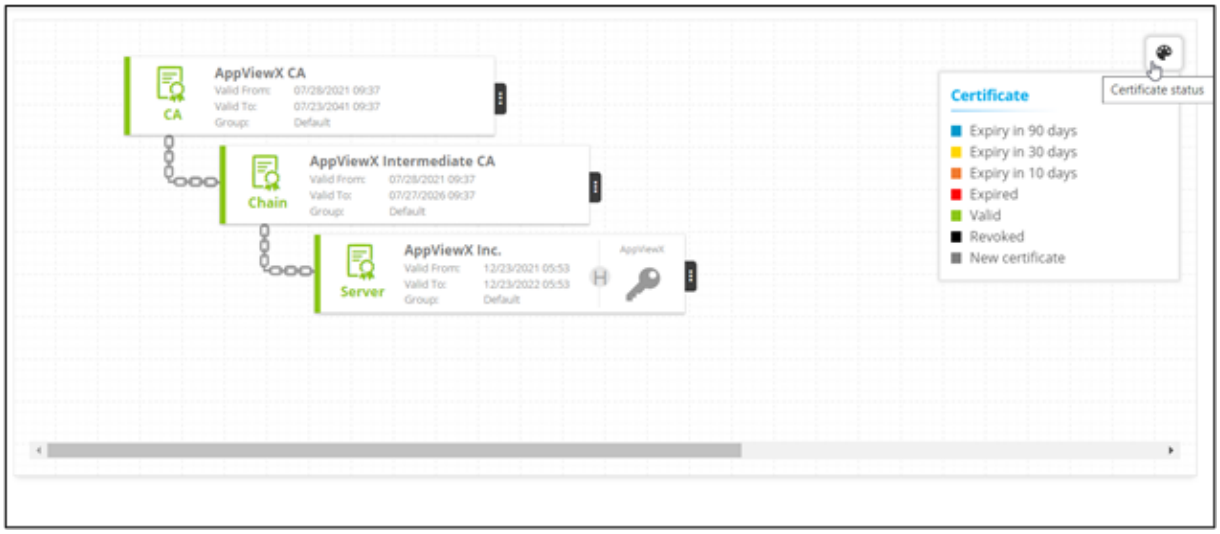
- Email notification received.



21. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



22. Hover your mouse over  to view the **Certificate status**.

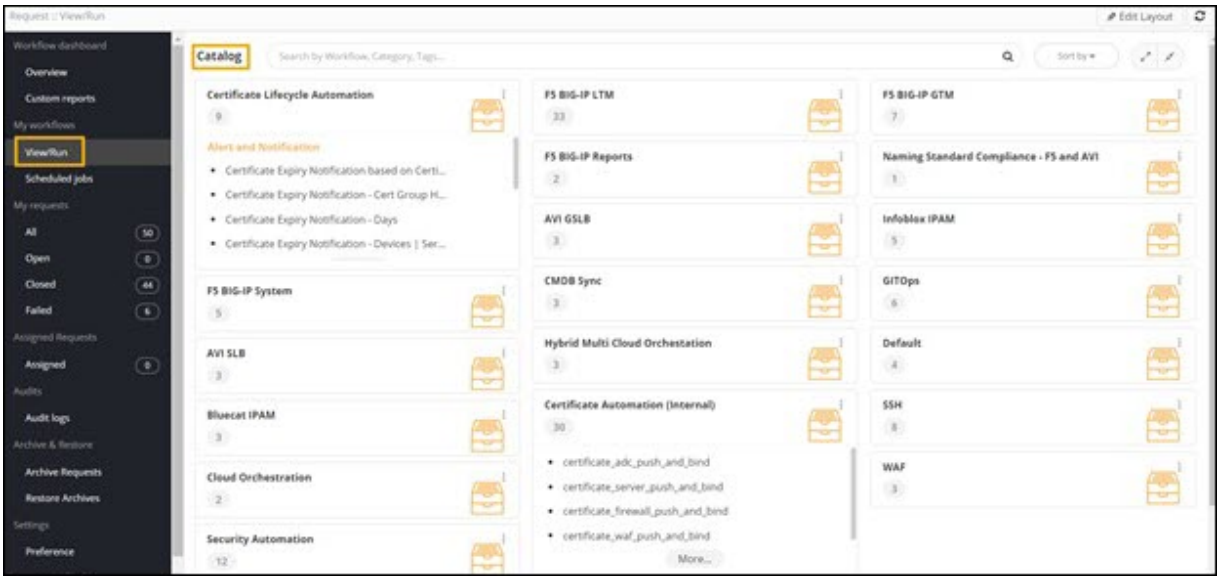


Renew Certificate and Push with ServiceNow

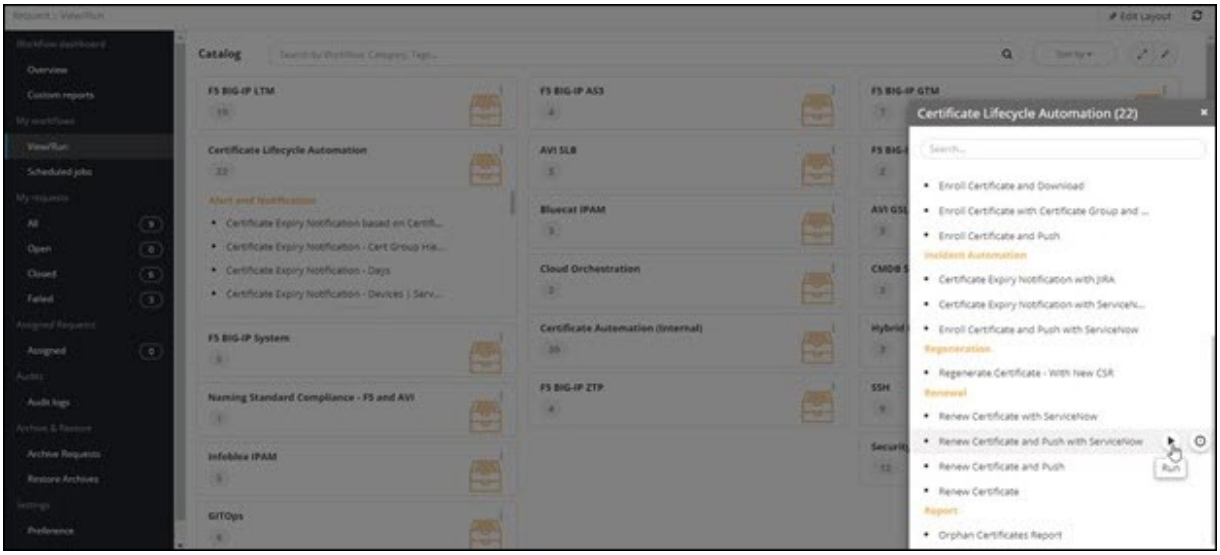
This workflow allows you to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.

To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.

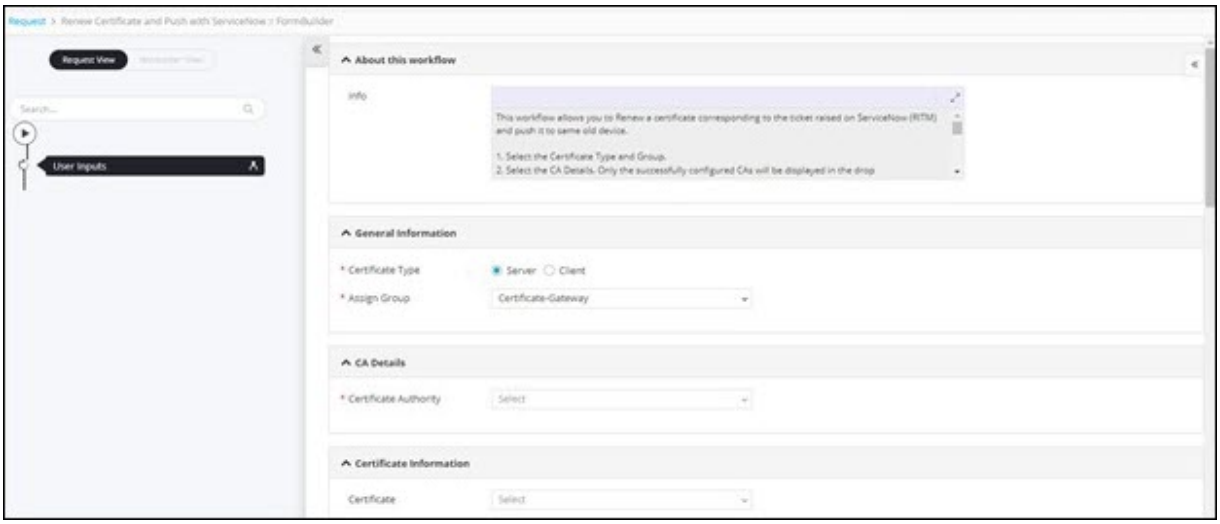


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push with ServiceNow** workflow and click .

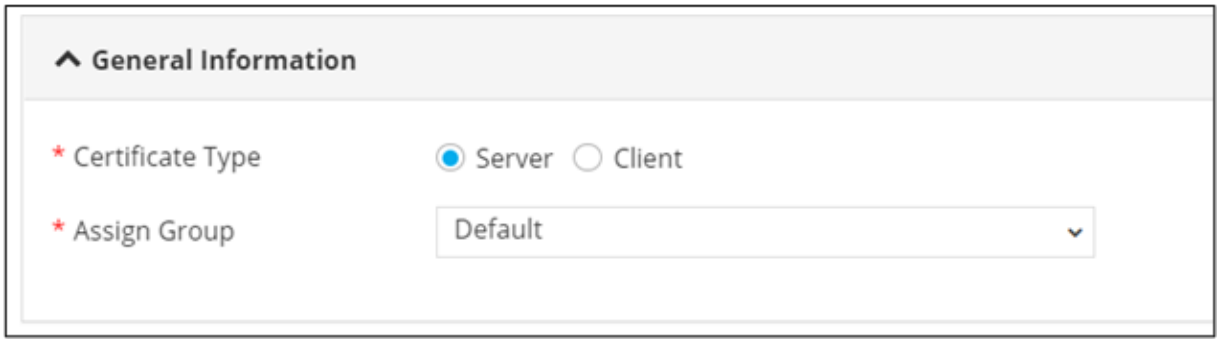


Tip: You can also search for the workflow by typing the workflow name in the search bar.

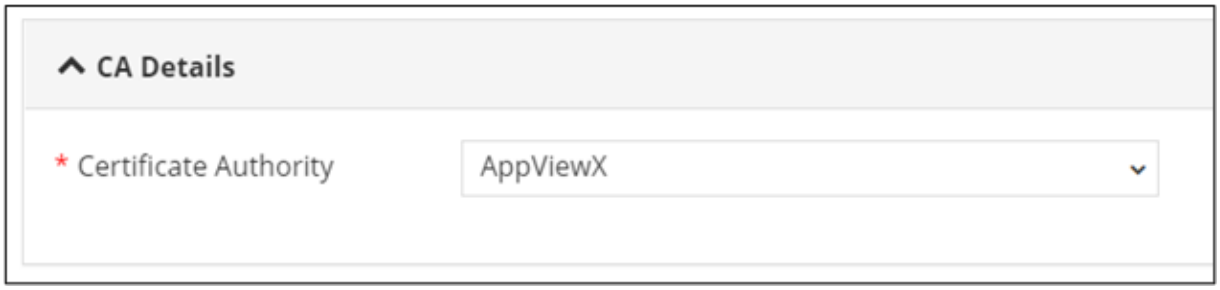
The workflow execution page is displayed with the workflow inputs requested at the first stage.



5. Under the **General Information** section, select the **Certificate Type** (mandatory).
6. Under the **General Information** section, select the **Assign Group** (mandatory).

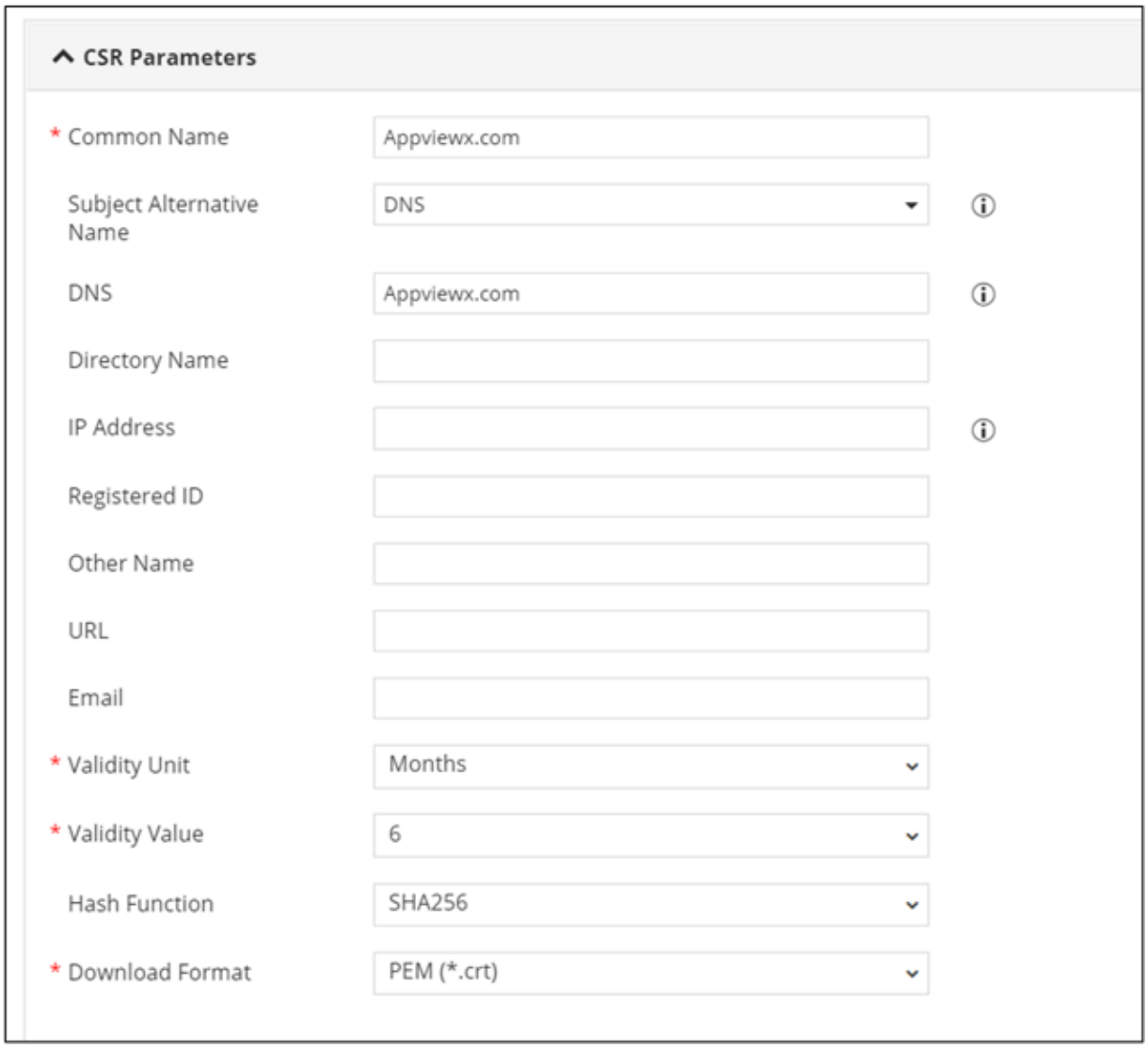


7. Under the **CA Details** section, select the **Certificate Authority** (mandatory).



8. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.

9. Under the **CSR Parameters** section**,** enter or select the field information as shown.

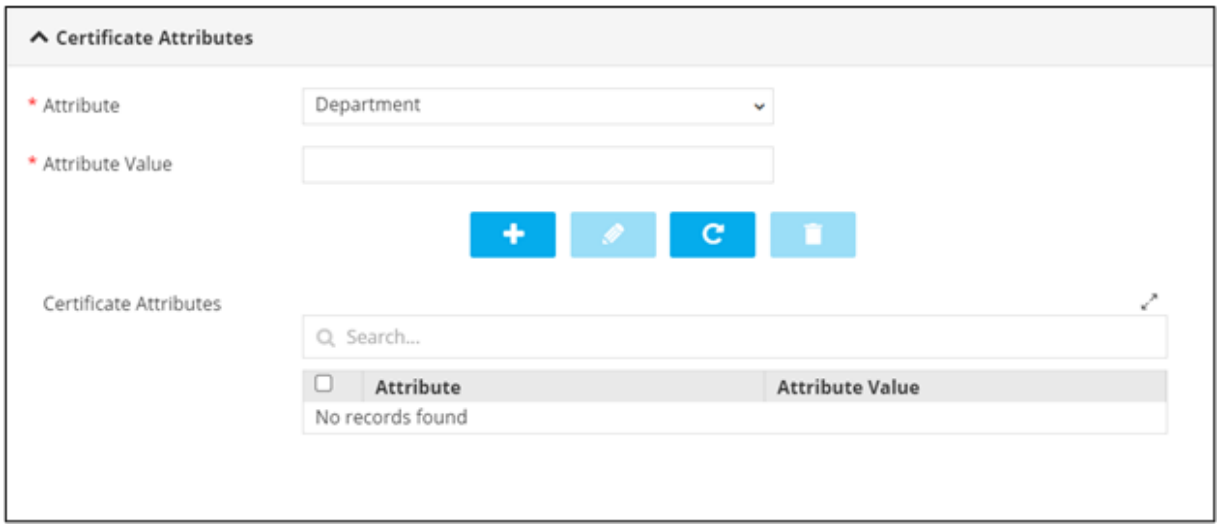


The following table describes the fields in the **CSR Parameters** section:

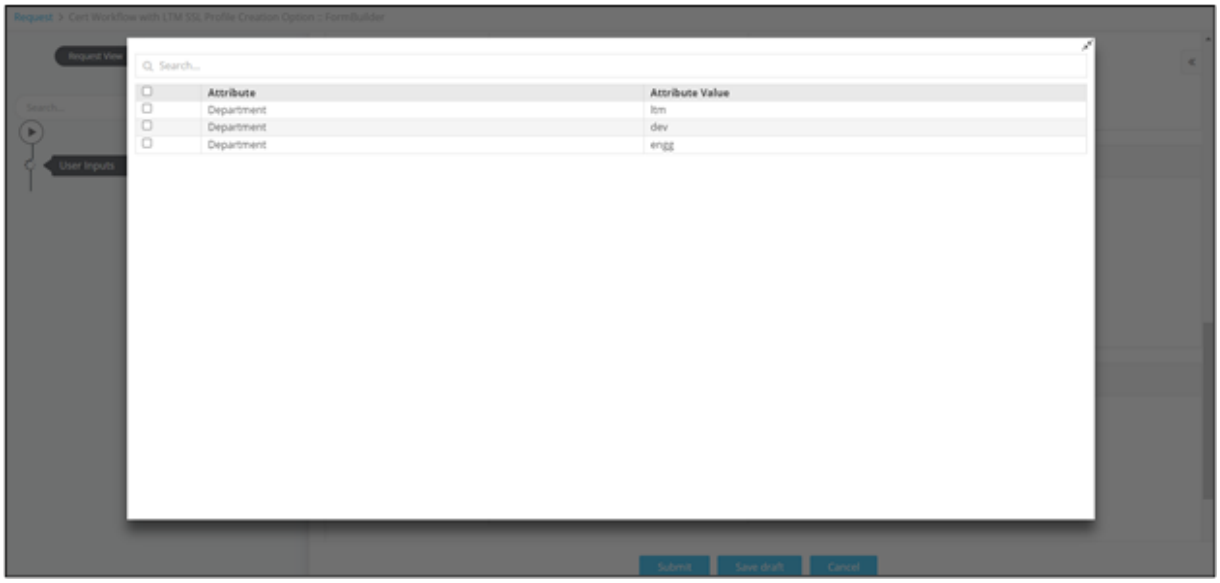
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID** • **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email	Enter a valid Email address if you select the **Email** option in the **SAN** field.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
***Download Format**	Select the format for downloading the certificate from the available options.

Field	Description
All asterisk (*) marked fields are mandatory.	

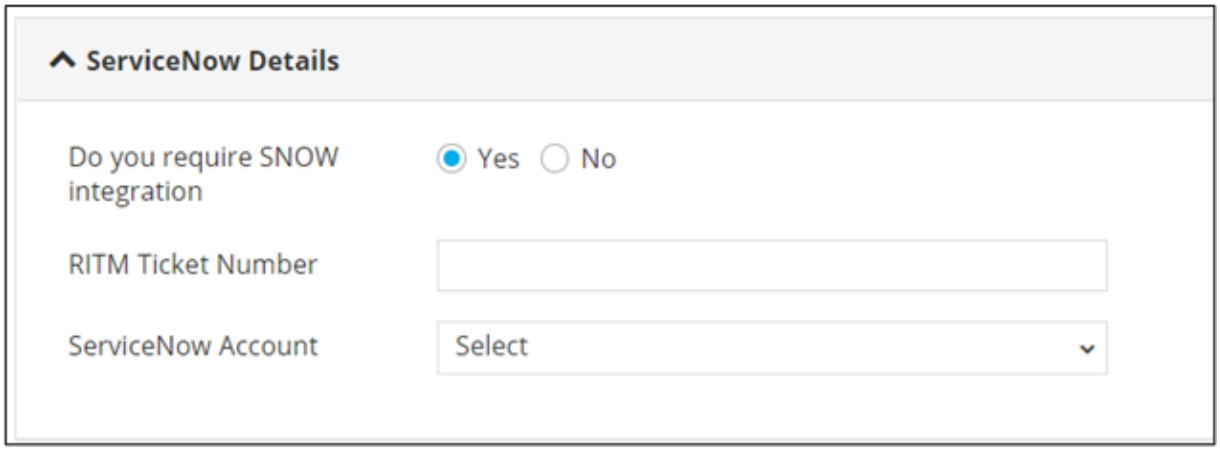
10. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
11. Enter a value for the selected attribute.



12. To add this attribute to the **Certificate Attributes** grid, click  .
13. To edit the value of a particular attribute, select the attribute in the grid and click  .
14. Enter the new value for the attribute in the **Value** field and click  again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click  .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .



17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Under the **ServiceNow Details** section, enter or select the required field information.

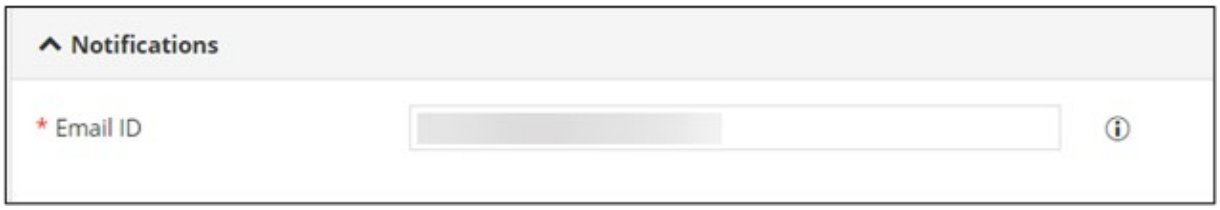


The following table describes the field information in the **ServiceNow Details** section:

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached.

Field	Description
	Note: This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

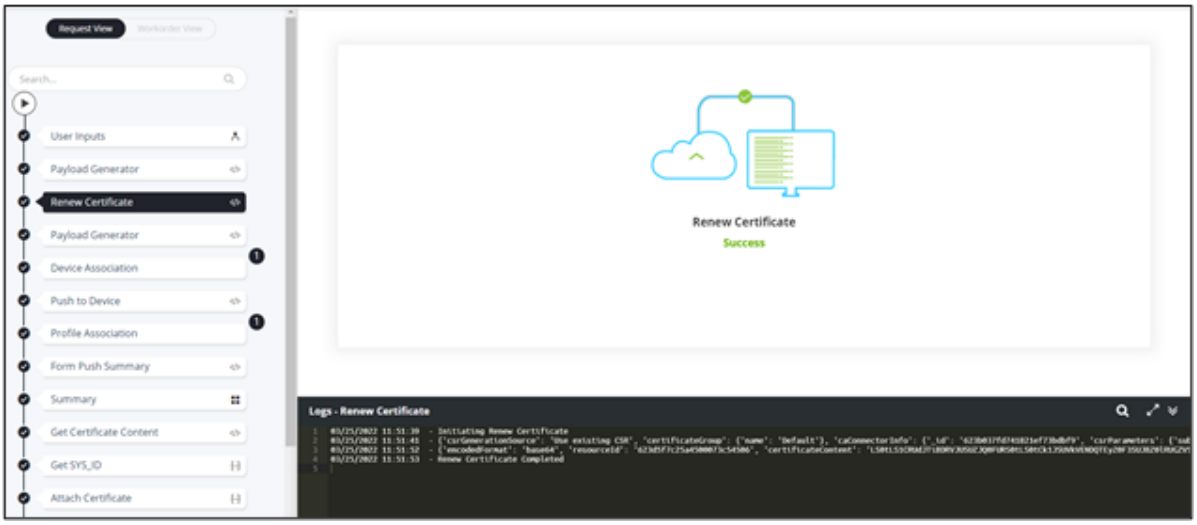
19. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.



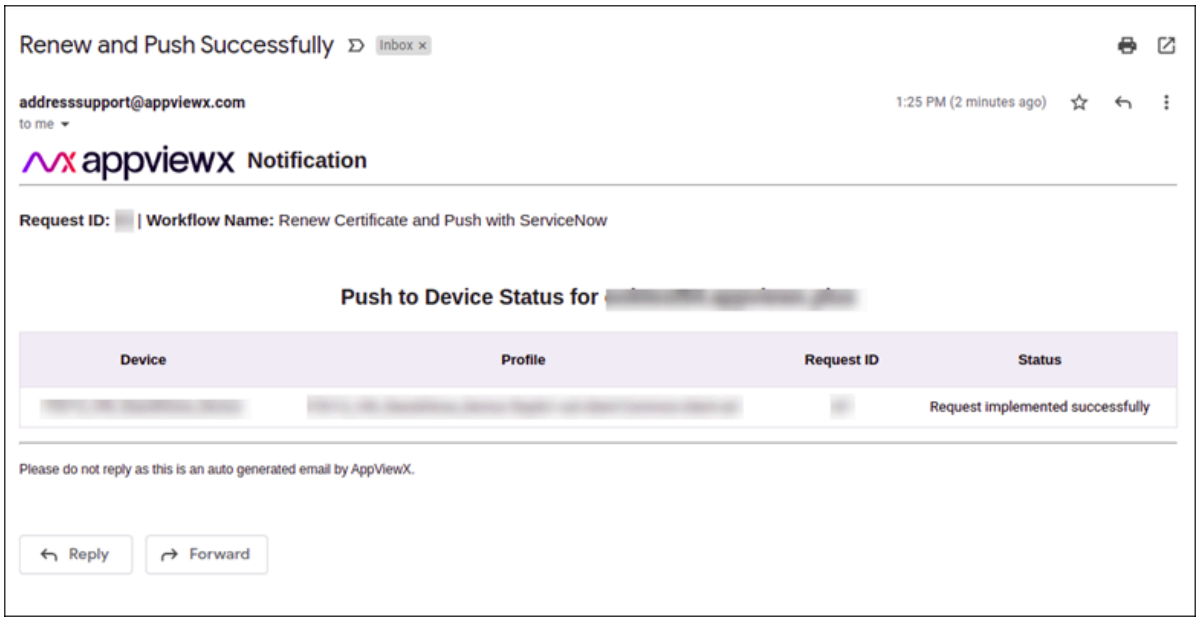
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

20. Click **Submit**.

• Certificate renewed successfully.



• Email notification received.



21. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.

22. Hover your mouse over  to view the **Certificate status**.

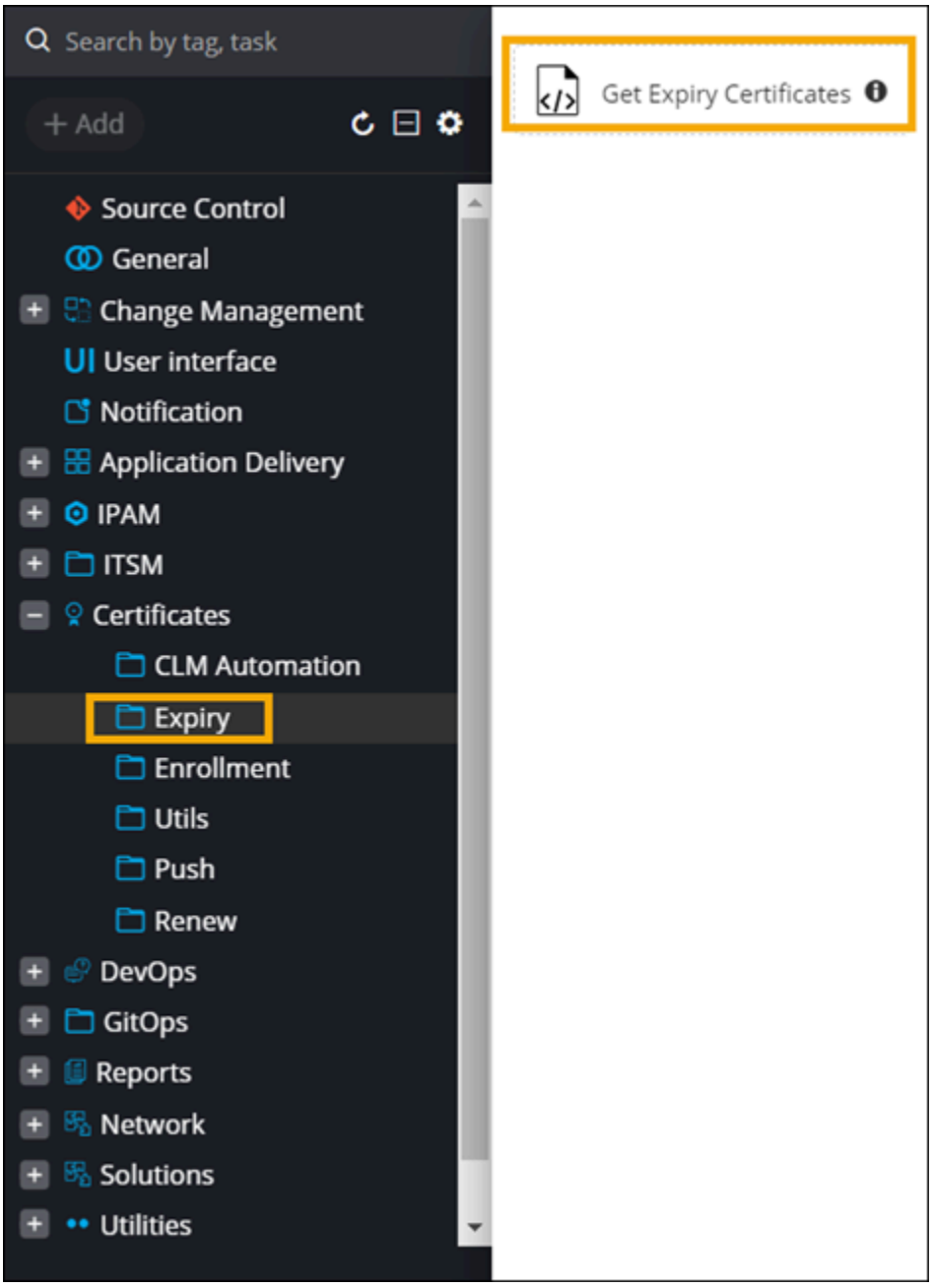
Chapter 8: Automation Workflow Tasks

Overview

This section will describe the various OOB tasks available in the Workflow Studio.

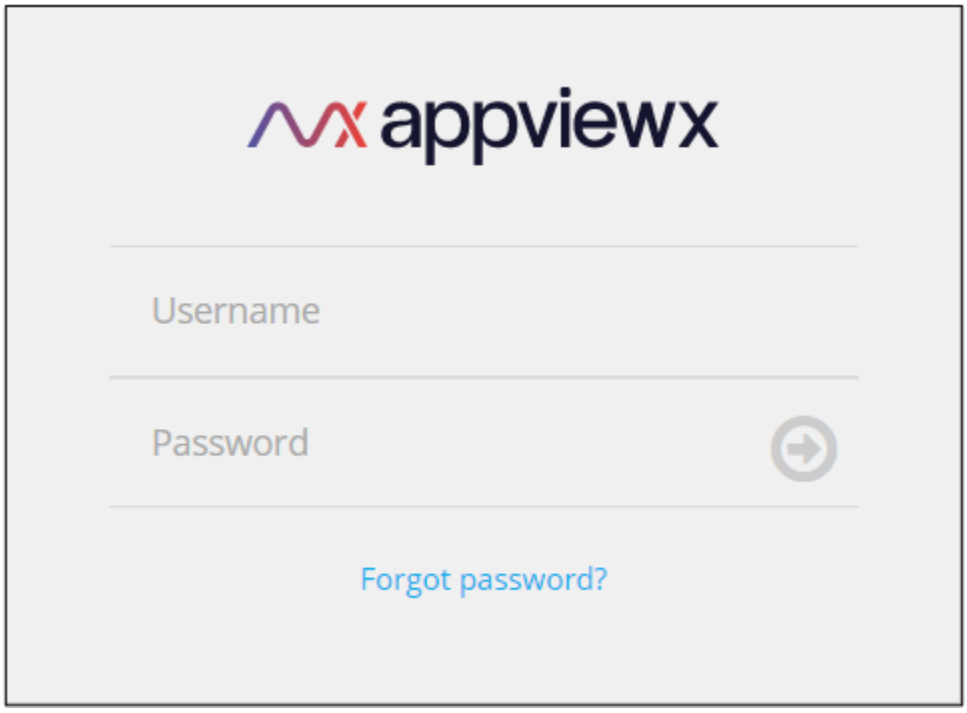
Expiry Task

You can design a custom workflow for receiving certificate expiry notifications using the prebuilt task for getting expiry certificates available in the **Workflow Studio**. The OOB script task for getting expiry certificates can be found under **Certificates**, in the **Expiry** folder.

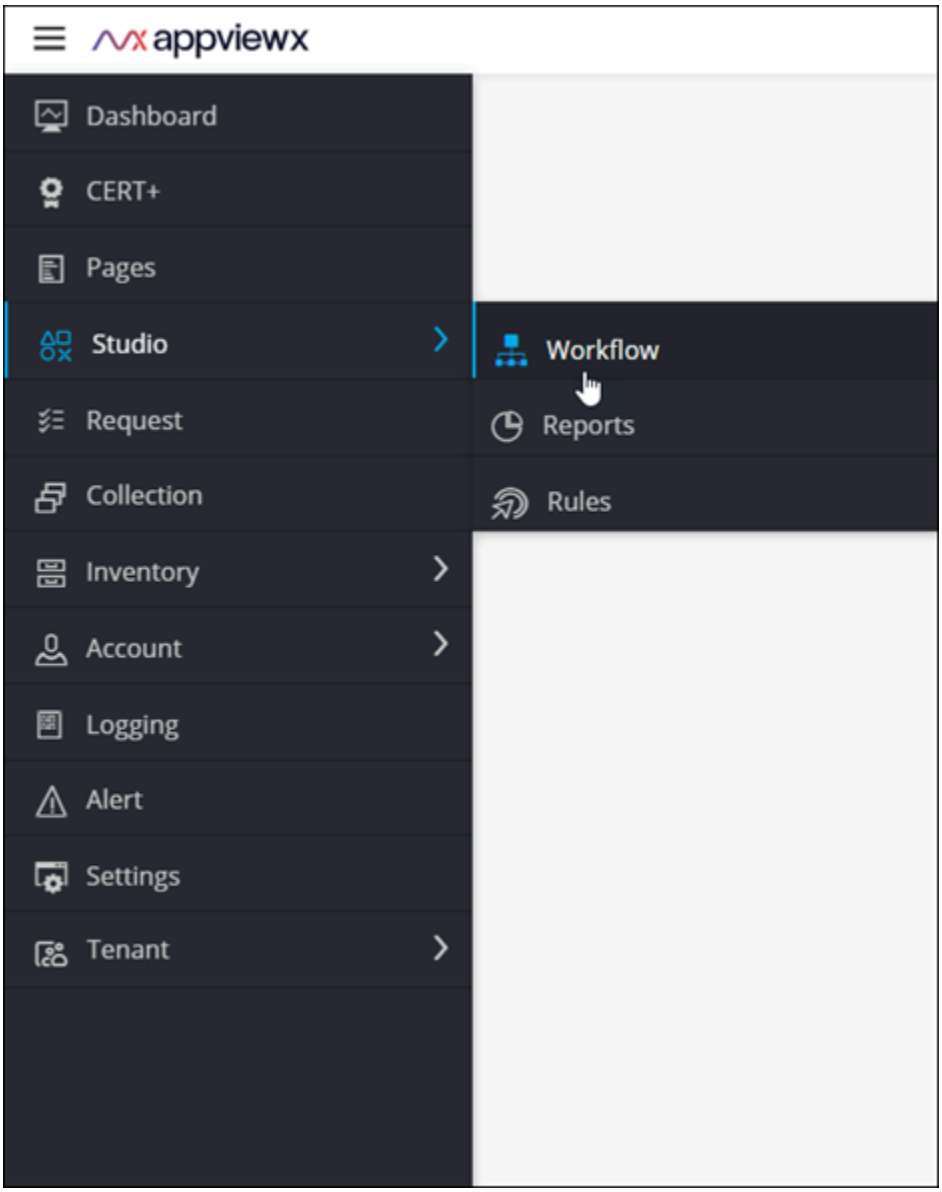


To design a custom workflow using the **Get Expiry Certificates** task

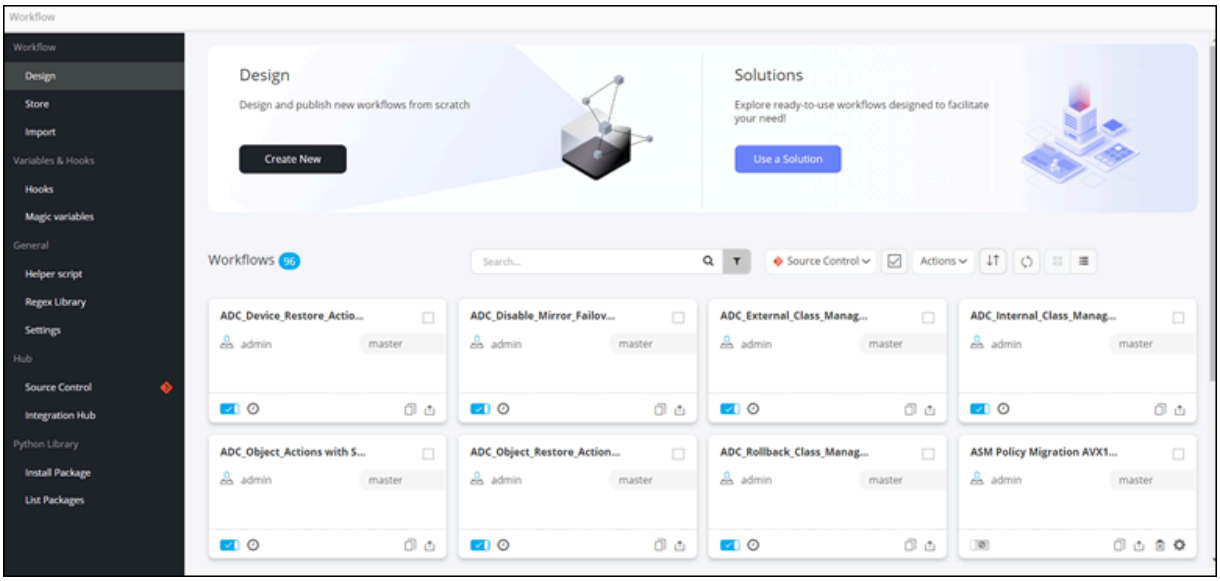
1. Log into AppViewX with valid credentials.



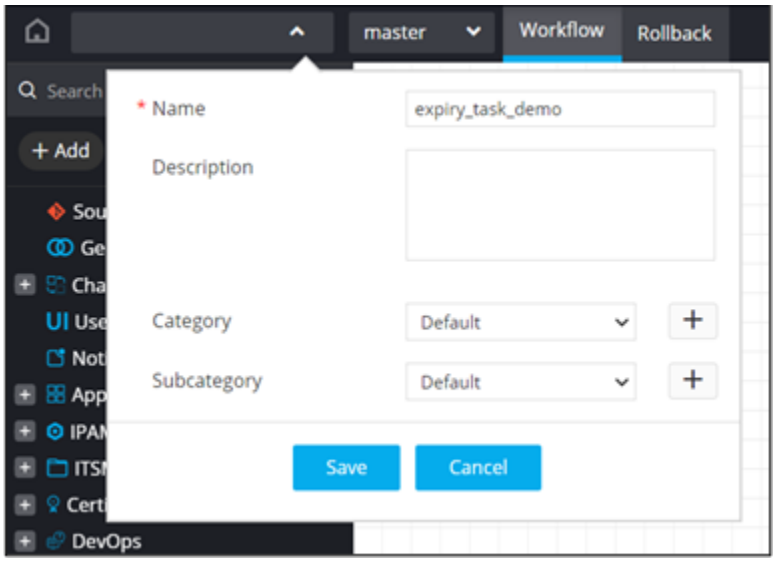
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



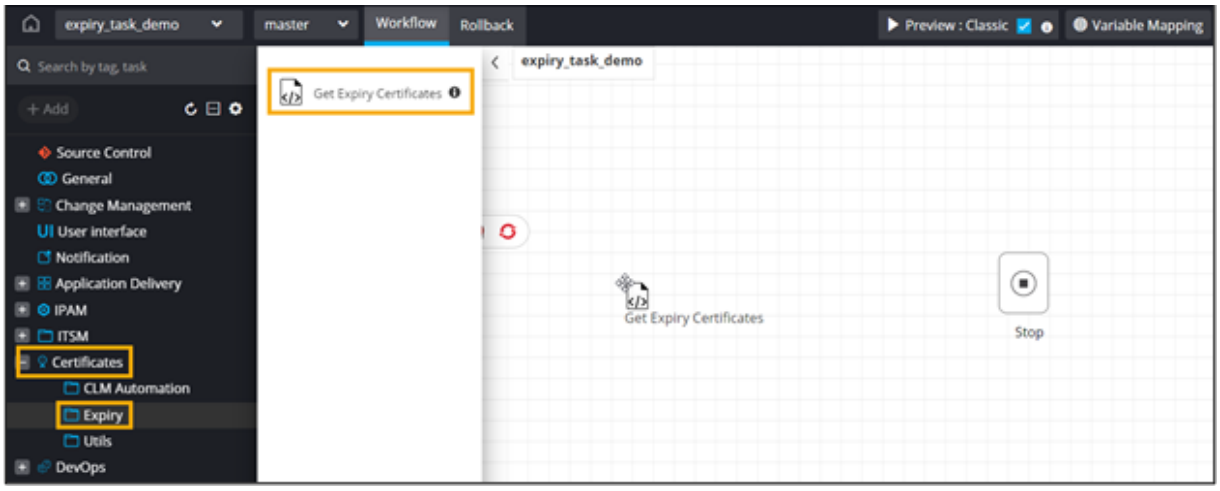
The **Workflow** inventory page is displayed.



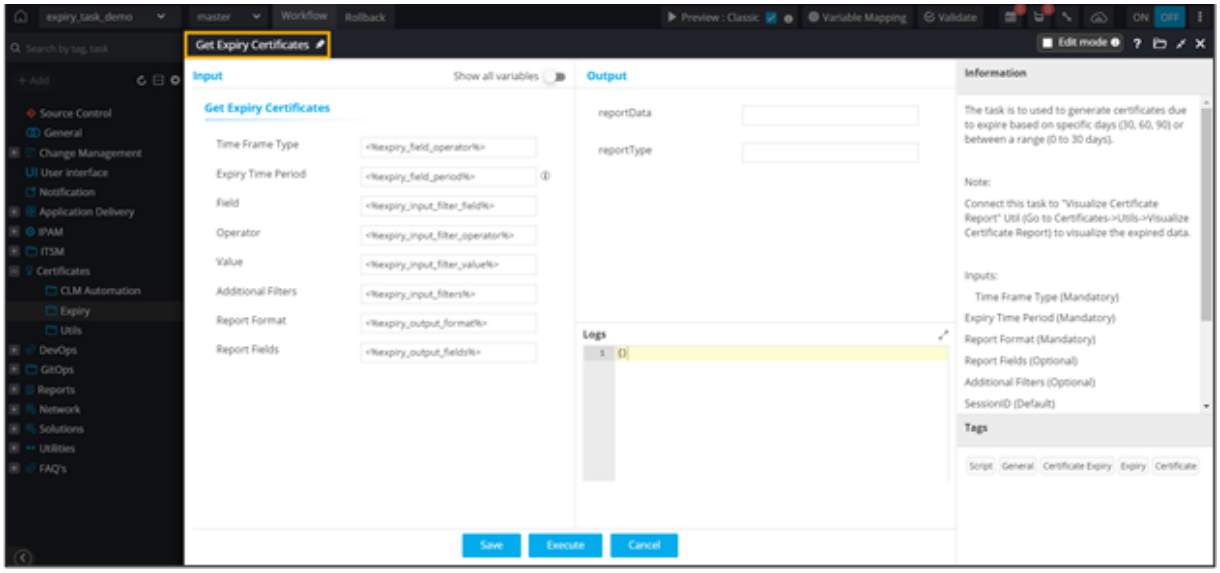
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



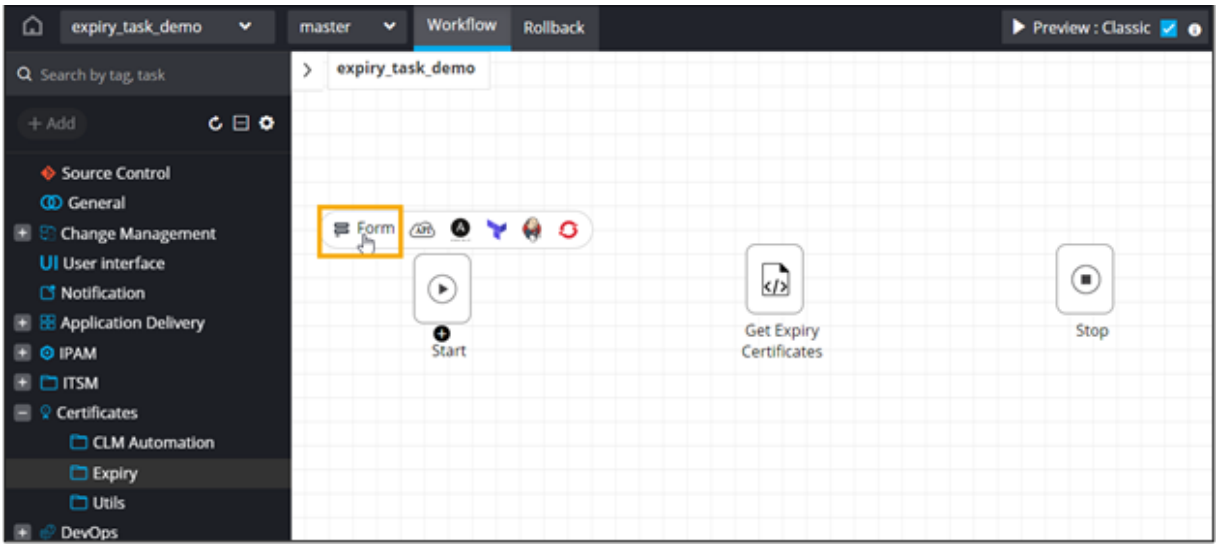
7. From the **Certificates** folder, under **Expiry**, drag and drop the **Get Expiry Certificates** task.



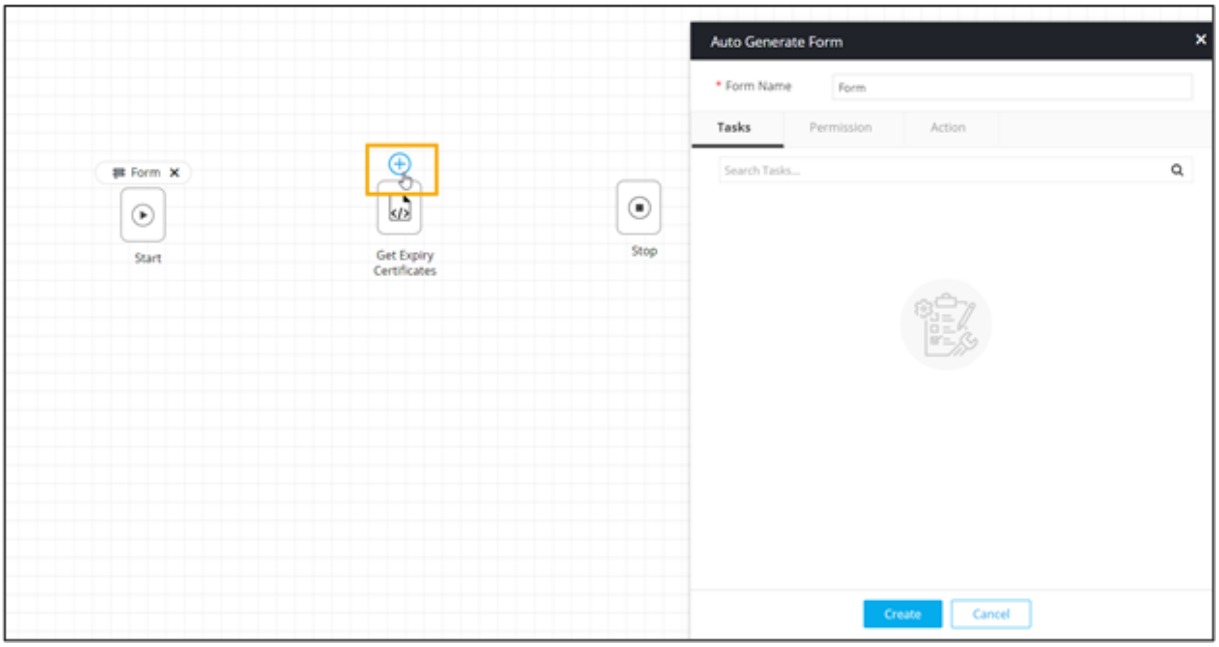
This task can be used to generate a report listing certificates due to expire in a specific number of days.



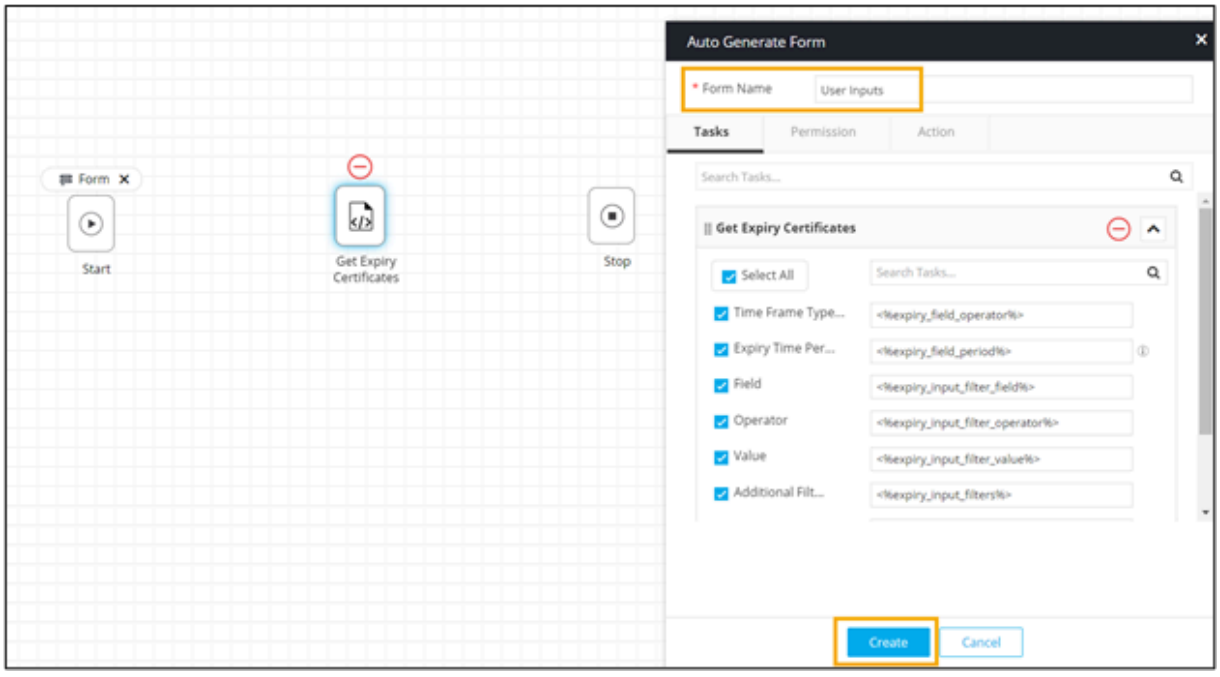
8. To auto-generate a form for this workflow, click **Form** above the **Start** task.



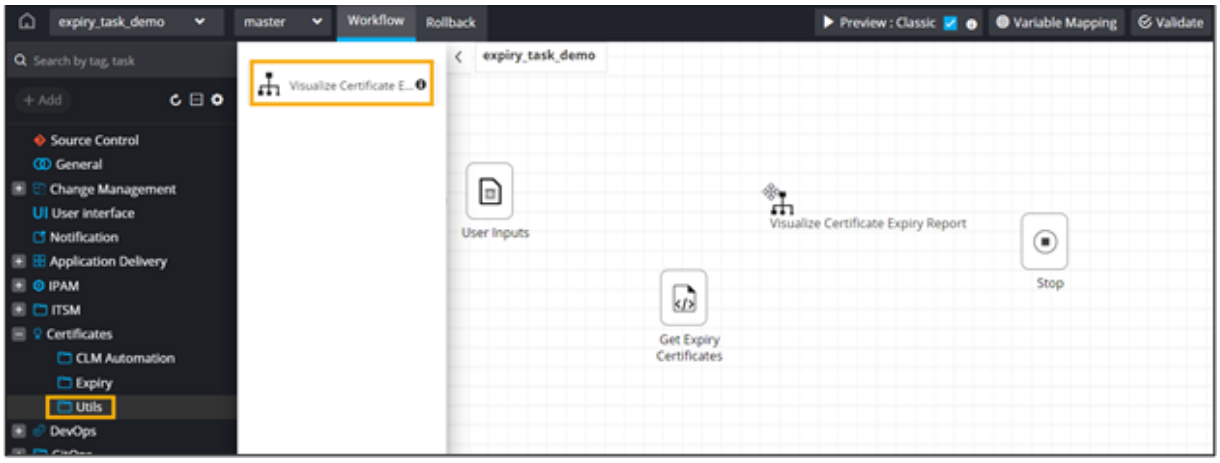
9. Click ⊕ above the **Get Expiry Certificates** task to auto-populate the form fields.



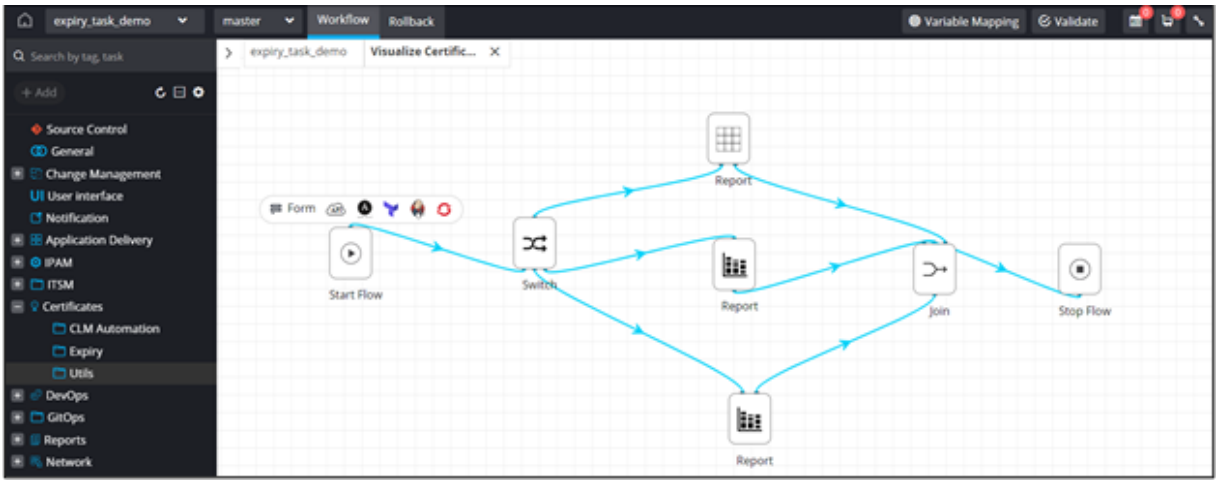
10. Select the fields required in the input form.
11. Provide a **Form Name** and click **Create**.



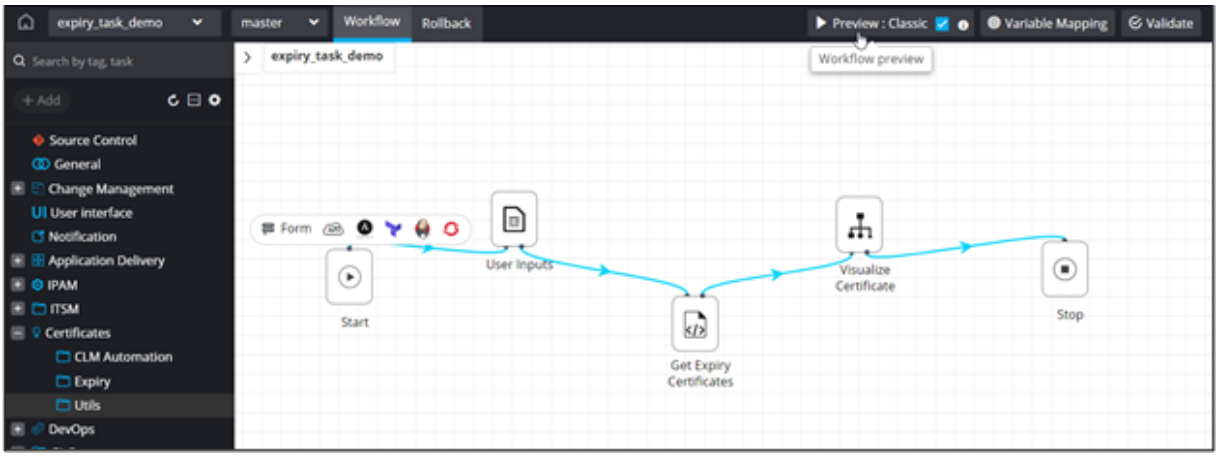
12. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.



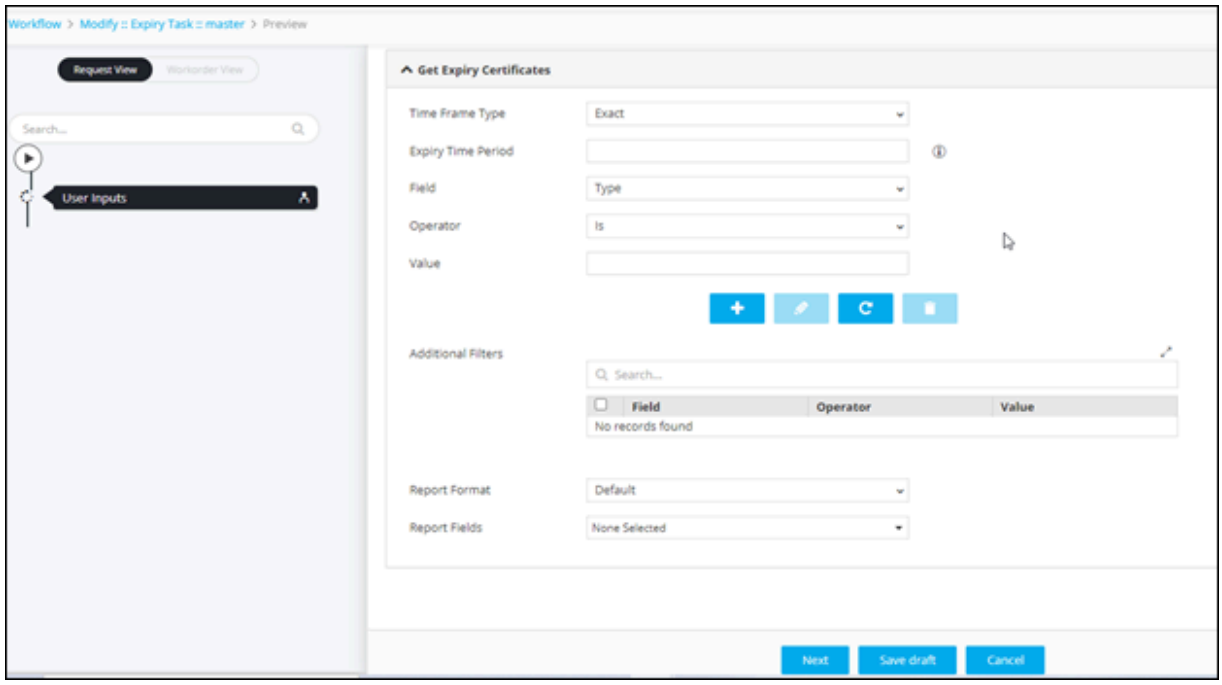
This subflow includes User Interface tasks such as Grid and Chart (Pie chart and Stacked bar chart). The report generated will be displayed as a grid or a chart based on the inputs provided in the input form.



13. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.



User Inputs form is displayed.



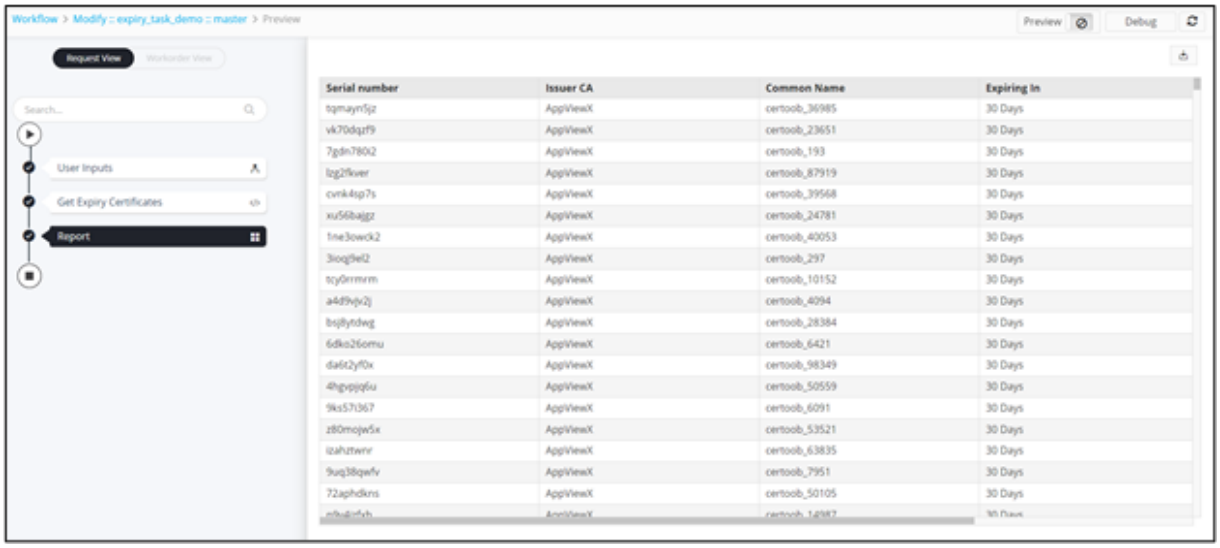
The following table describes the field information in the **User Inputs** form:

Field	Description
Time Frame Type	Enter the time frame type from the available options: • **Exact** - Allows you to enter the exact value for the expiry time period (30 days). • **Range** - Allows you to give a range for the expiry time period (0 - 30). **Note: Exact** is the default selection.
Expiry Time Period	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Field	Select the field from the options available in the dropdown.
Operator	Select the conditional operator: • **Is** • **Is Not**

Field	Description
Value	Enter a valid value for filtering the certificates.
Additional Filters	This grid displays the values selected in these fields: • **Field** • **Operator** • **Value** **Note:** The steps to apply these additional filters are given below the table.
Report Format	Select the format in which the report is displayed from the available options: • **Default** • **Pie Bar Chart** • **Stacked/Bar Chart**
Report Fields	Select the fields to be displayed in the report from the options available in the dropdown.

14. To add filters to the **Additional Filters** grid, click 
15. To edit the value of a particular filter, select the filter in the grid and click  .
16. Enter the new value(s) for the filters (Field/Operator/Value) and click  again to update the value(s).
17. To delete a filter, select the filter in the grid and click  .
18. To maximize the **Additional Filters** grid, from the top right corner of the grid, click  .
19. Click **Next**.

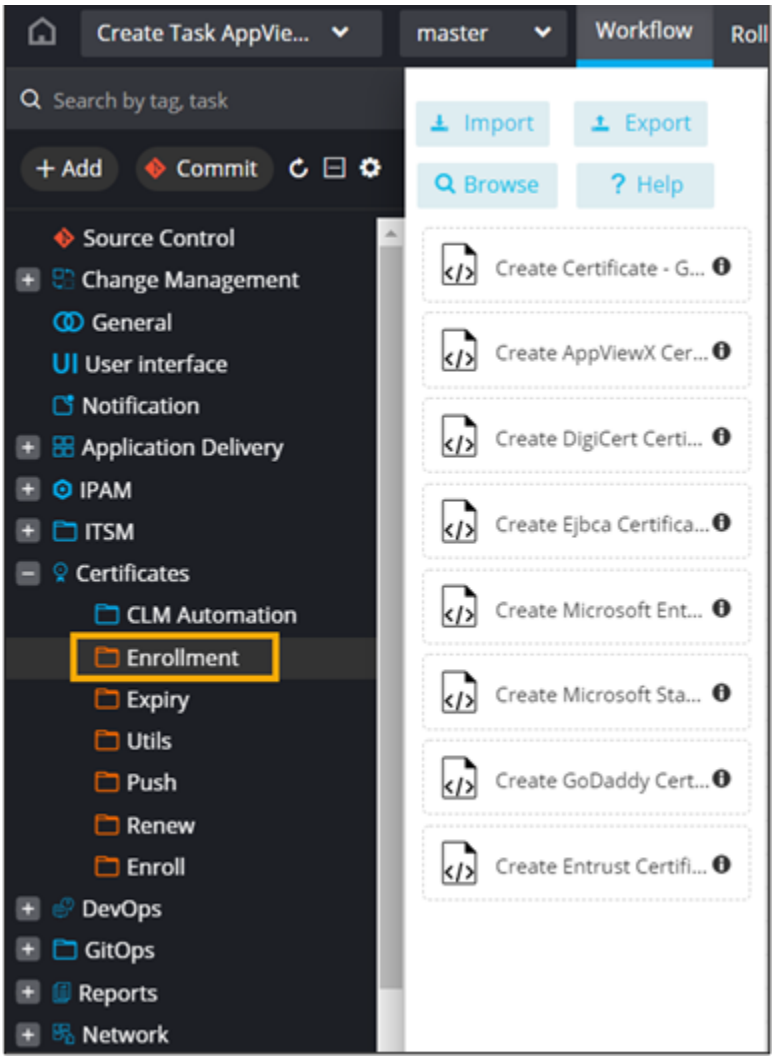
    Report generated with expiry certificates data is displayed in Grid format.



Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

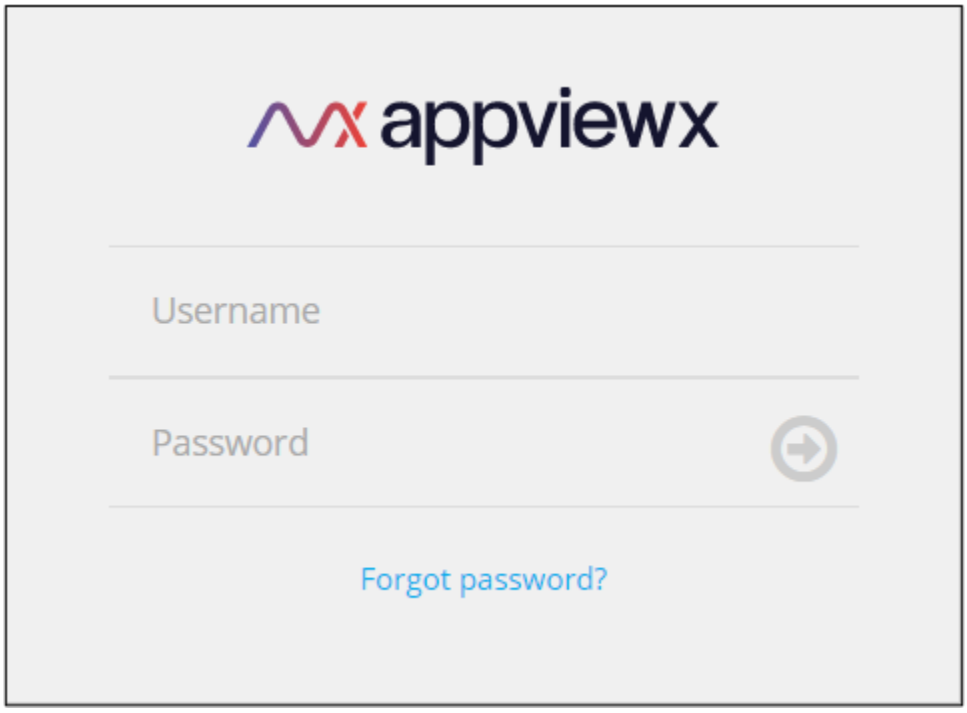
Enrollment Tasks

You can design a custom workflow for enrolling a certificate using the prebuilt Create Certificate tasks available in the **Workflow Studio**. The OOB script task for enrolling certificates through different Certificate Authorities can be found under **Certificates**, in the **Enrollment** folder.

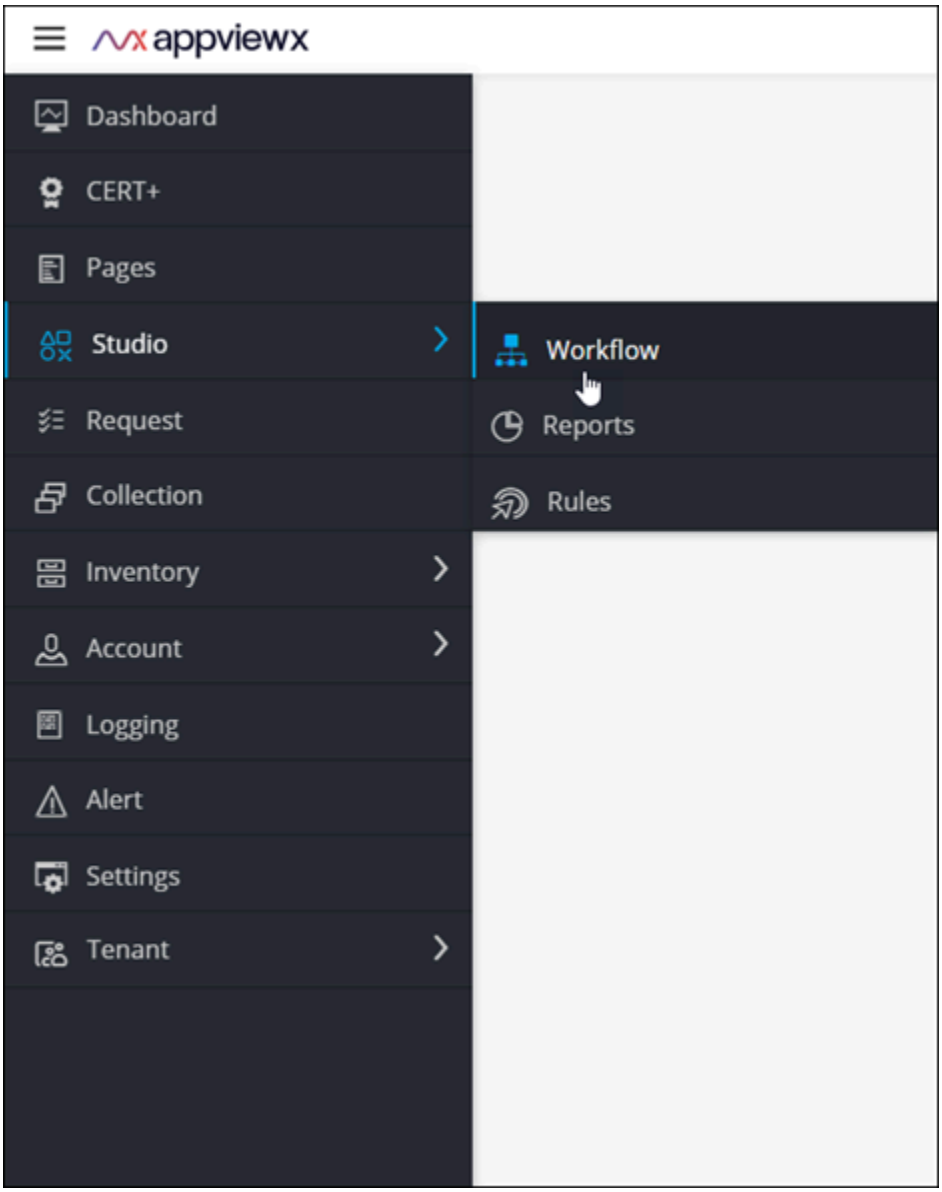


To design a custom workflow using **Enrollment** tasks:

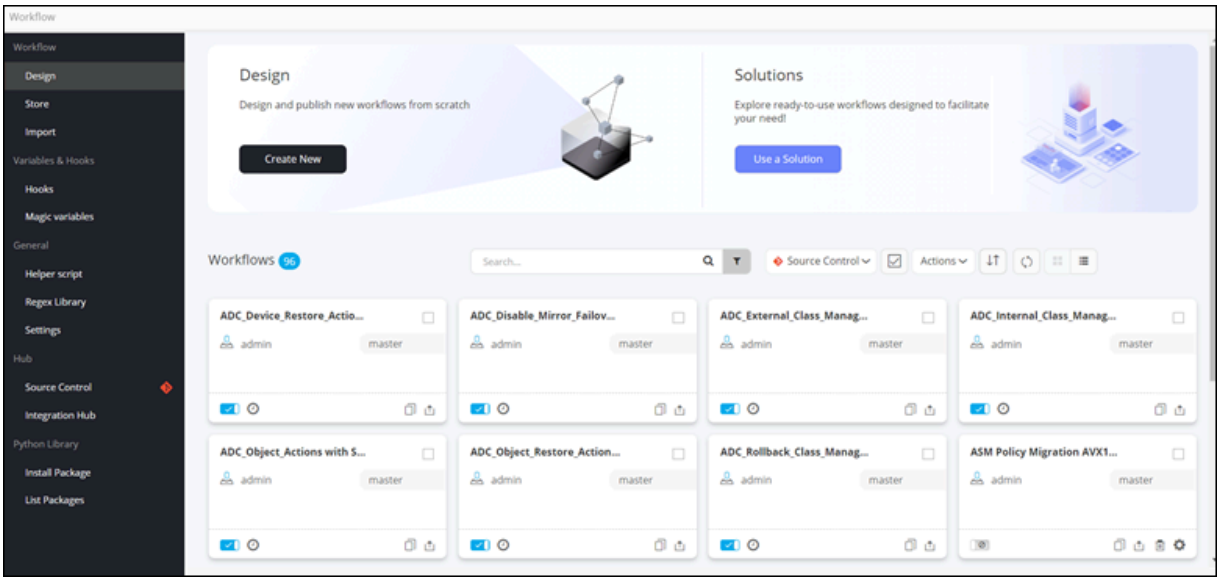
1. Log into AppViewX with valid credentials.



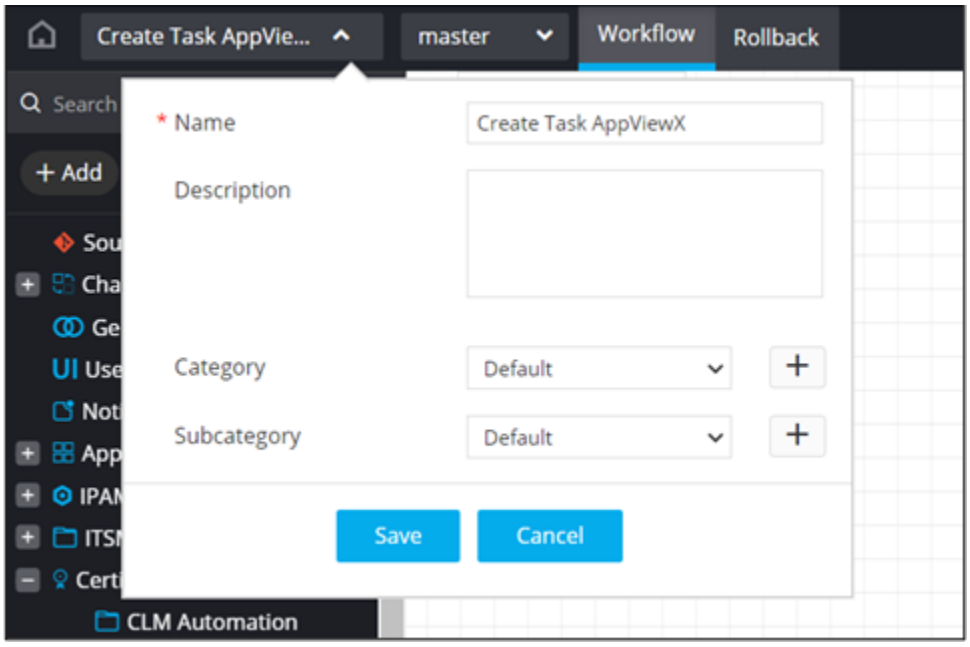
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



The **Workflow** inventory page is displayed.



4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



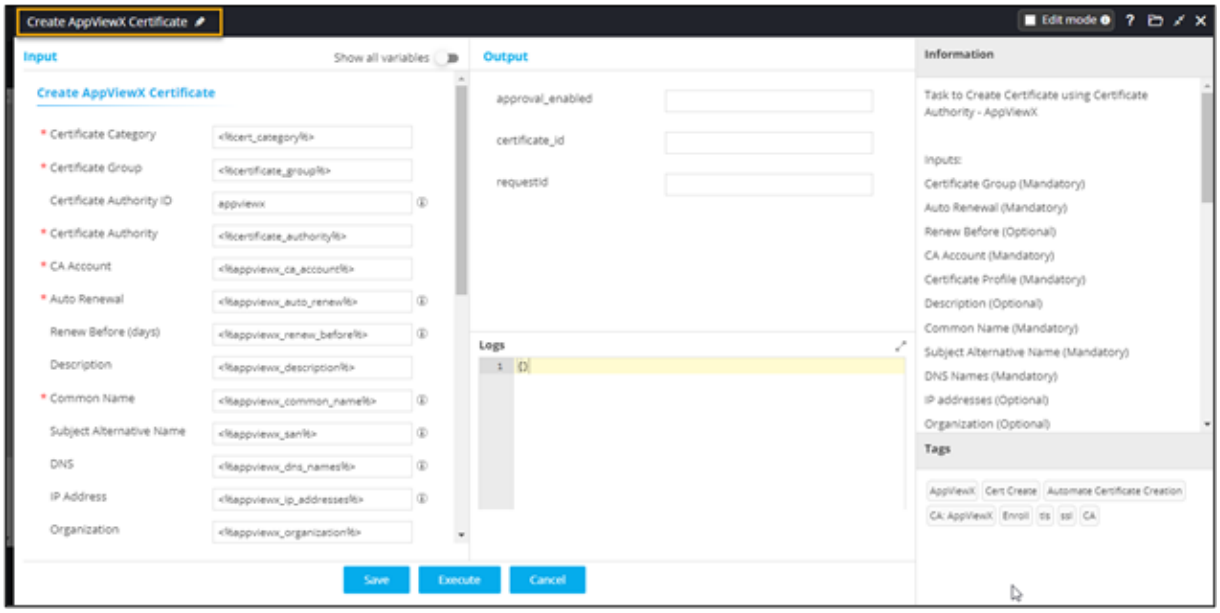
7. From the **Certificates** folder, click **Enrollment**.

   The tasks for the following CAs are available in the **Enrollment** folder:

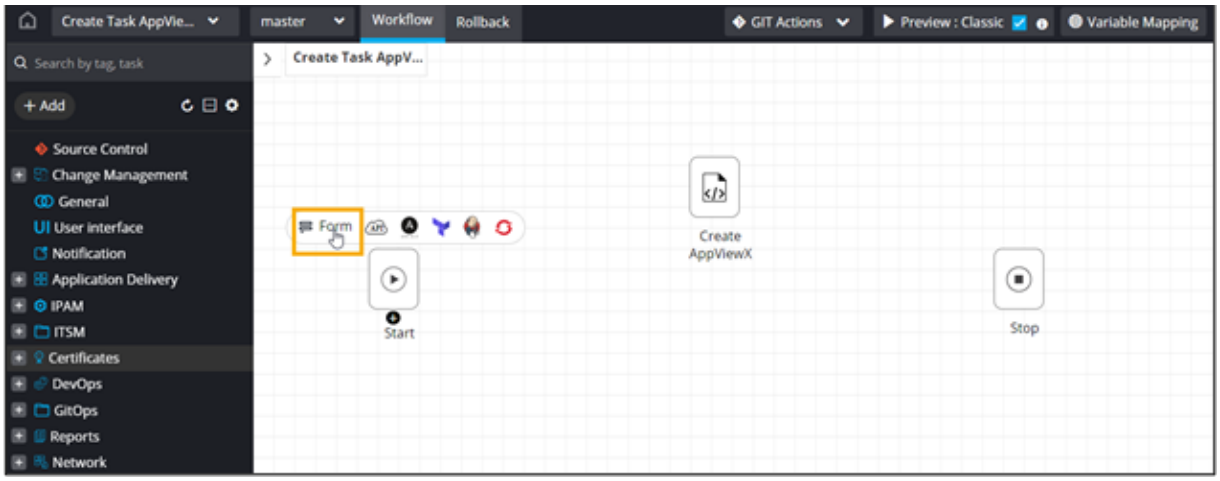
   - Appviewx
   - Digicert
   - Ejbca

- Entrust
- Microsoft Enterprise
- Microsoft Standalone
- GoDaddy

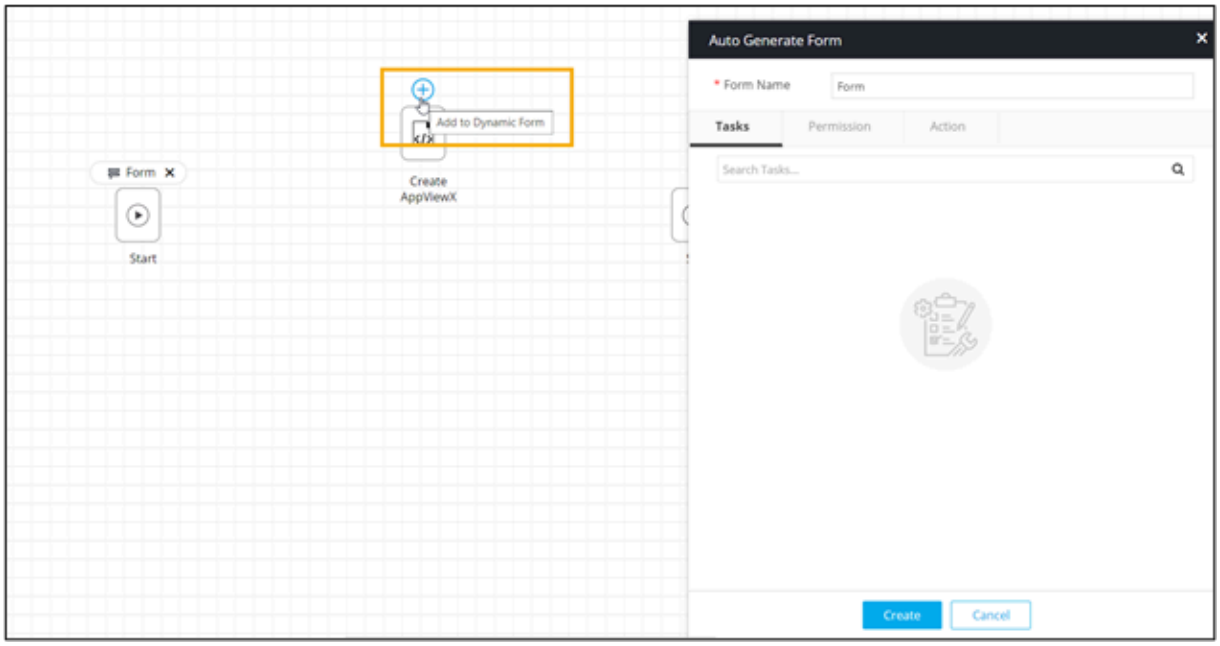
8. From the **Enrollment** folder, drag and drop any of the Create Certificate tasks. For example, the **Create AppViewX Certificate** task.



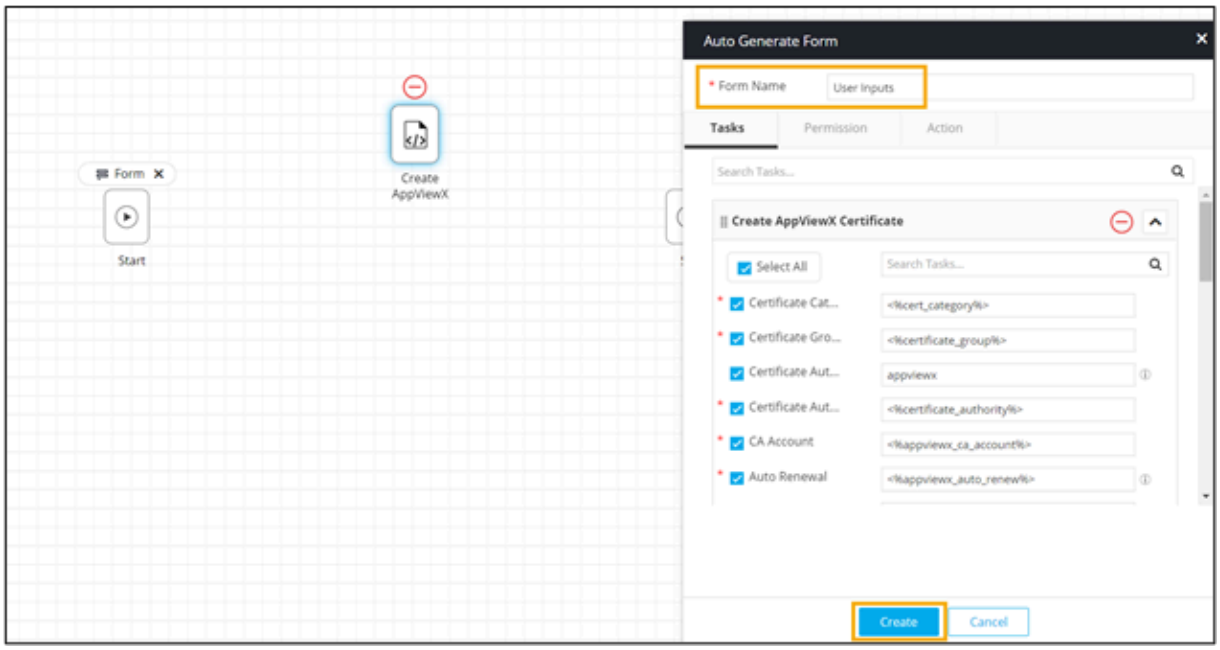
9. Click **Save**.
10. To auto-generate a form for this workflow, click **Form** above the **Start** task.



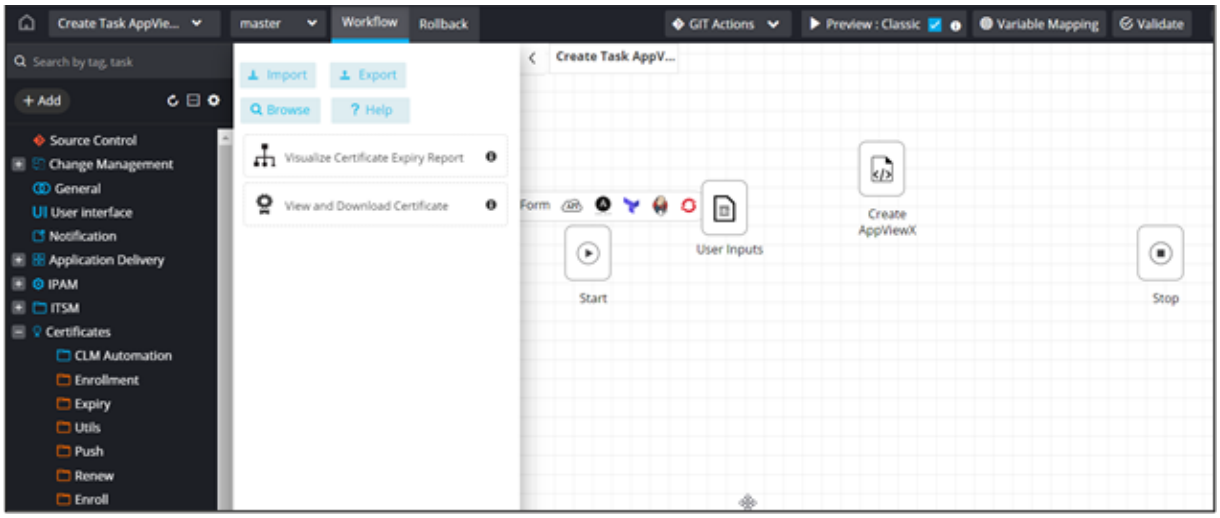
11. Click ⊕ above the **Create AppViewX** task to auto-populate the form fields.



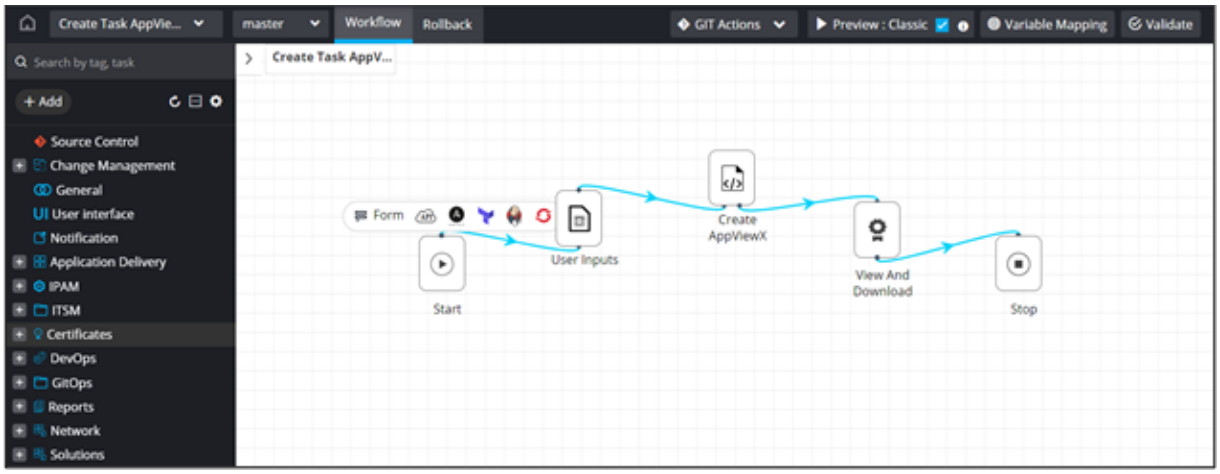
12. Select the fields required in the input form.
13. Provide a **Form Name** and click **Create**.



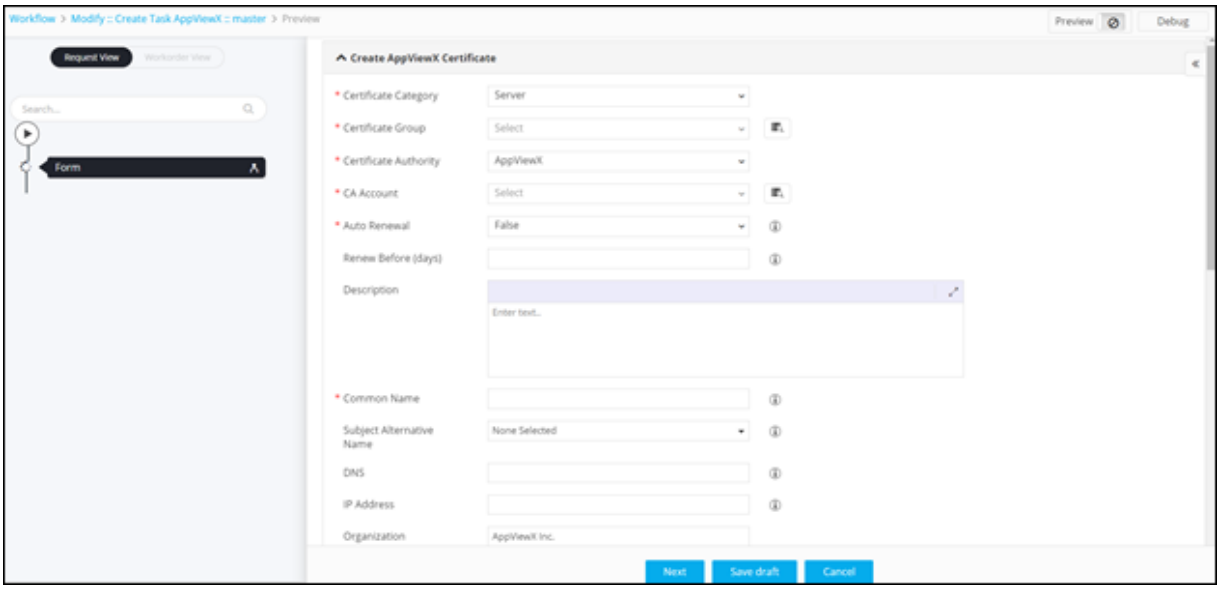
14. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.



15. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.



User Inputs form when the **Create AppViewX Certificate** task is selected is displayed.



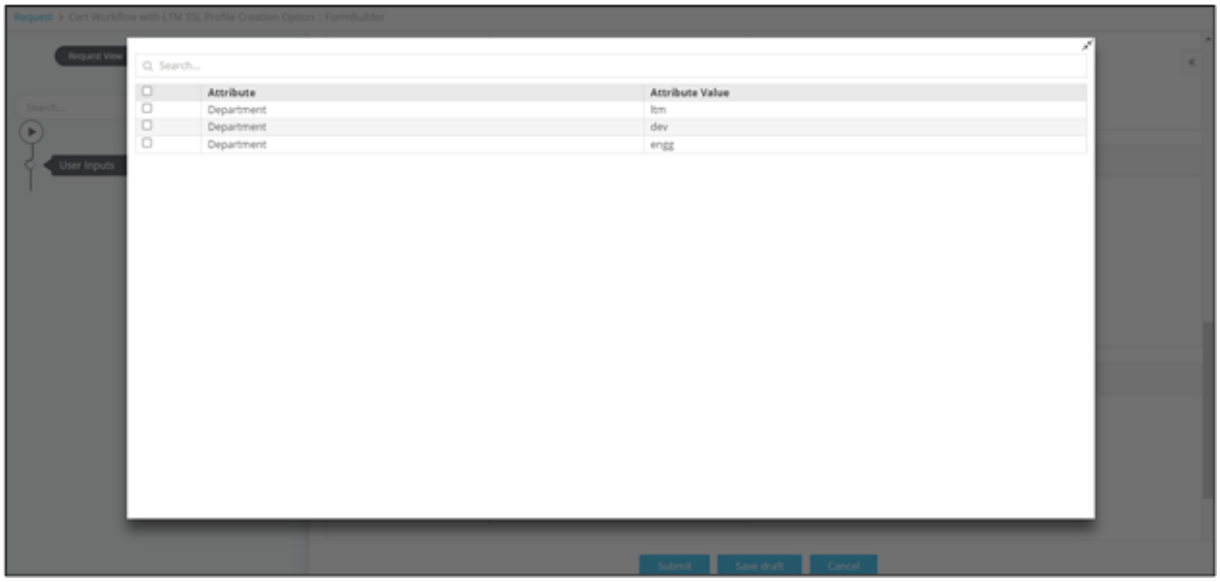
The following table describes the field information in the **User Inputs** form when the **Create AppViewX Certificate** task is selected:

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the **Certificate Group** field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the **CA Account** field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.

Field	Description
Renew Before (days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date.
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter theEmail Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Enter the challenge password.
***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.

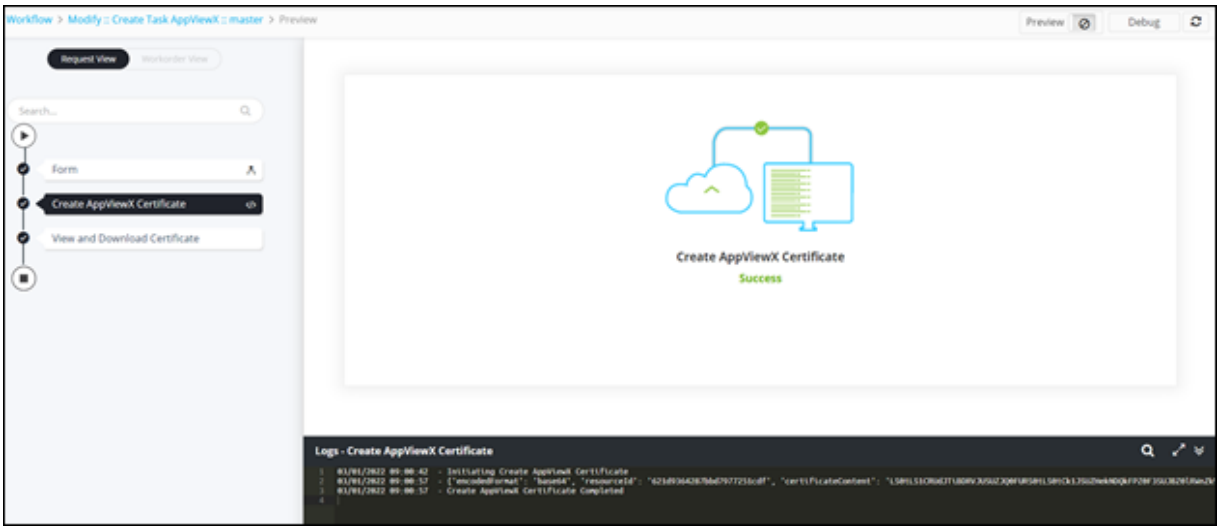
Field	Description
	Note: To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All asterisk (*) marked fields are mandatory.	

16. To add the attribute to the **Certificate Attributes** grid, click .
17. To edit the value of a particular attribute, select the attribute in the grid and click .
18. Enter the new value for the attribute in the **Value** field and click again to update the value.
19. To delete a certificate attribute, select the attribute in the grid and click .
20. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .

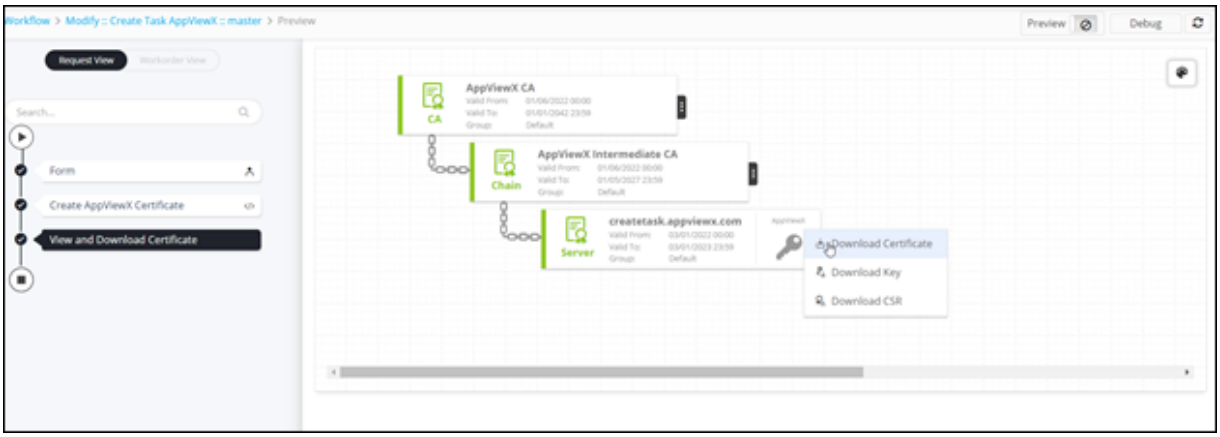


21. To search for a particular attribute in the grid, type the keyword(s) in the search field.
22. Click **Next**.

    AppViewX Certificate created.



23. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



24. Hover your mouse over  to view the **Certificate status**.

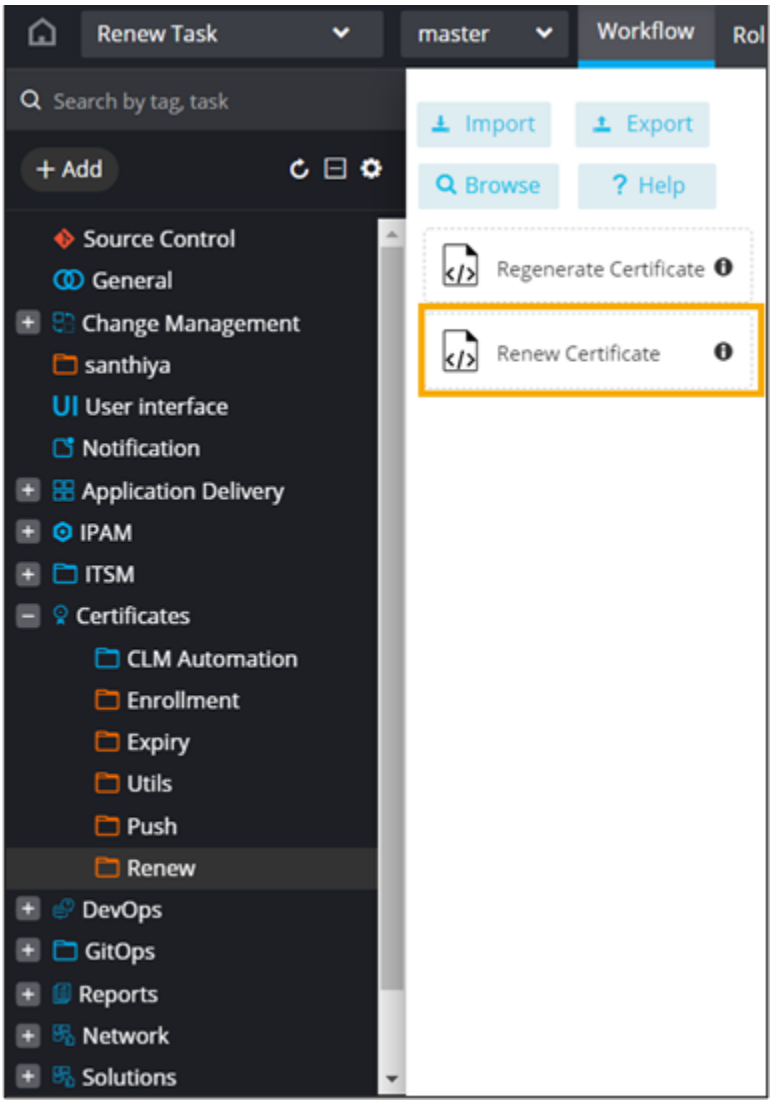
Renew Tasks

This section describes the Renew and Regenerate tasks that can be integrated with custom workflows to renew and regenerate certificates.

- Renew Task
- Regenerate Task

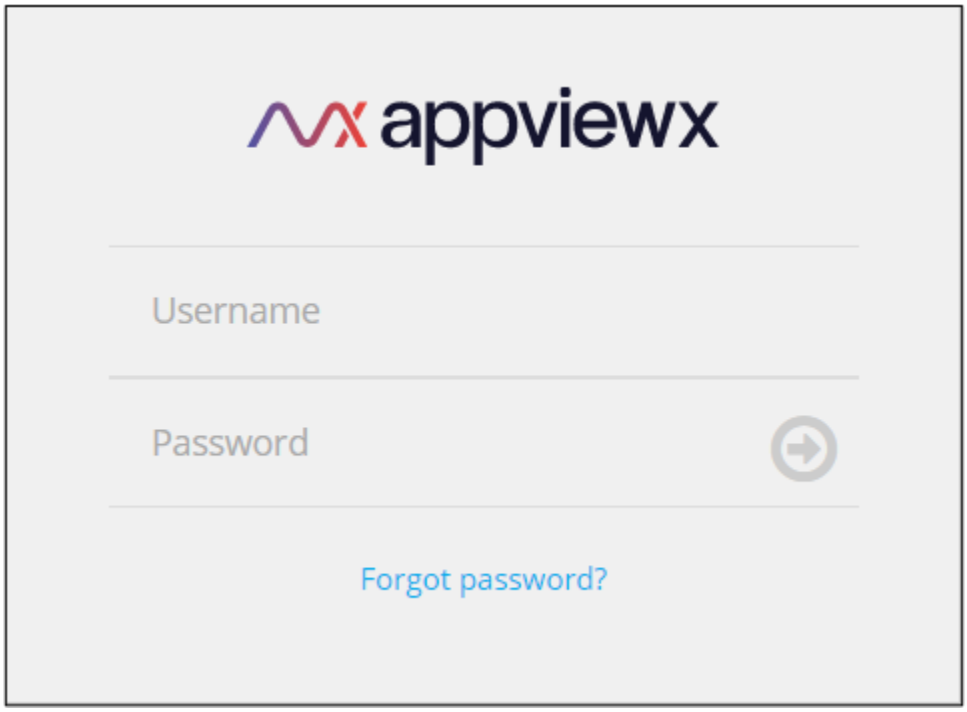
Renew Task

The OOB script task for renewing certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.

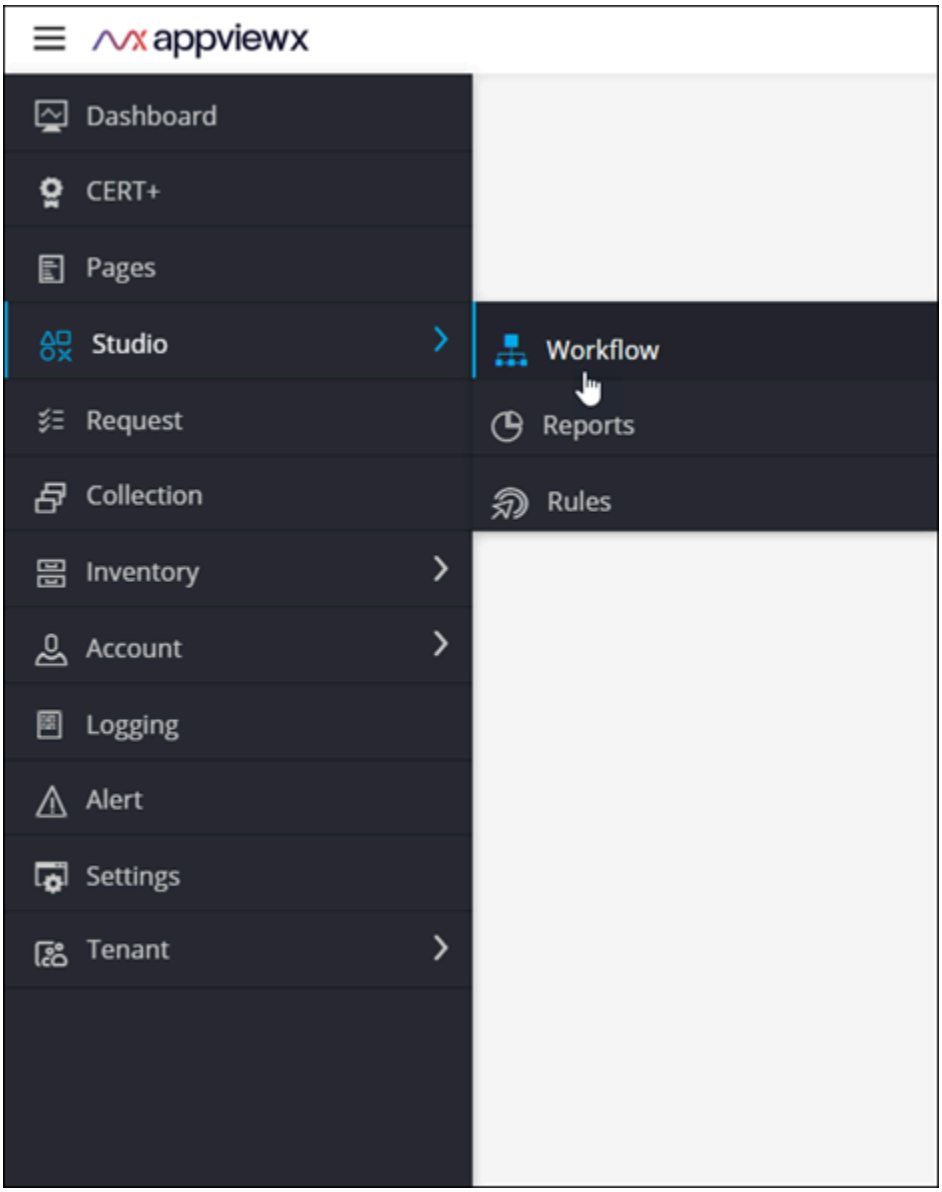


To design a custom workflow using the **Renew** task:

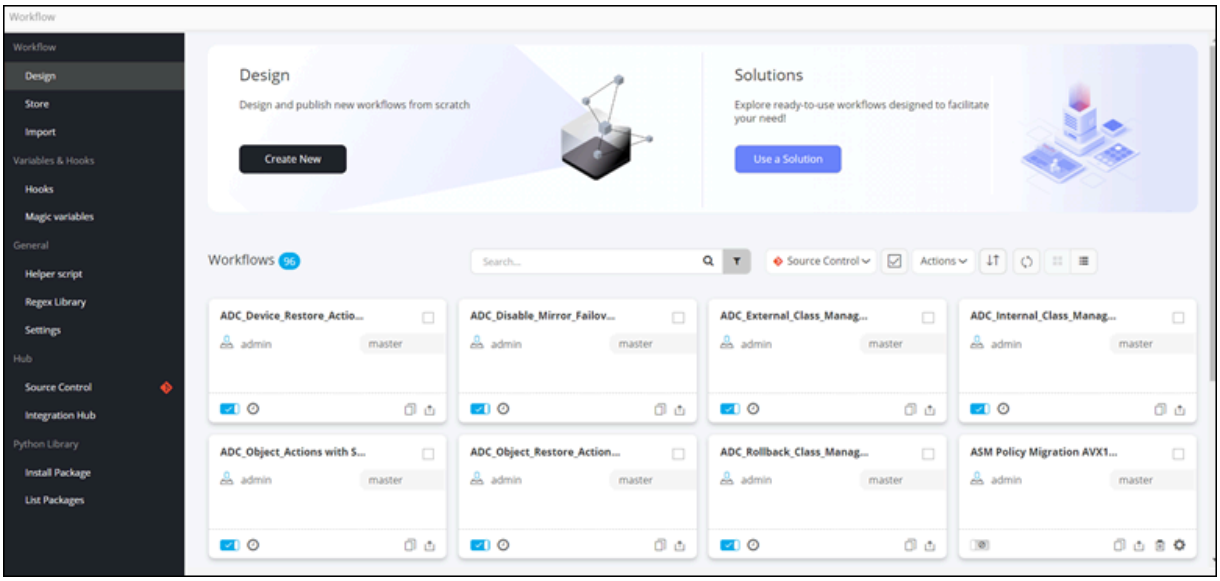
1. Log into AppViewX with valid credentials.



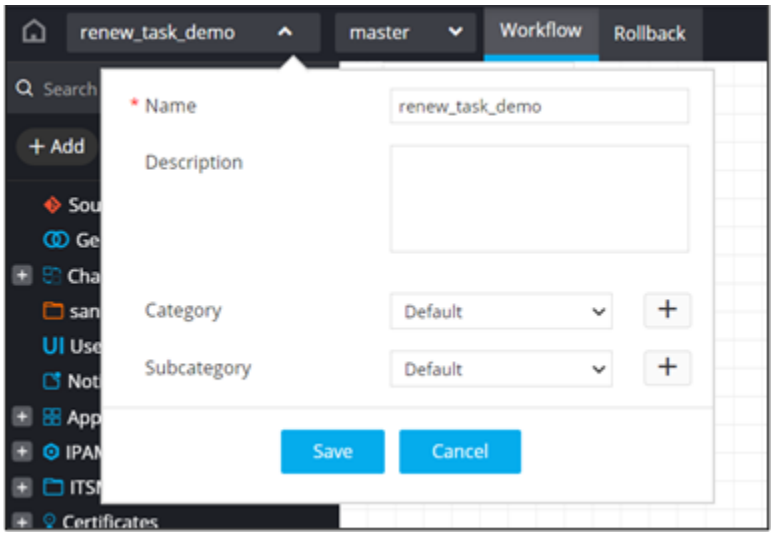
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



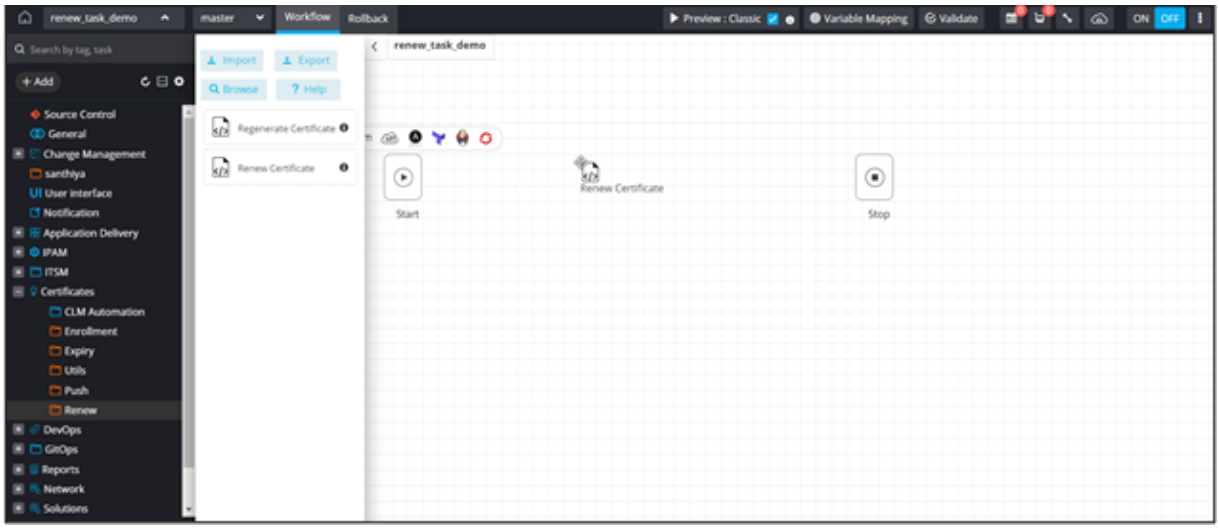
The **Workflow** inventory page is displayed.



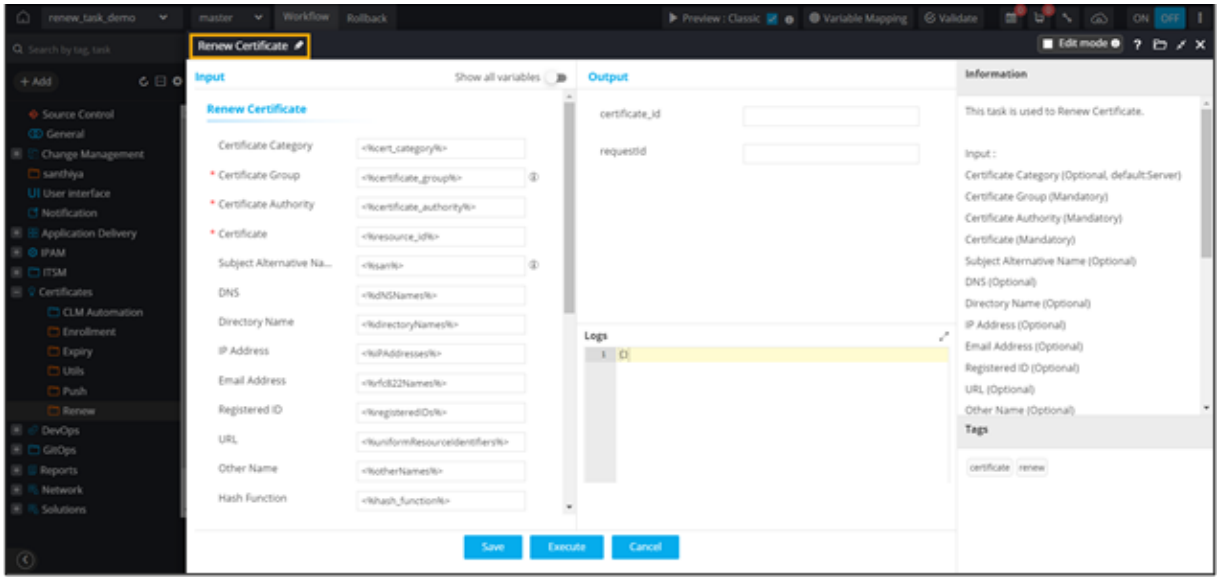
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



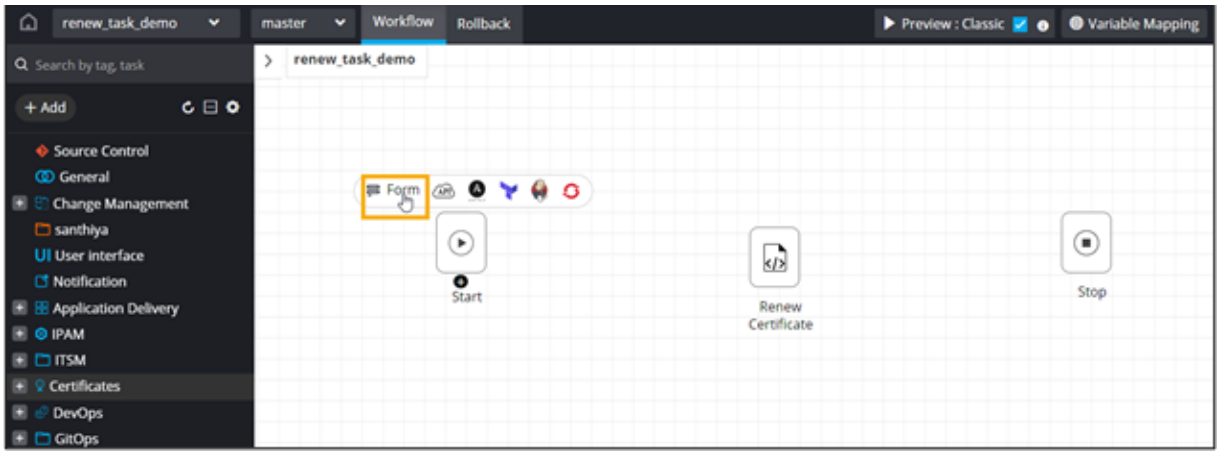
7. From the **Certificates** folder, under **Renew**, drag and drop the **Renew Certificate** task.



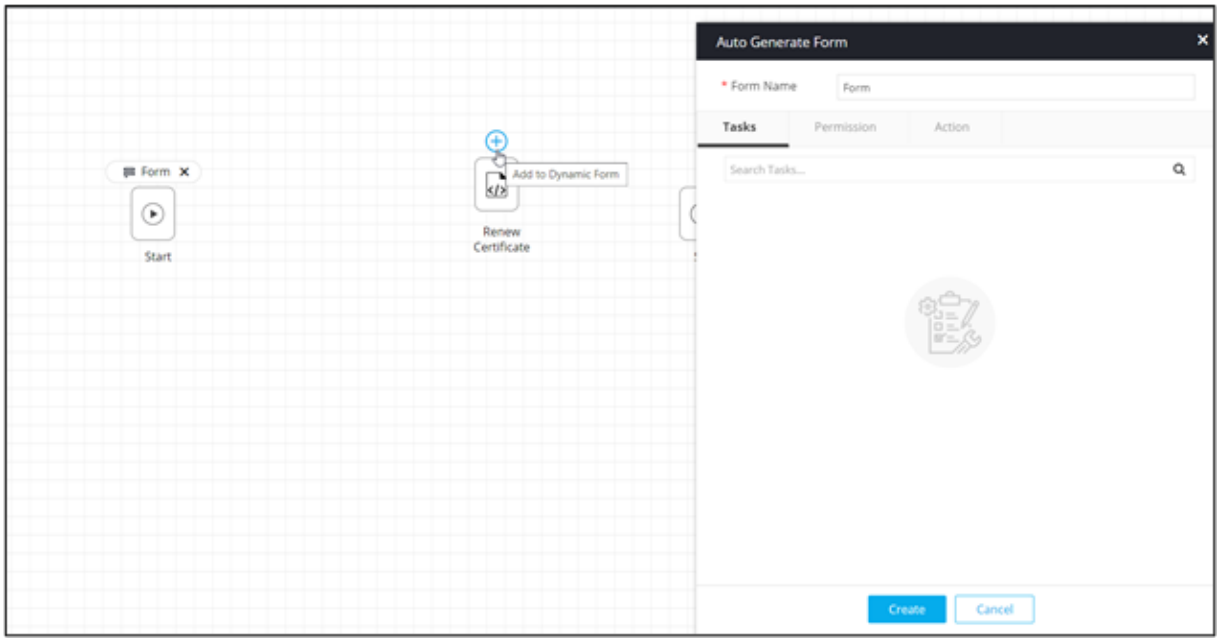
This task can be used to renew certificates.



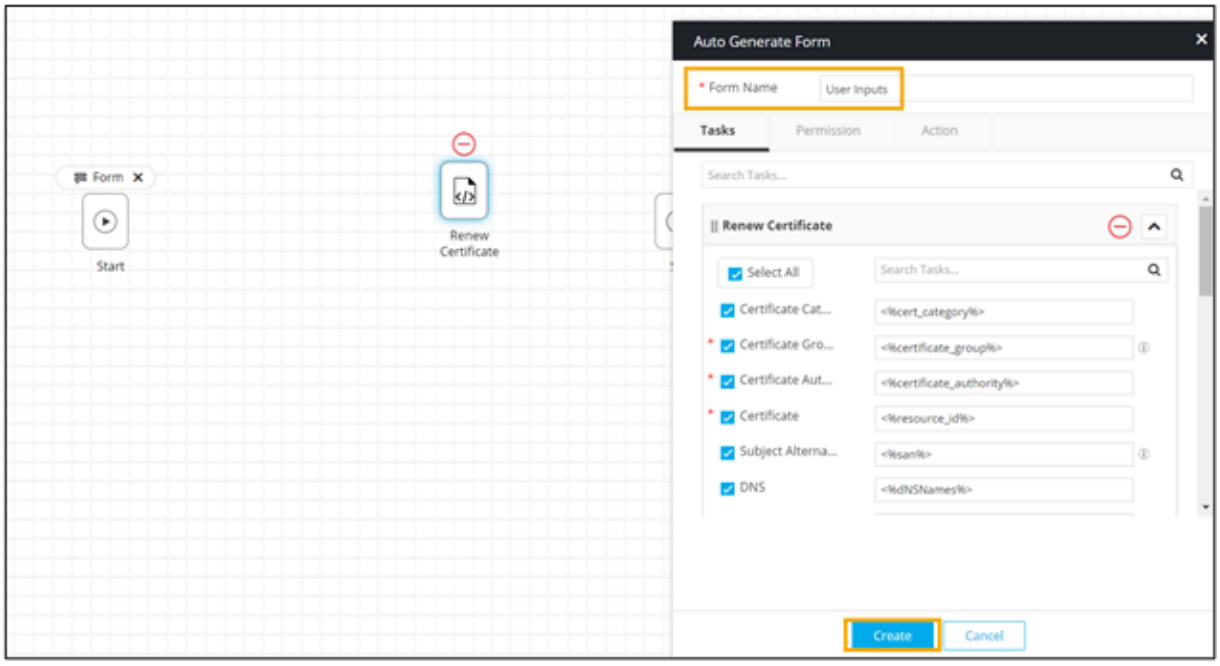
8. To auto-generate a form for this workflow, click **Form** above the **Start** task.



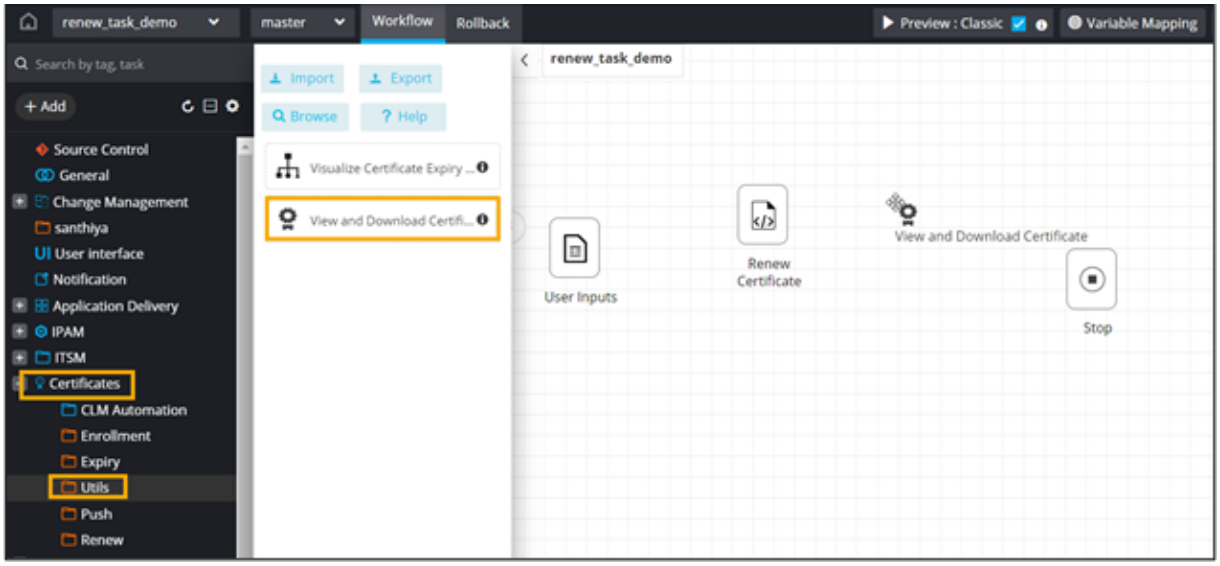
9. Click ⊕ above the **Renew Certificates** task to auto-populate the form fields.



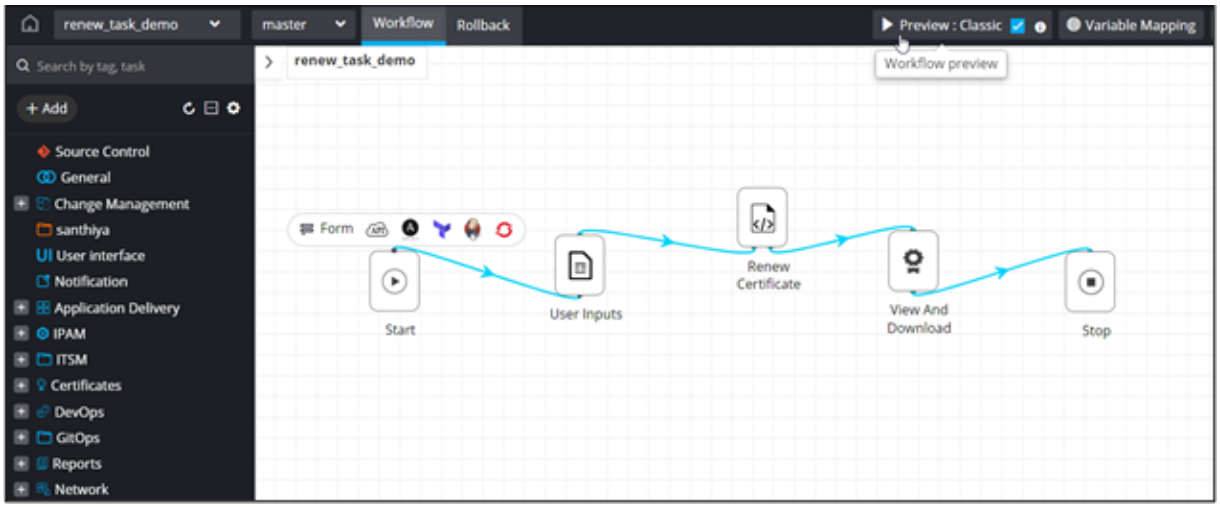
10. Select the fields required in the input form.
11. Provide a **Form Name** and click **Create**.



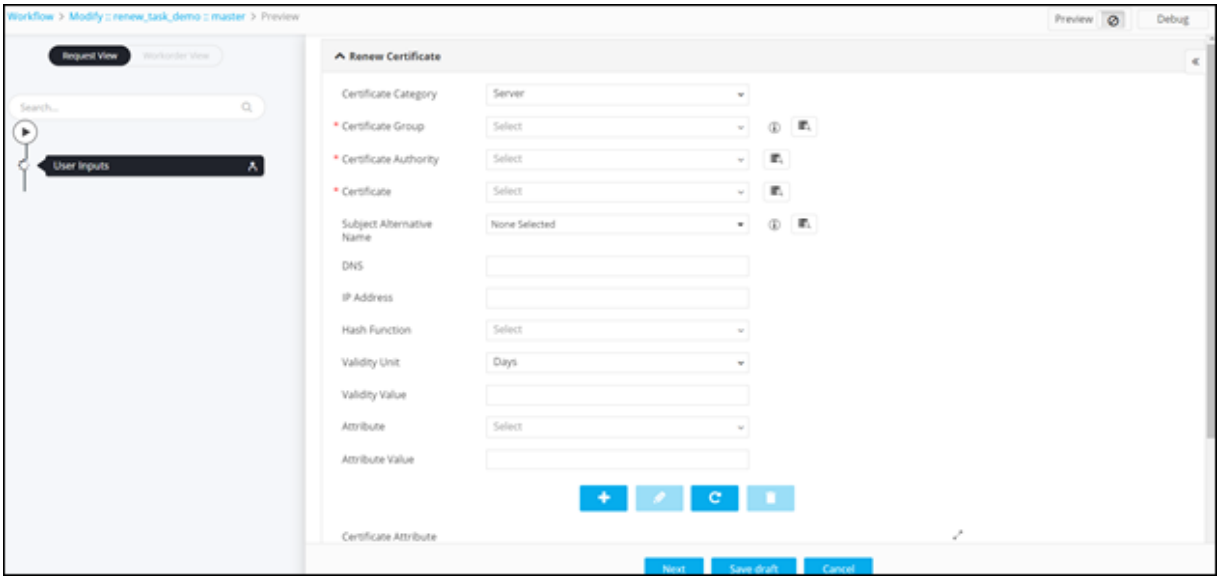
12. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.



13. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.



The **User Inputs** form is displayed on the screen.



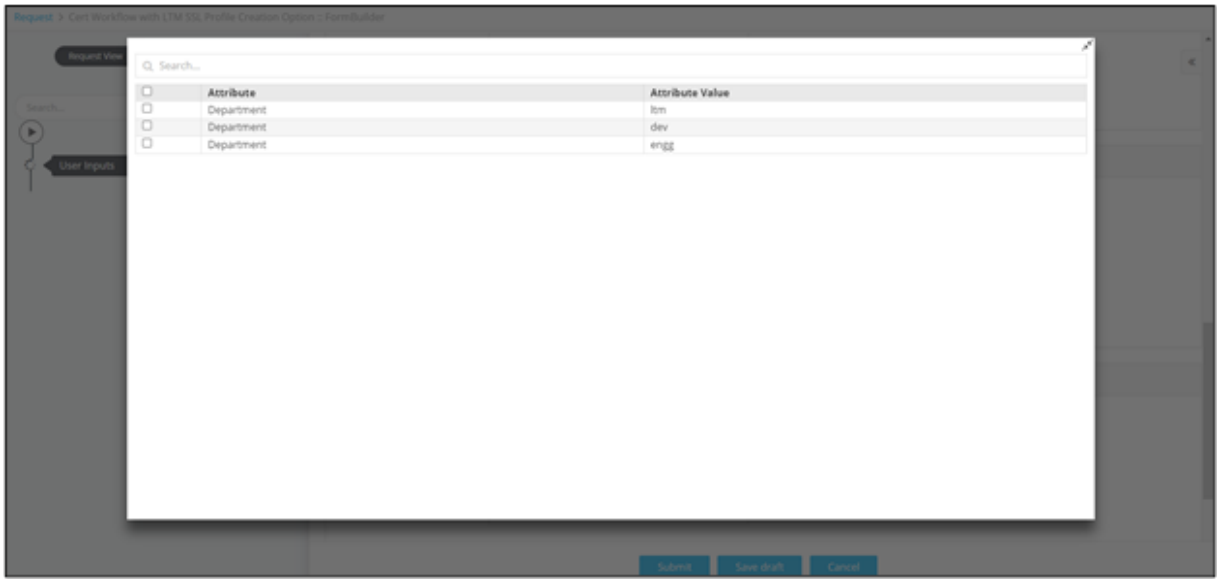
The following table describes the fields in the **User Inputs** form:

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.

Field	Description
	Note: To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
Validity Unit	Select the **Validity Unit** from the options available in the dropdown.
Validity Value	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

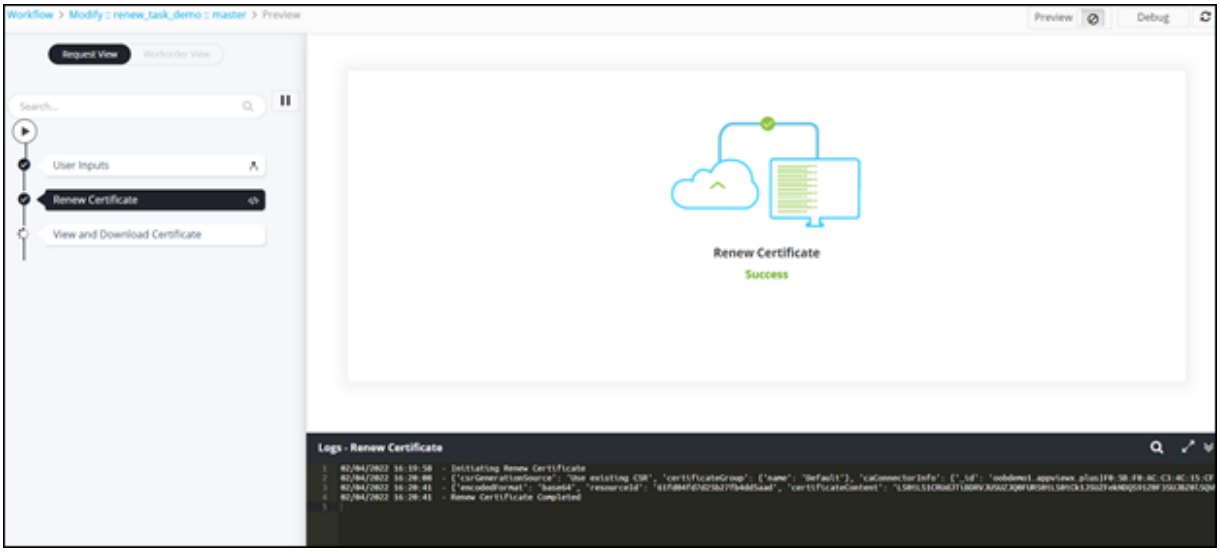
14. To add this attribute to the **Certificate Attributes** grid, click .
15. To edit the value of a particular attribute, select the attribute in the grid and click .

16. Enter the new value for the attribute in the **Value** field and click  again to update the value.
17. To delete a certificate attribute, select the attribute in the grid and click  .
18. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .

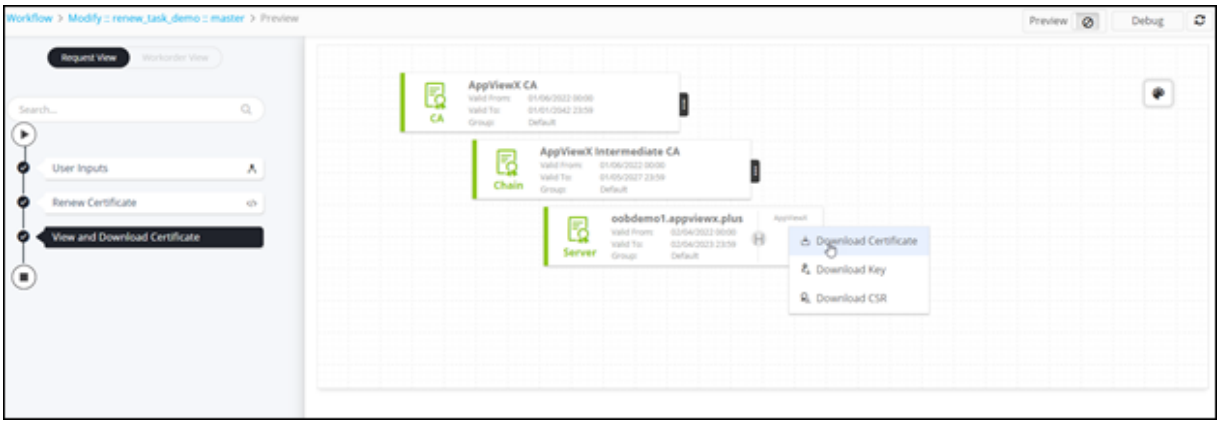


19. To search for a particular attribute in the grid, type the keyword(s) in the search field.
20. Click **Next**.

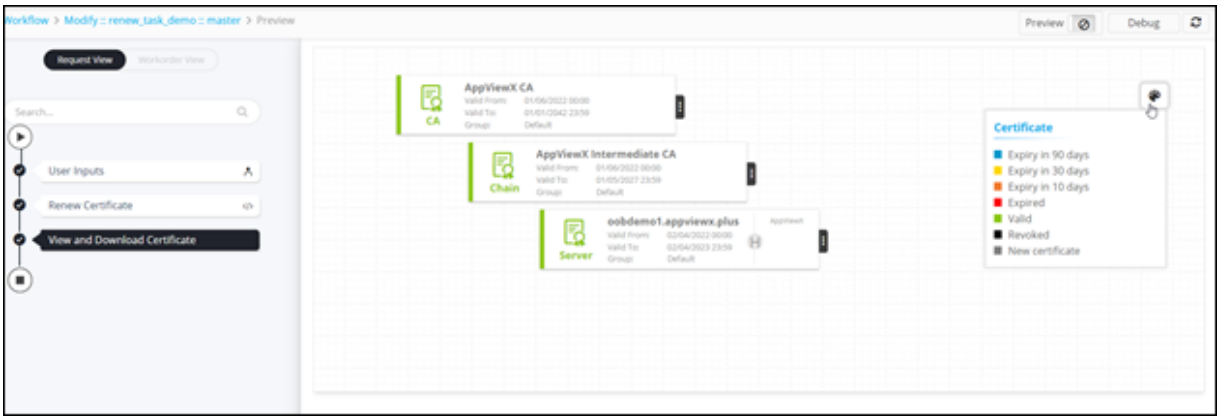
    Certificate renewed successfully.



21. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



22. Hover your mouse over  to view the **Certificate status**.

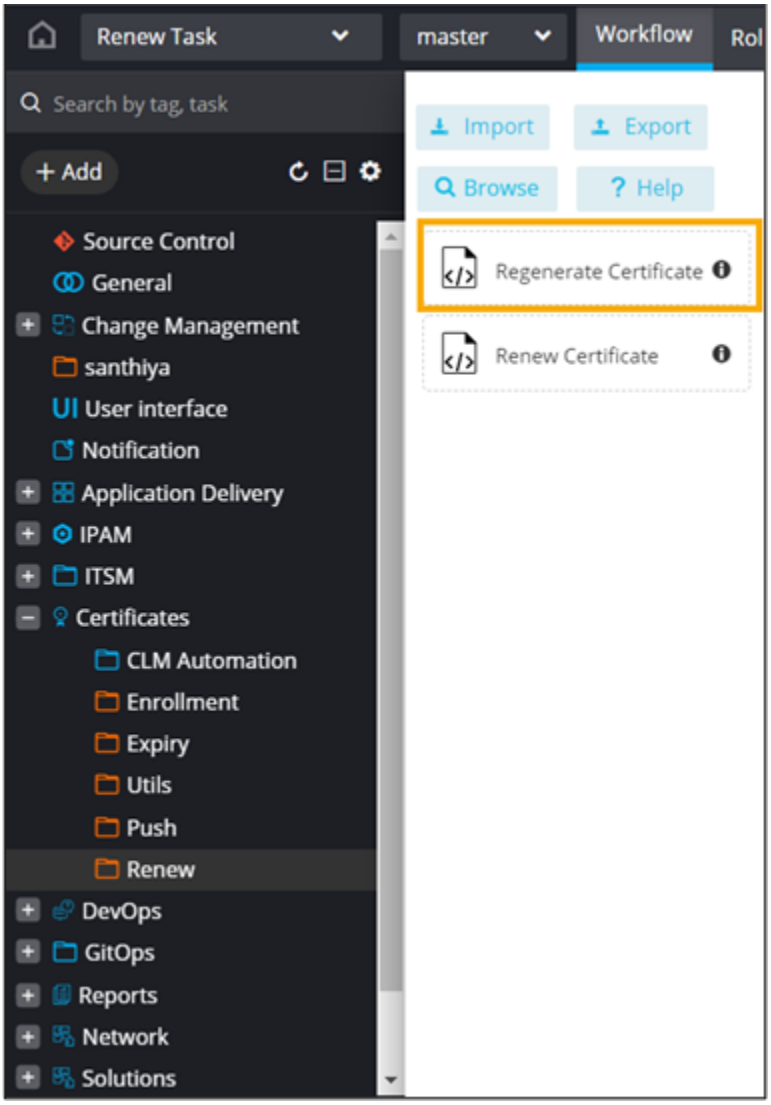


23. Click on the renewed certificate to view the **Certificate Details**.

Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

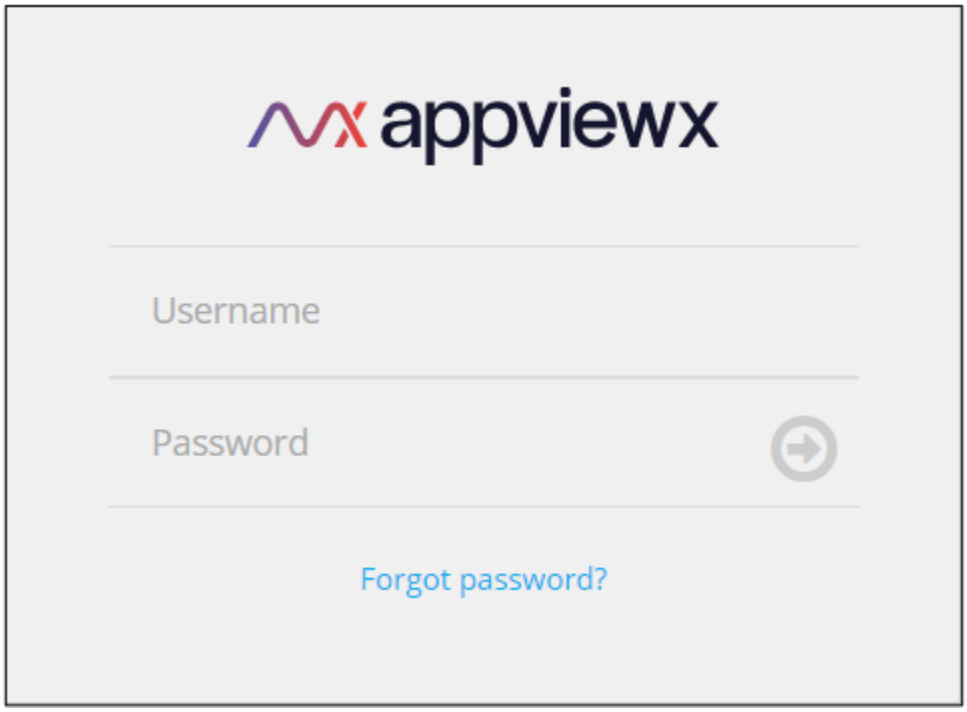
Regenerate Task

The OOB script task for regenerating certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.

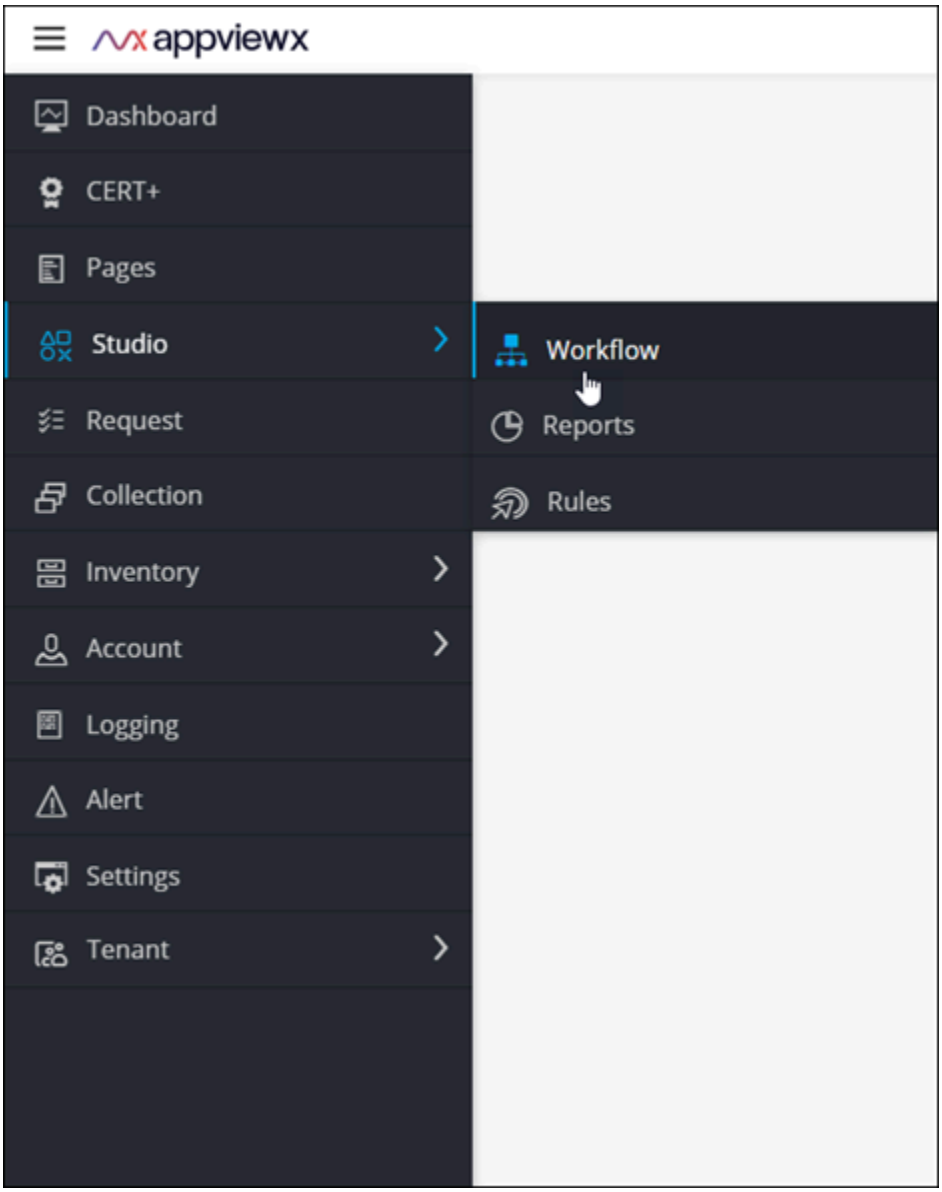


To design a custom workflow using the **Regenerate** task:

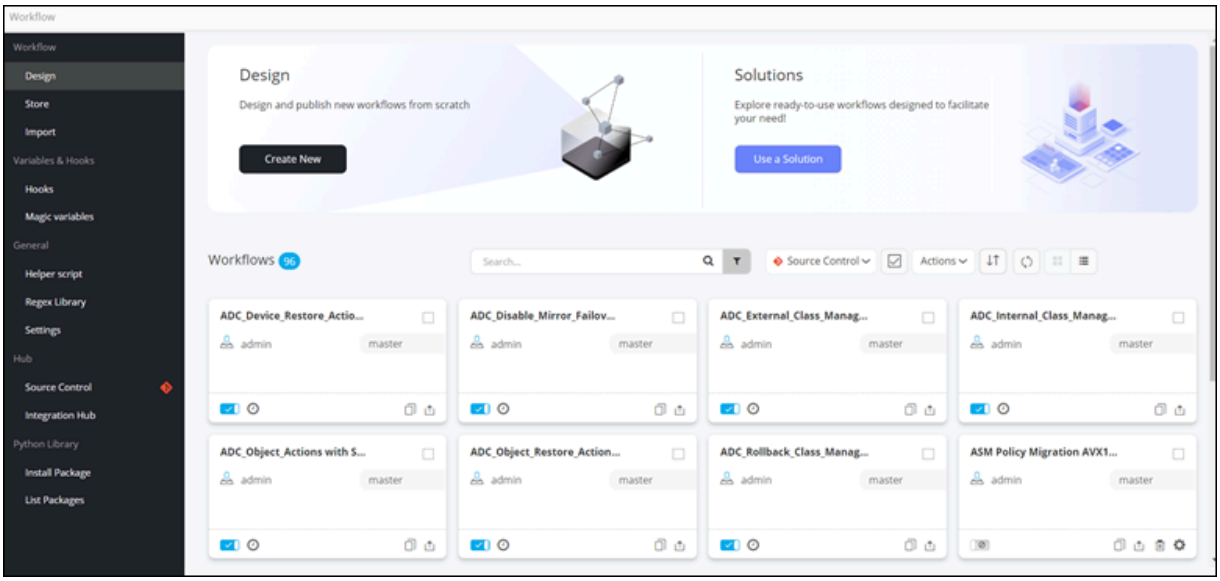
1. Log into AppViewX with valid credentials.



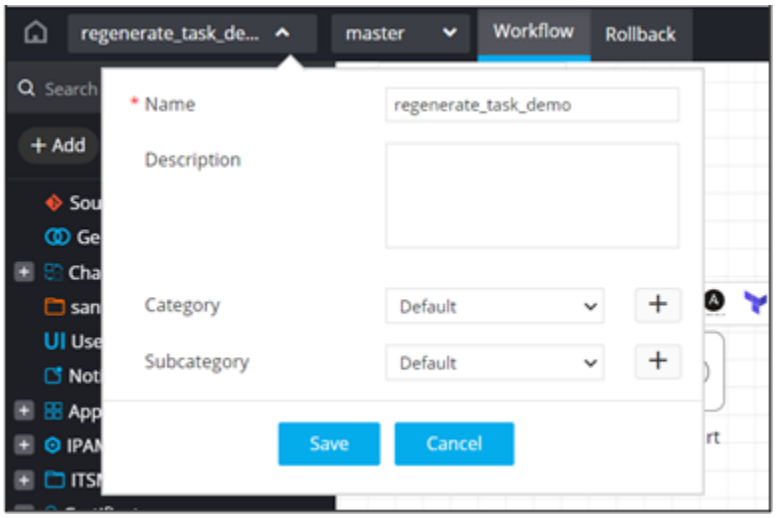
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



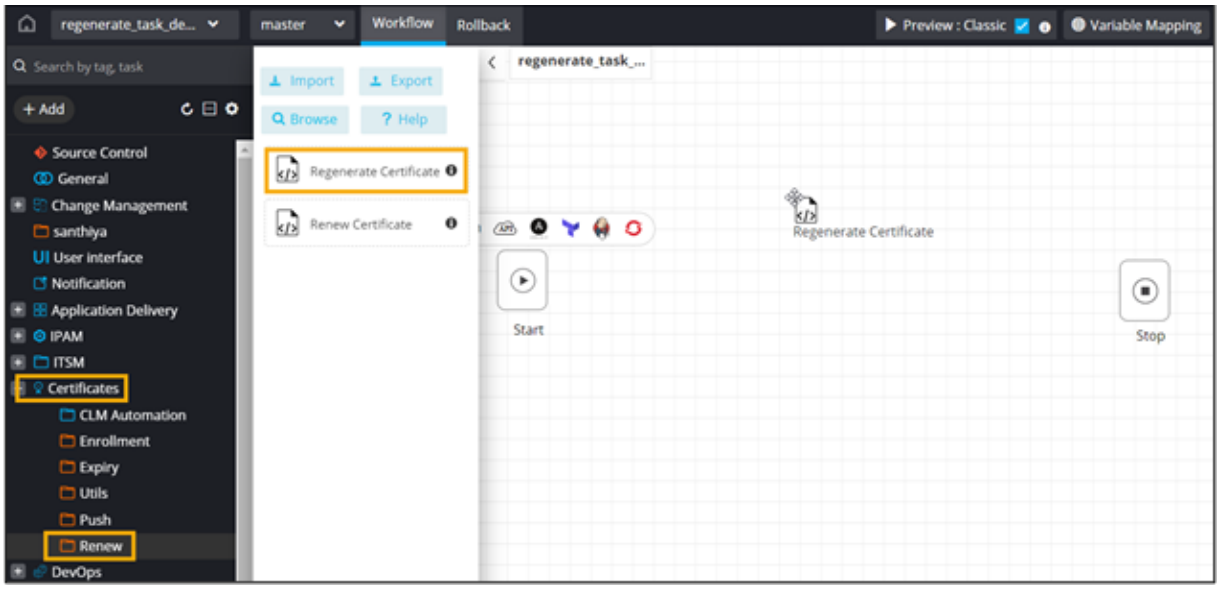
The **Workflow** inventory page is displayed.



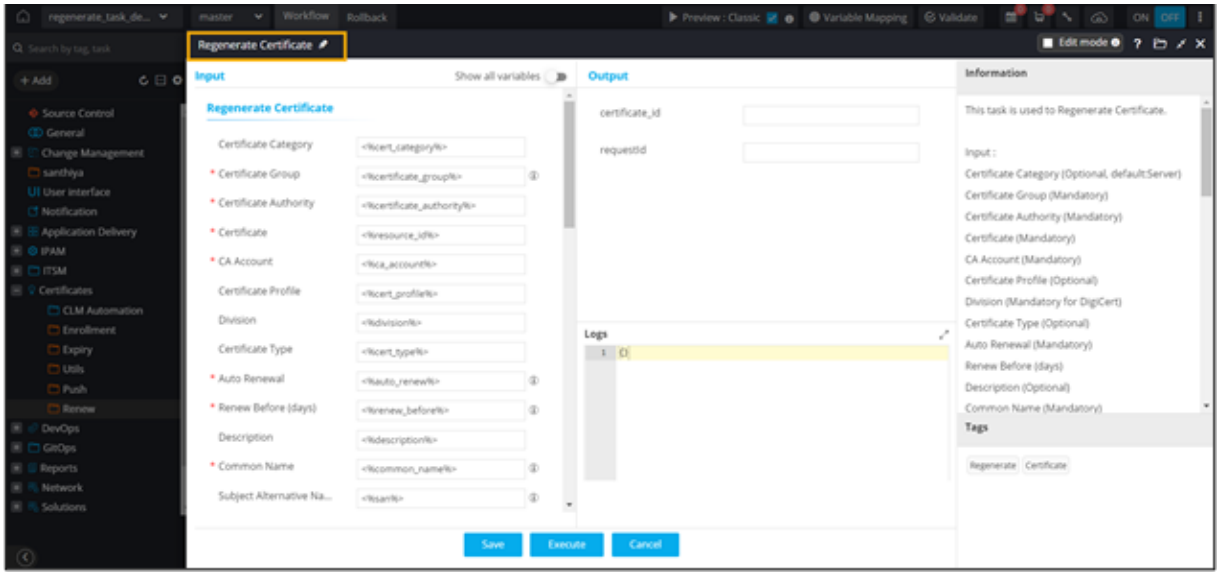
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



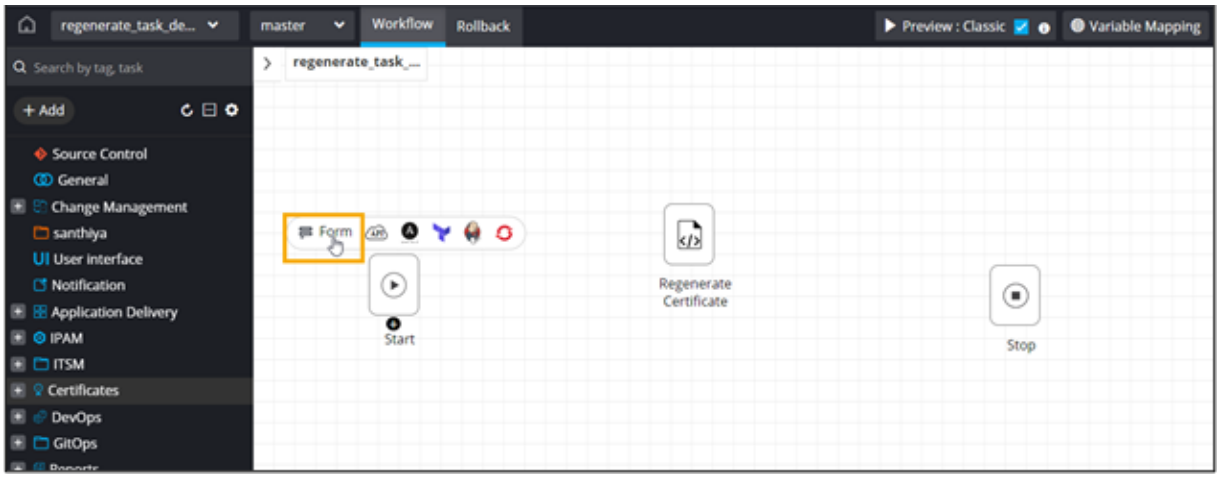
7. From the **Certificates** folder, under **Renew**, drag and drop the **Regenerate Certificate** task.



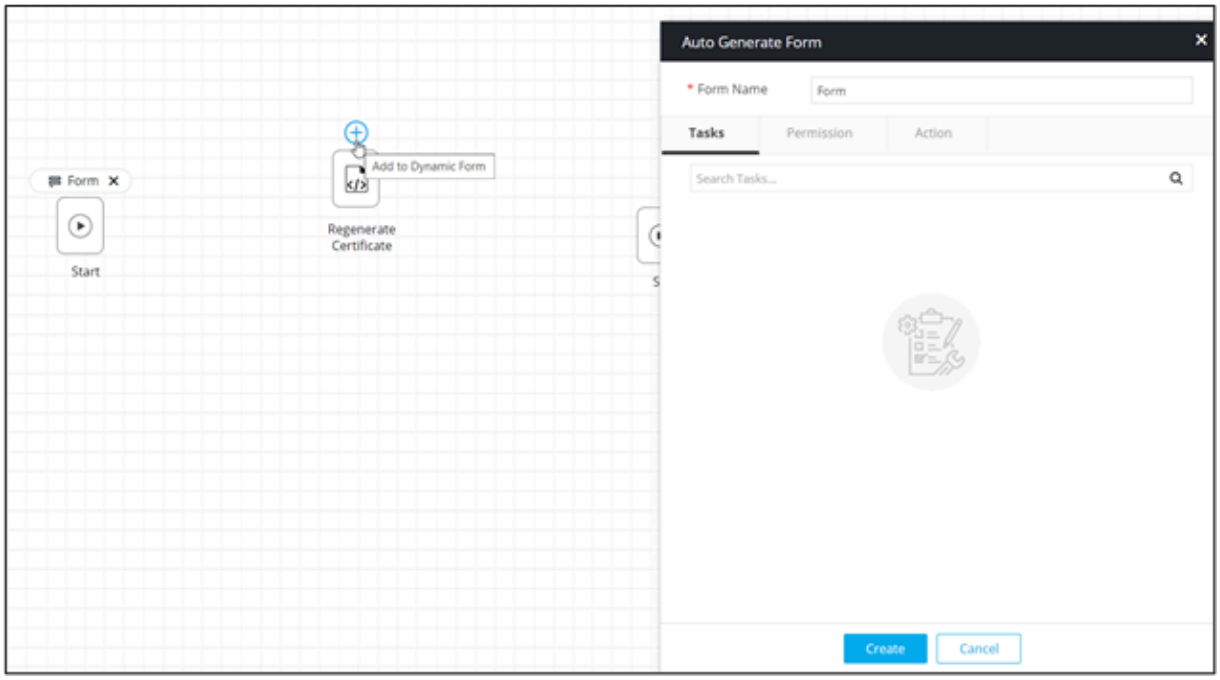
This task can be used to regenerate certificates.



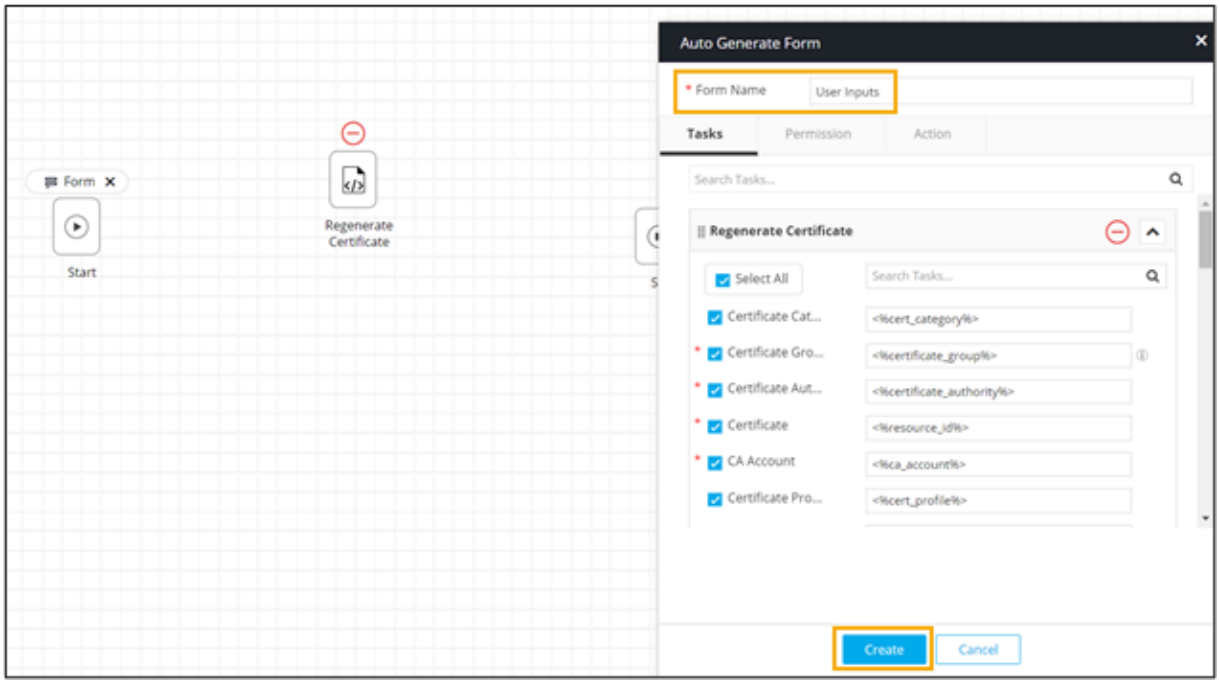
8. To auto-generate a form for this workflow, click **Form** above the **Start** task.



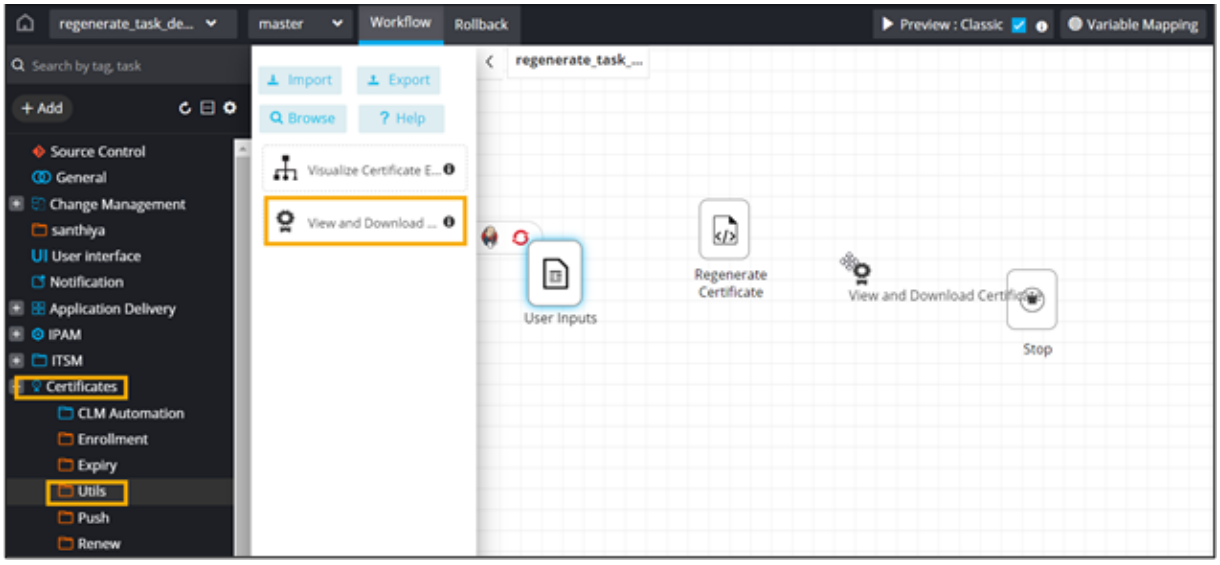
9. Click ⊕ above the **Regenerate Certificates** task to auto-populate the form fields.



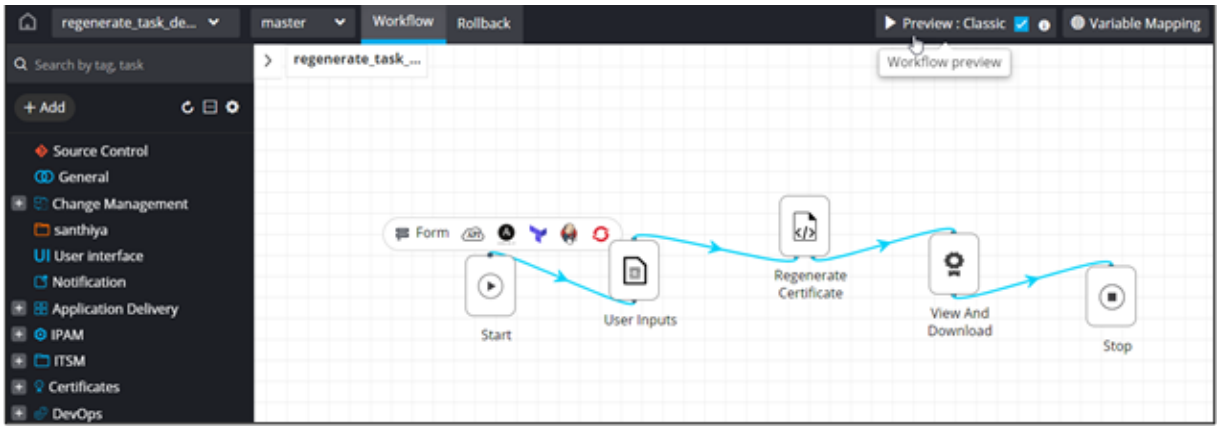
10. Select the fields required in the input form.
11. Provide a **Form Name** and click **Create**.



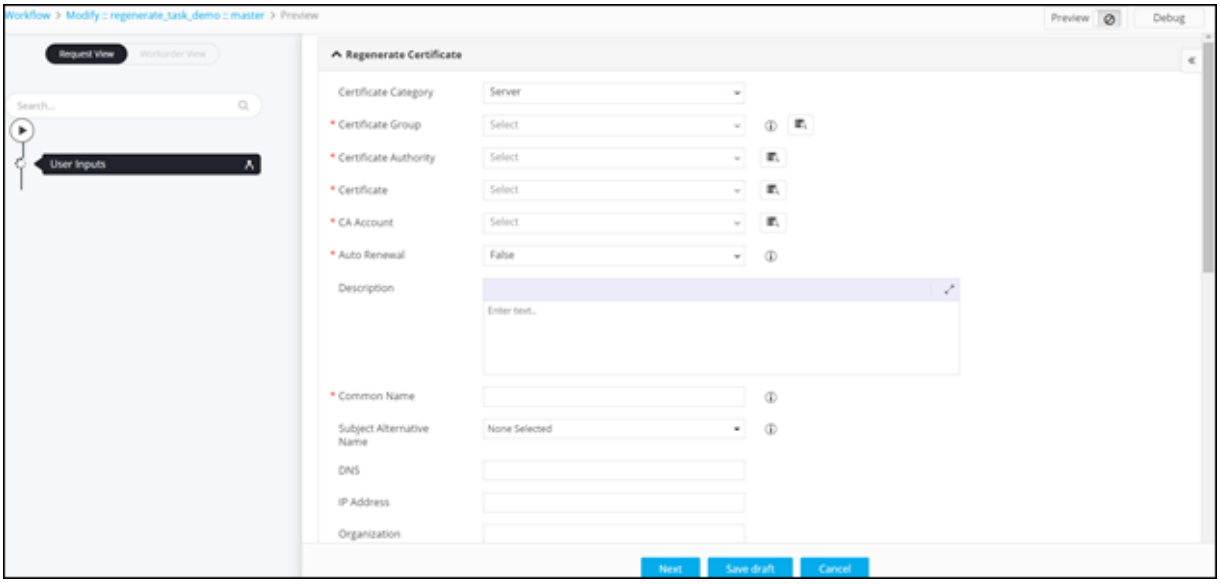
12. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.



13. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.



The **User Inputs** form is displayed on the screen.



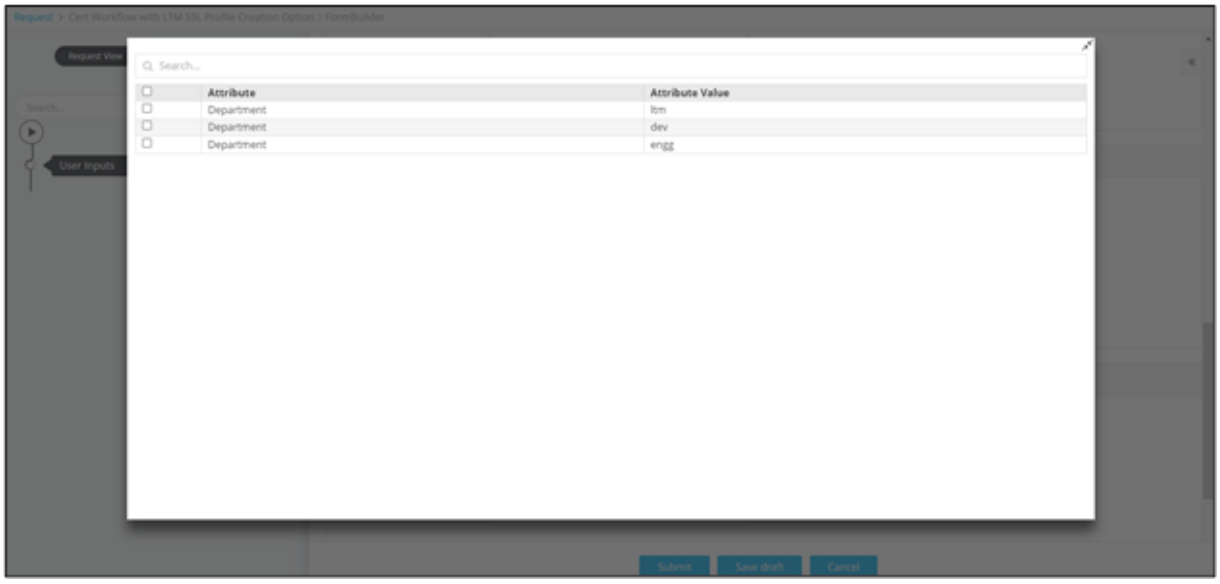
The following table describes the fields in the **User Inputs** form:

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the CA Account field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Description	Provide a description for the regenerated certificate.
***Common Name**	This field is populated on the basis of the certificate selected.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
City	Enter the name of the city in which the organization is located.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.

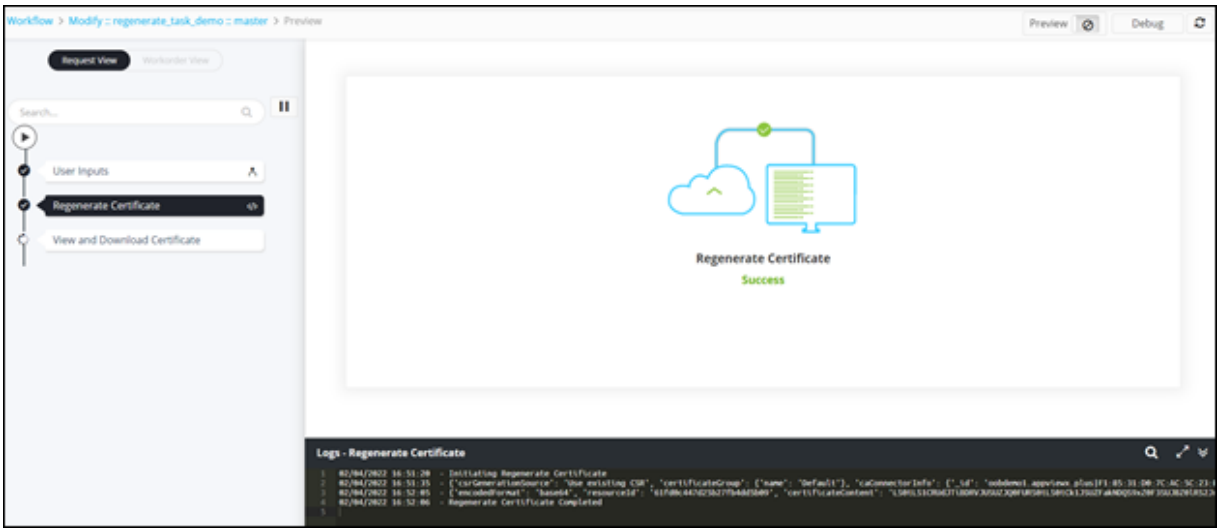
Field	Description
Email Address	Enter the email address associated with the organization.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type**from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.  **Note:** To retrieve the values in the Bit Length field, click  .
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

14. To add this attribute to the **Certificate Attributes** grid, click  .
15. To edit the value of a particular attribute, select the attribute in the grid and click  .
16. Enter the new value for the attribute in the **Value** field and click  again to update the value.
17. To delete a certificate attribute, select the attribute in the grid and click  .
18. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .

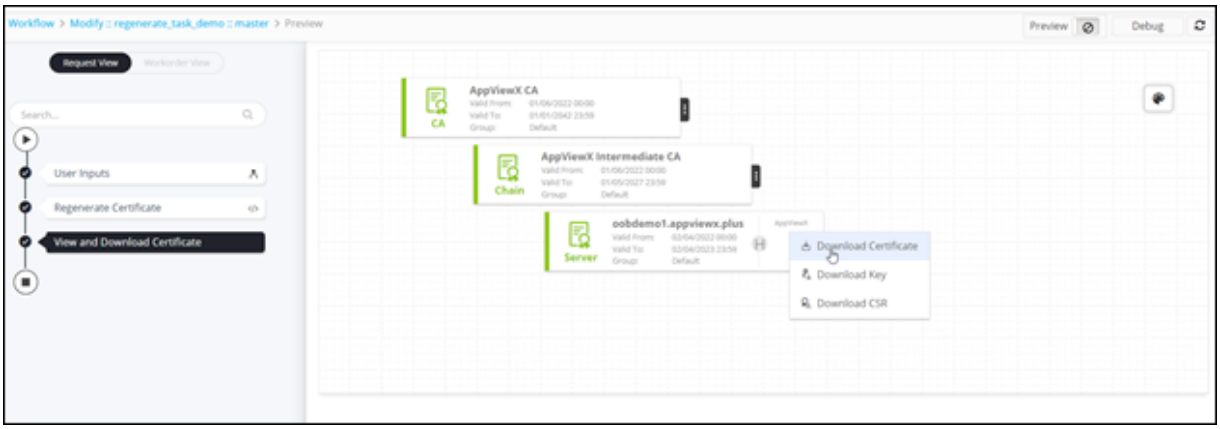


19. To search for a particular attribute in the grid, type the keyword(s) in the search field.
20. Click **Next**.

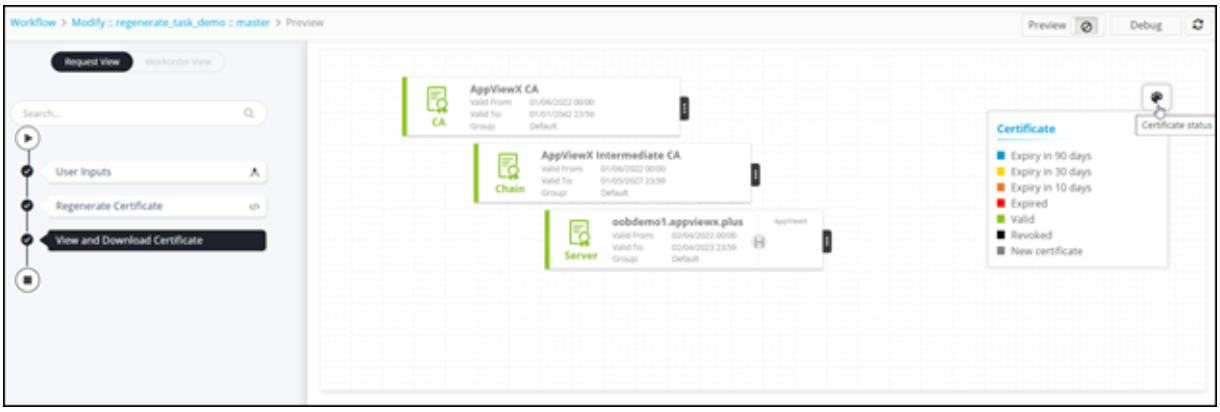
    Certificate regenerated successfully.



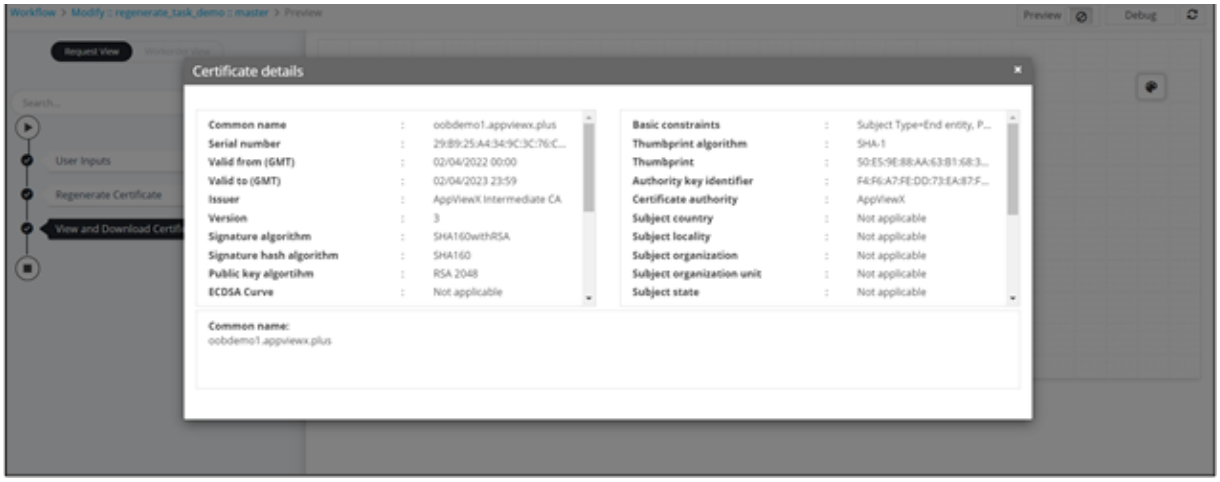
21. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



22. Hover your mouse over  to view the **Certificate status**.



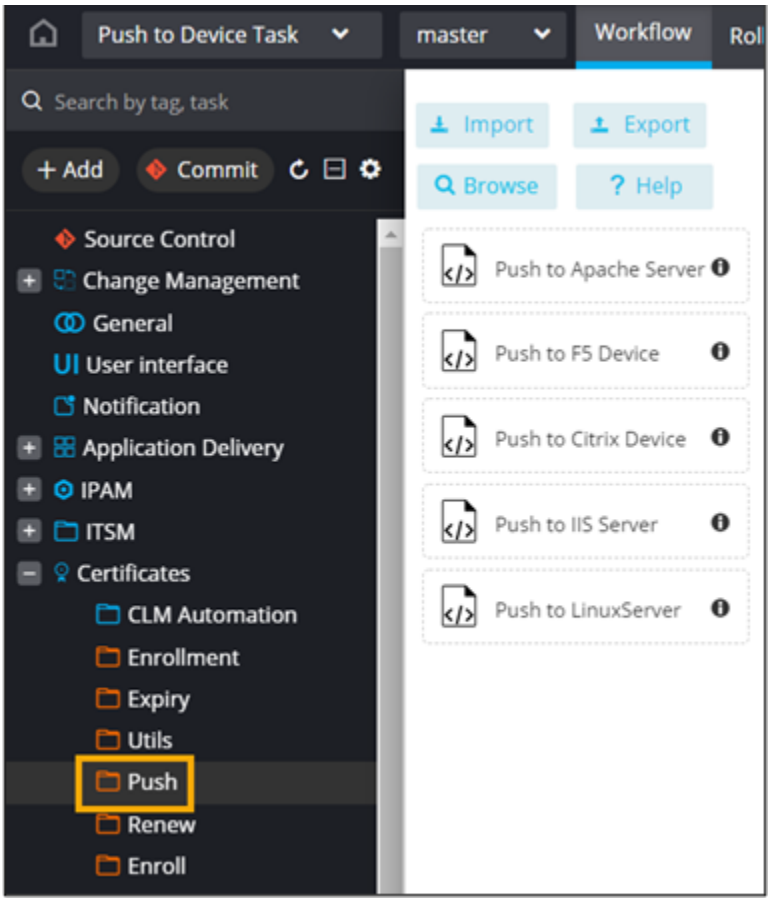
23. Click on the regenerated certificate to view the **Certificate Details**.



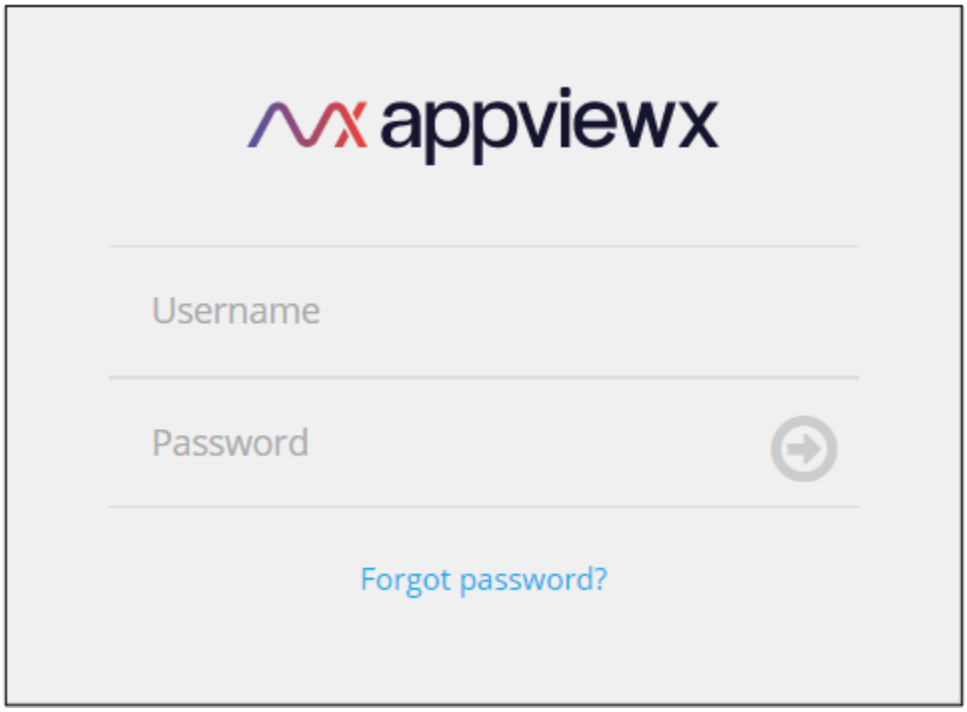
Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

Push Tasks

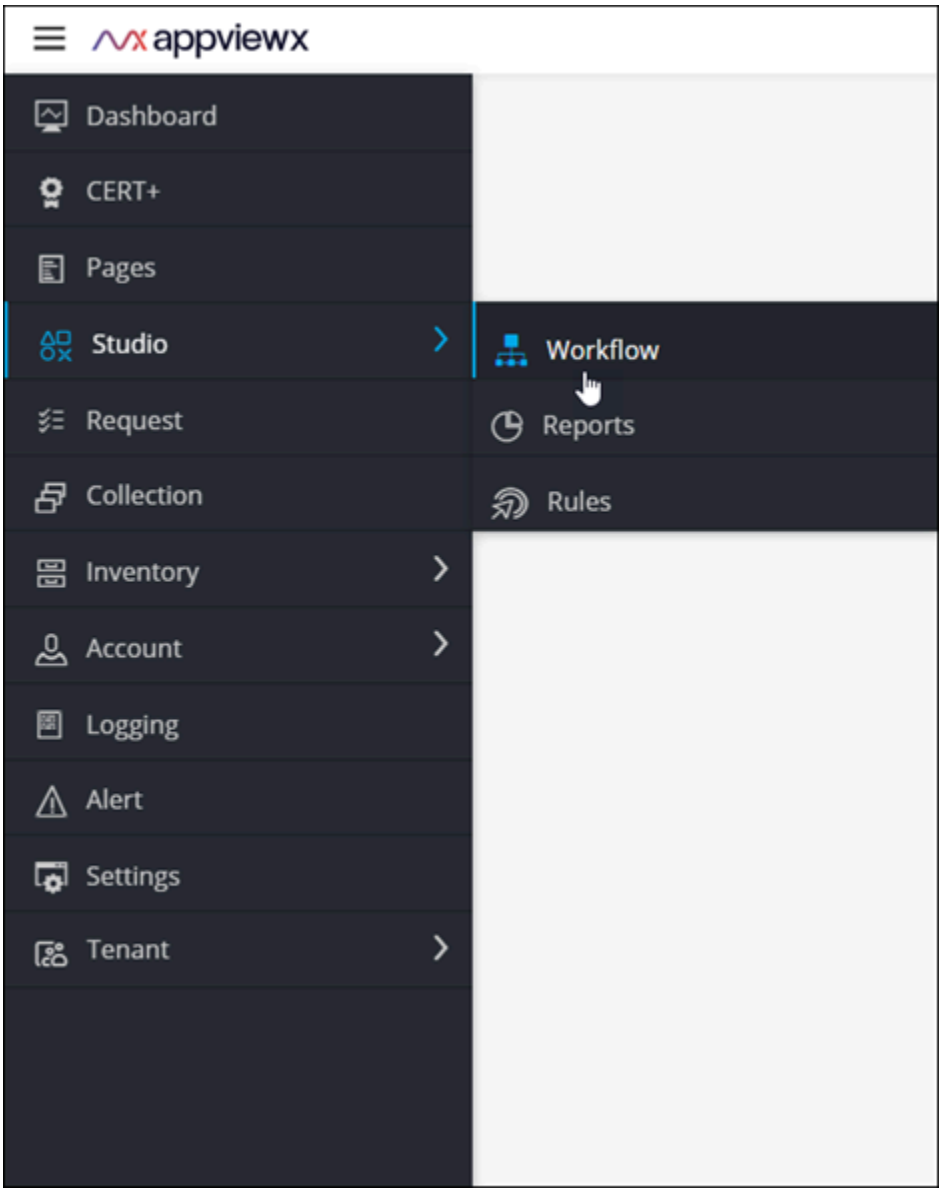
You can design a custom workflow for pushing a certificate to a device(s) or a server(s) using the prebuilt Push tasks available in the **Workflow Studio**. The OOB script task for pushing certificates to devices/ servers can be found under **Certificates**, in the **Push** folder.



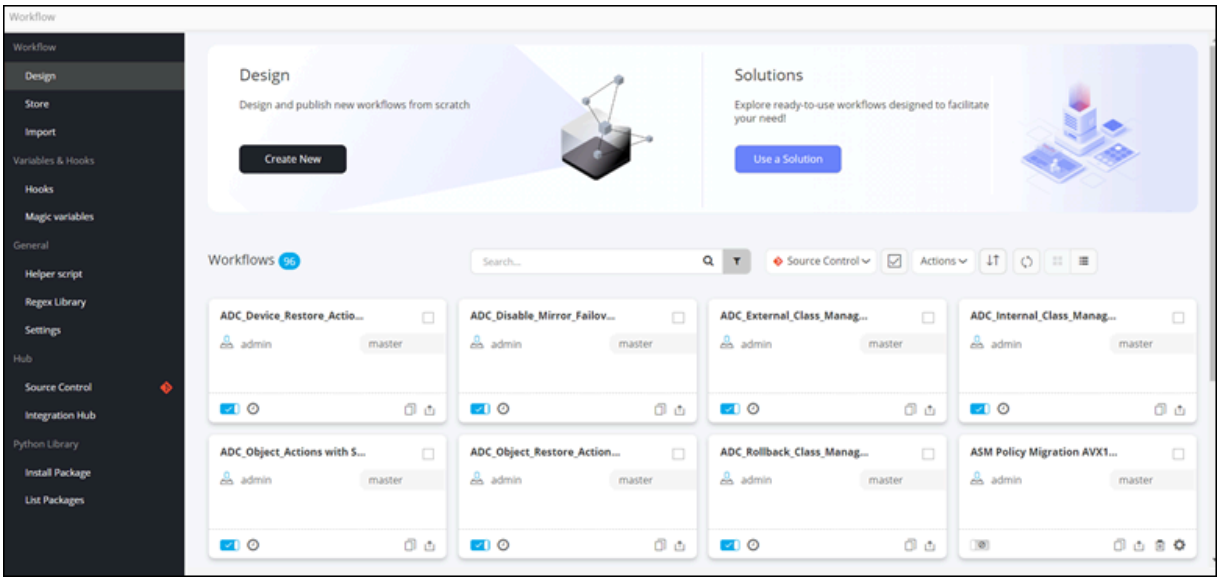
1. Log into AppViewX with valid credentials.



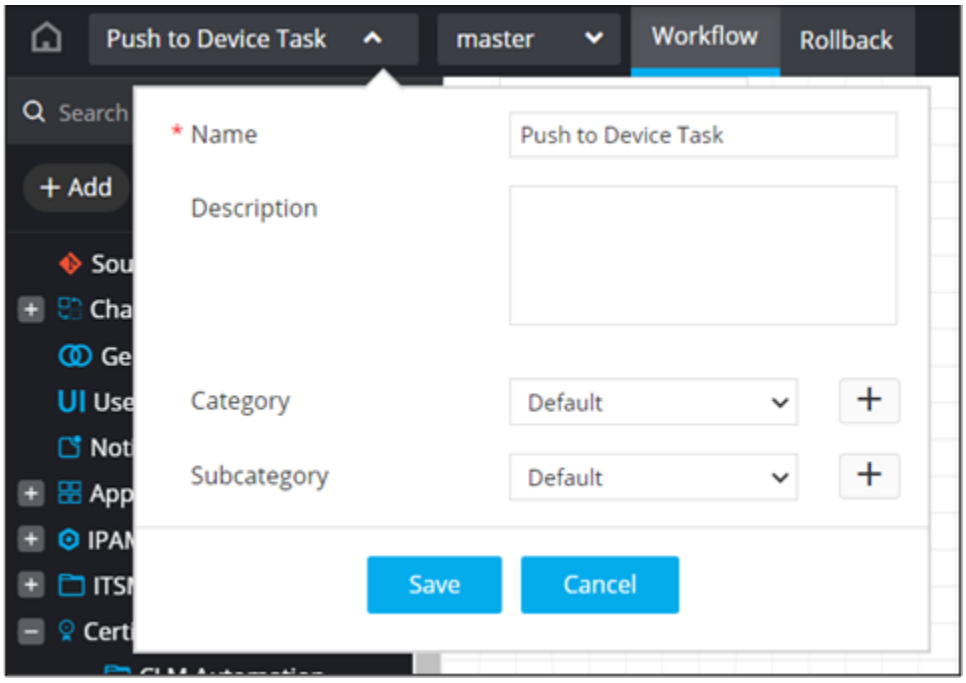
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



The **Workflow** inventory page is displayed.



4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



7. From the **Certificates** folder, click **Push**.

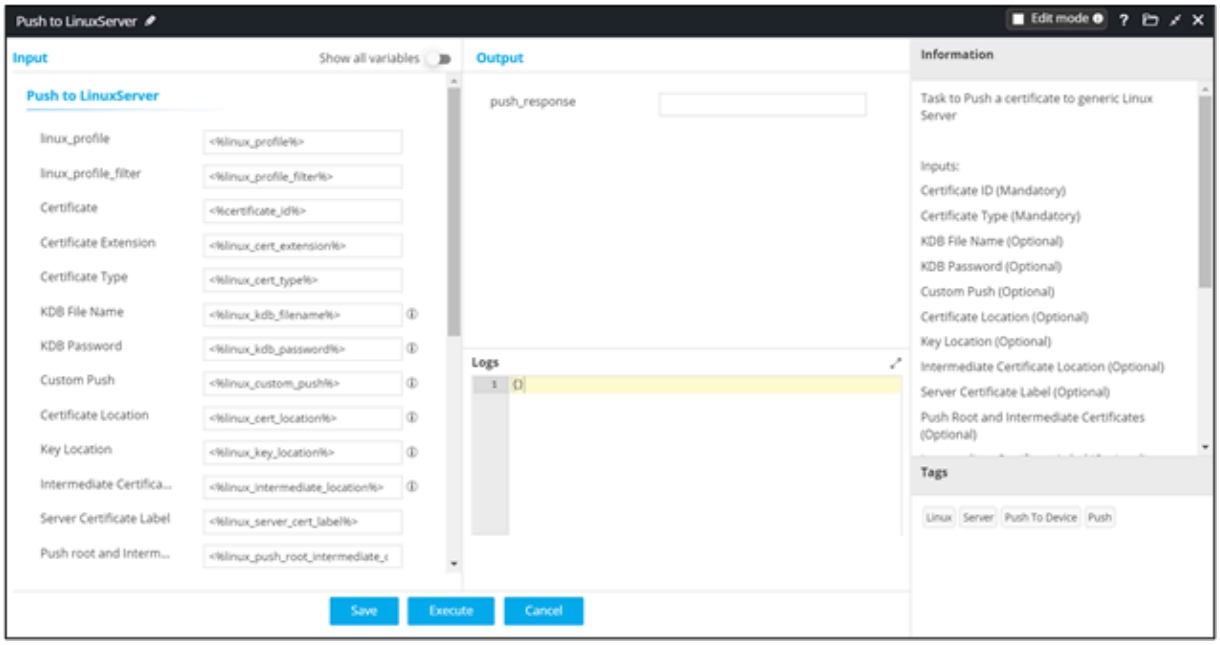
   The following tasks for pushing certificates are available in the **Push** folder:

   • Push to Apache Server

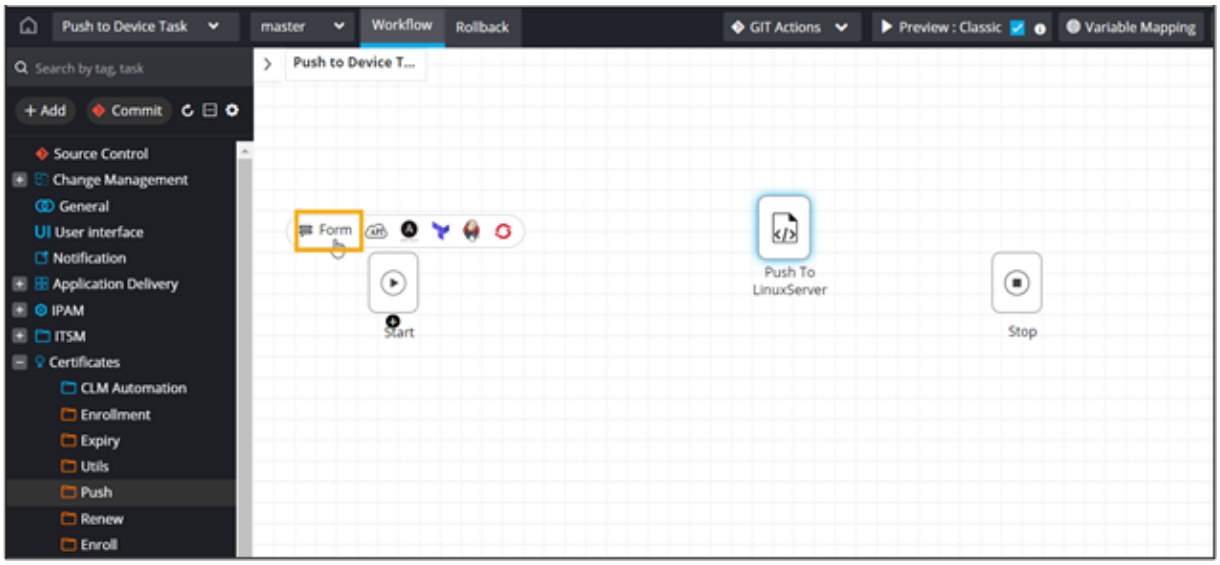
   • Push to F5 device

- Push to Citrix Device
- Push to IIS Server
- Push to Linux Server

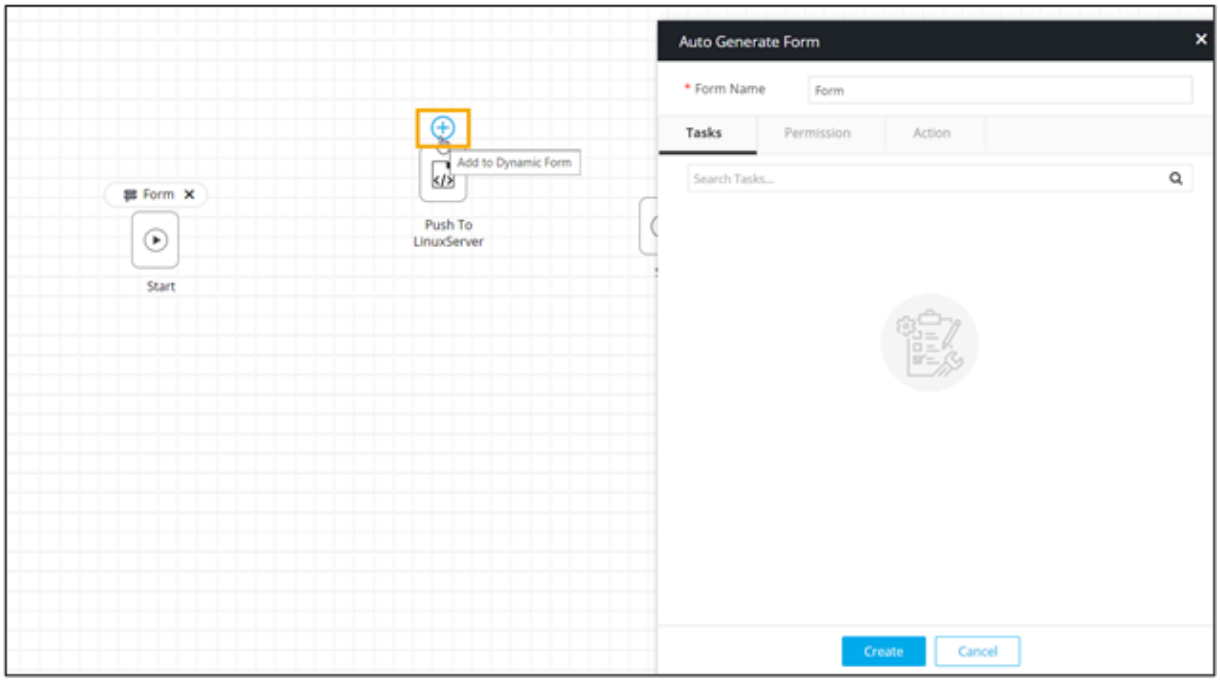
8. From the **Push** folder, drag and drop any of the Push tasks. For example, the **Push to Linux Server** task.



9. Click **Save**.
10. To auto-generate a form for this workflow, click **Form** above the **Start** task.

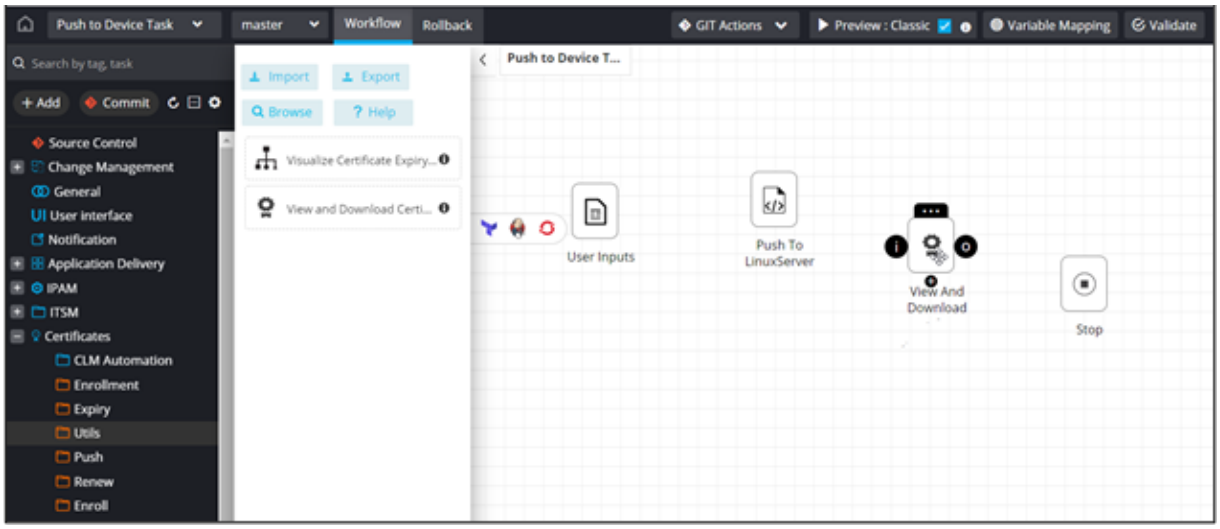


11. Click ⊕ above the **Push to LinuxServer** task to auto-populate the form fields.

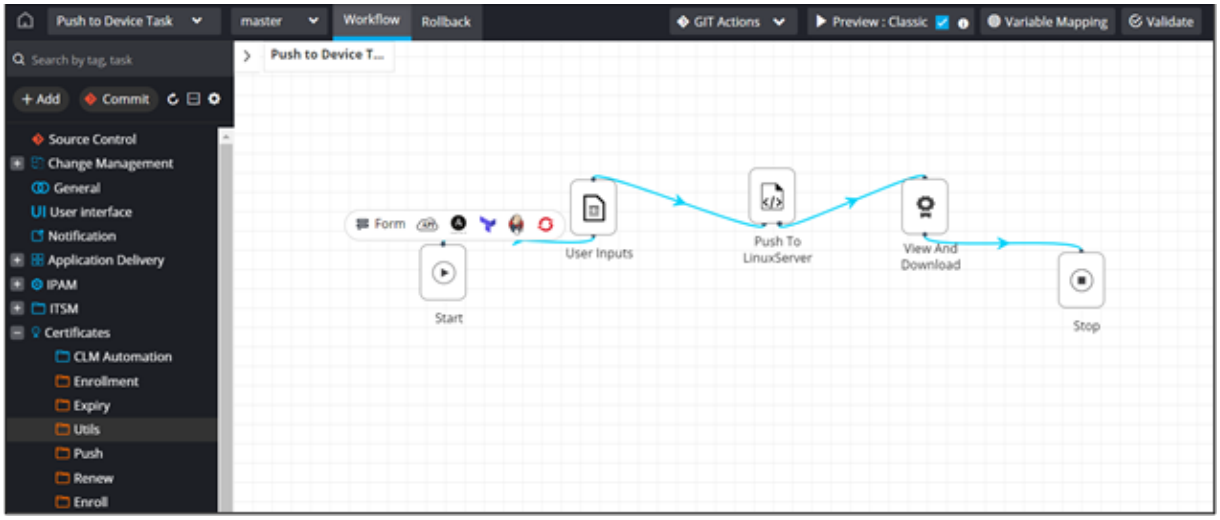


12. Select the fields required in the input form.
13. Provide a **Form Name** and click **Create**.

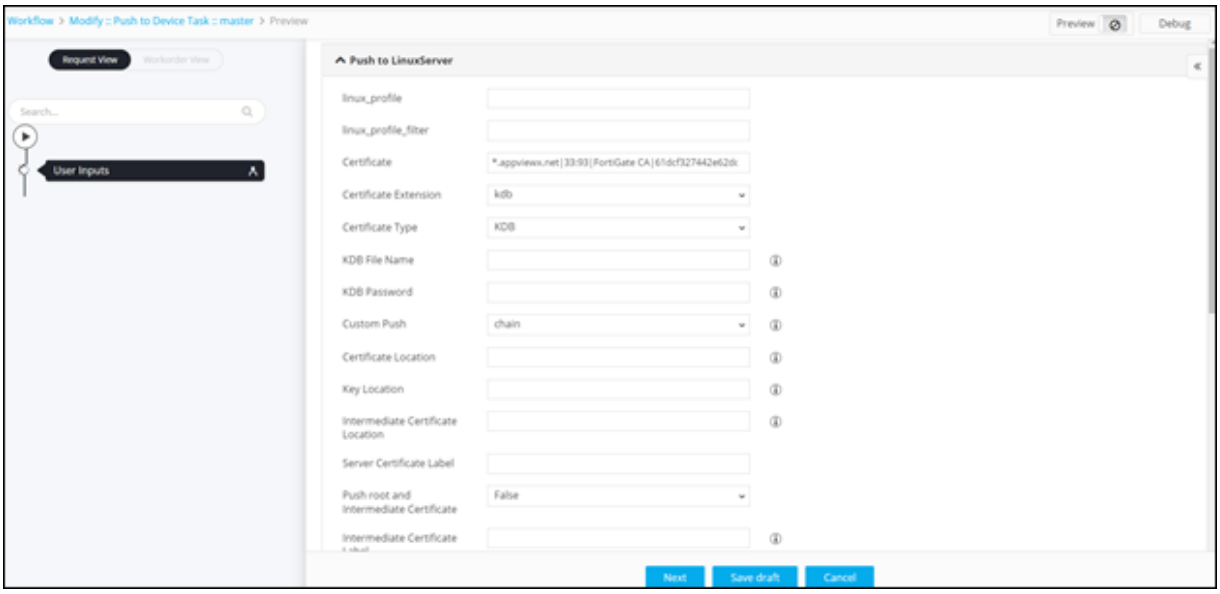
14. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.



15. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.



User Inputs form when the **Push to LinuxServer** task is selected is displayed.



Note: The fields displayed in the User Inputs form will vary depending on the Push task selected from the Push folder while designing the workflow.

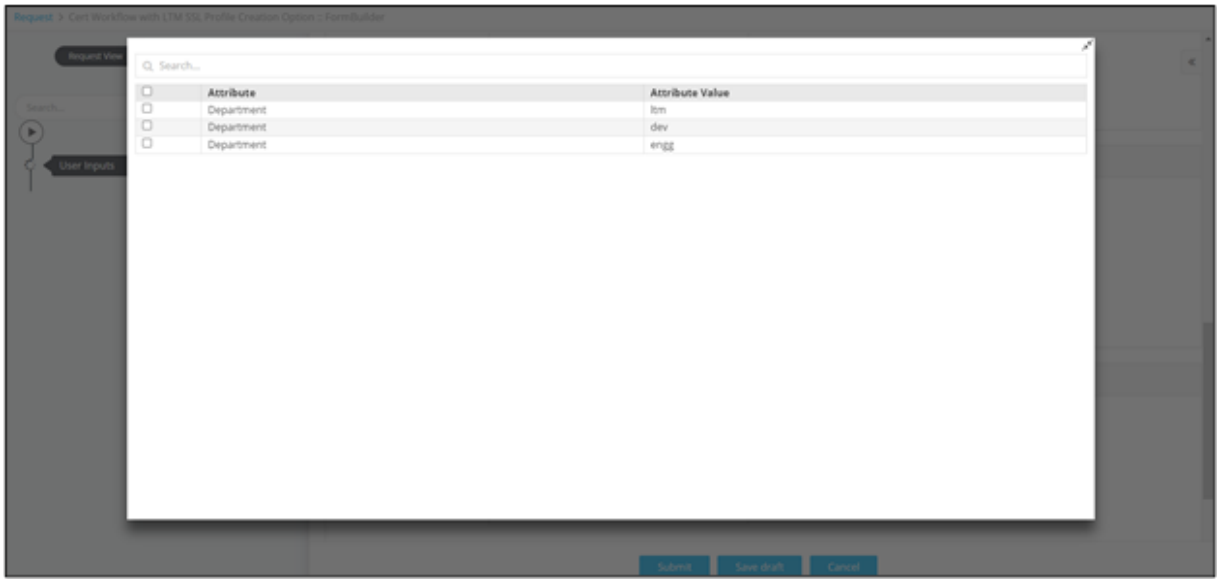
The following table describes the field information in the **User Inputs** form when the **Push to LinuxServer** task is selected:

Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note**: **Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX

Field	Description
	Note: This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note**: Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note**: This field is displayed only when the **Auto Renewal** field is enabled.
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter the Email Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.

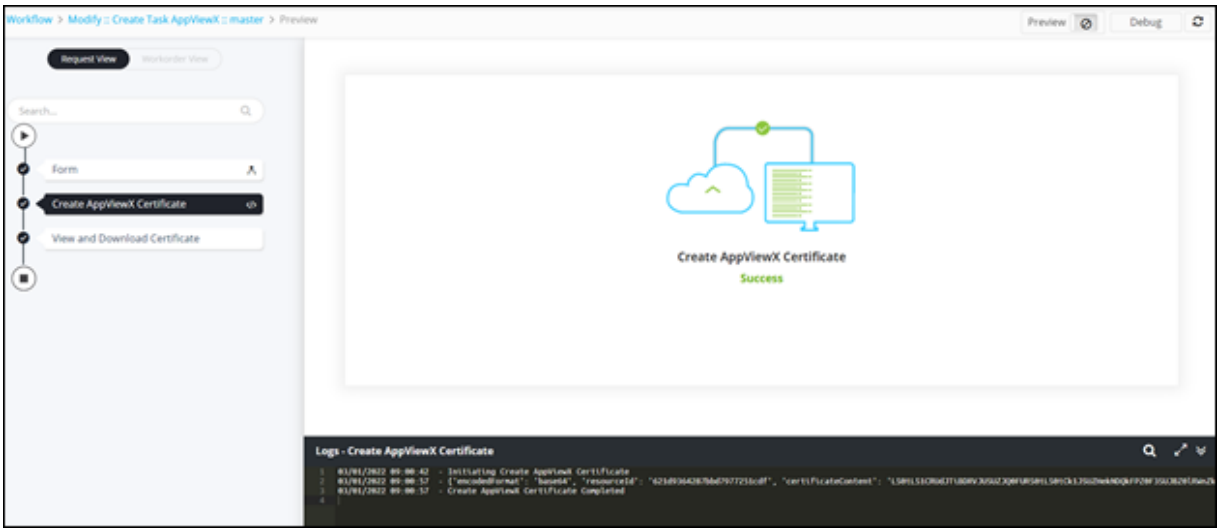
Field	Description
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown. **Note:** To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

16. To add this attribute to the **Certificate Attributes** grid, click .
17. To edit the value of a particular attribute, select the attribute in the grid and click .
18. Enter the new value for the attribute in the **Value** field and click again to update the value.
19. To delete a certificate attribute, select the attribute in the grid and click .
20. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .

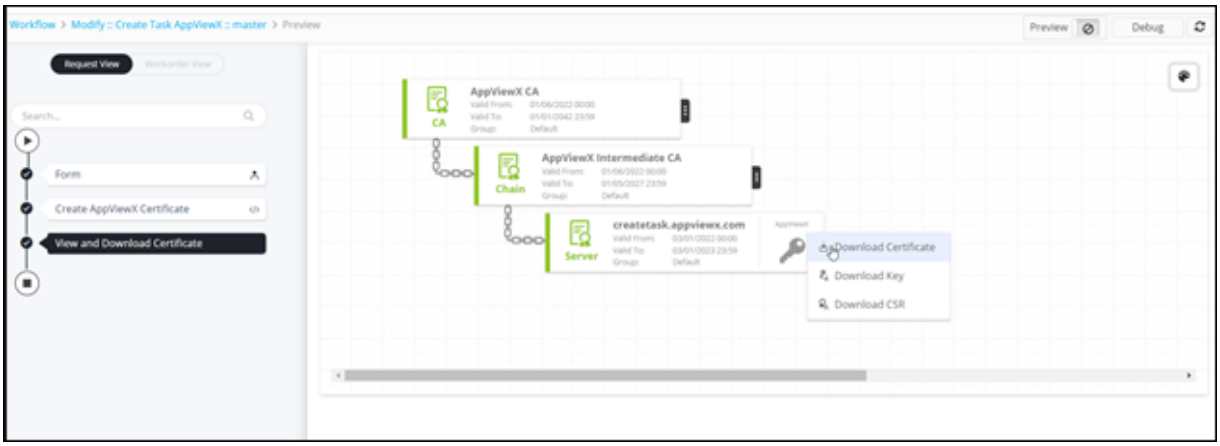


21. To search for a particular attribute in the grid, type the keyword(s) in the search field.
22. Click **Next**.

    Certificate created successfully.



23. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over  and from the options displayed, click **Download Certificate**.



24. Hover your mouse over  to view the **Certificate status**.

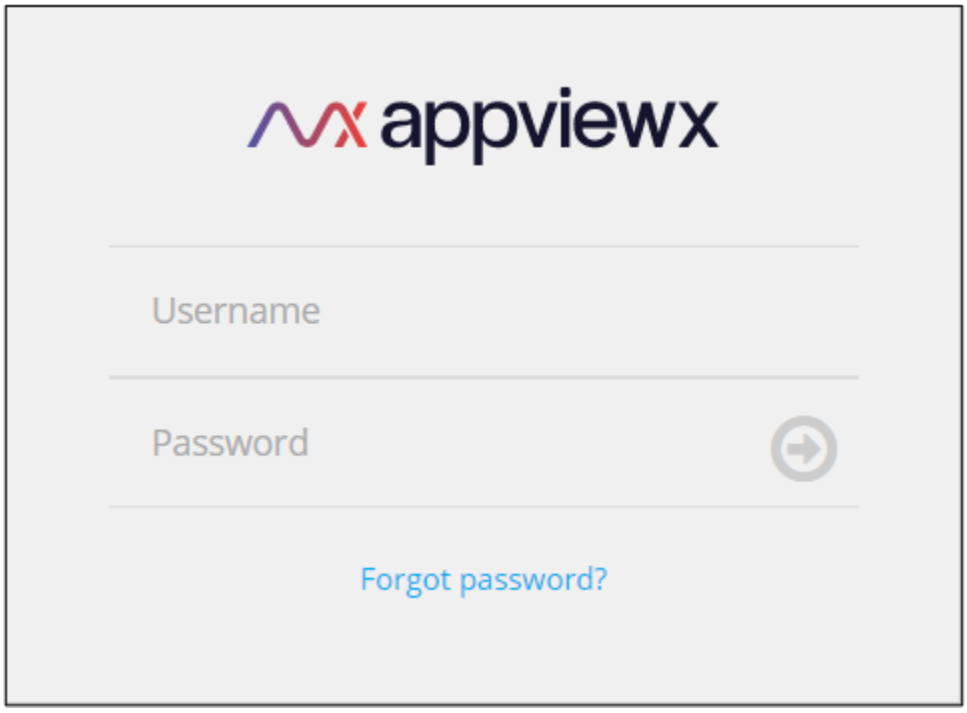
Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

Chapter 9: Designing a Custom Workflow using OOB Tasks

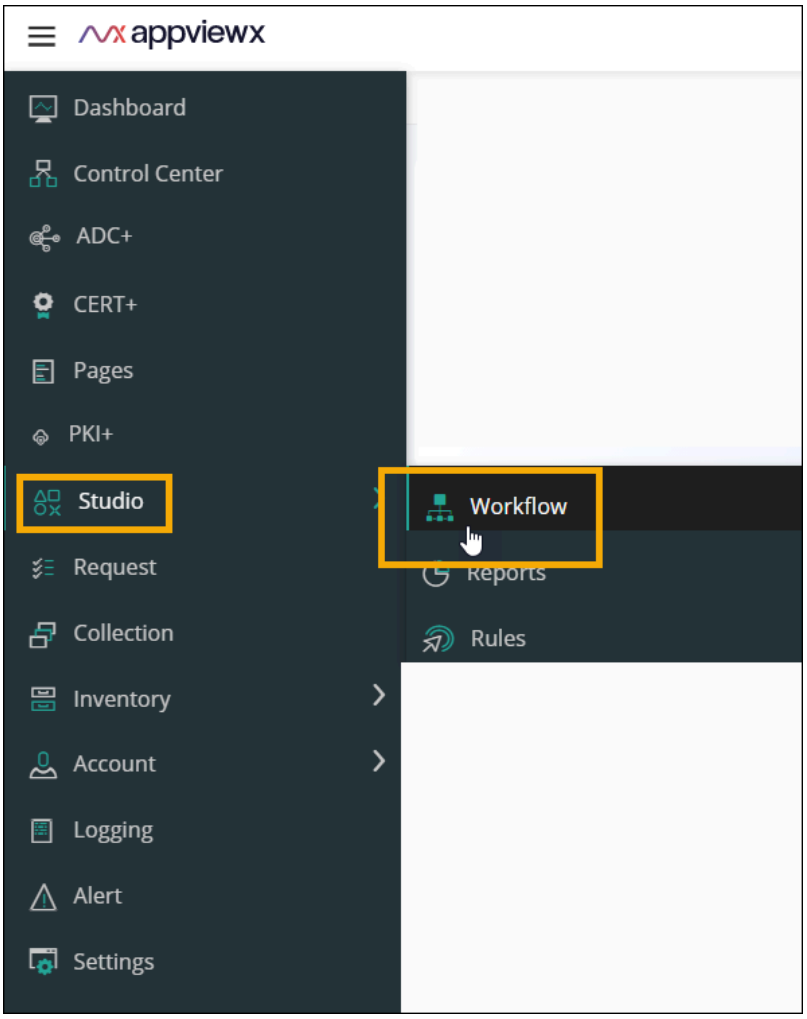
You can use the OOB tasks and subflows available in the Workflow Studio module to build custom workflows for enrolling and renewing certificates. You can also add the OOB Push to Device subflow to push the certificates to a selected device.

To design a custom workflow to enroll a certificate and push it to a device:

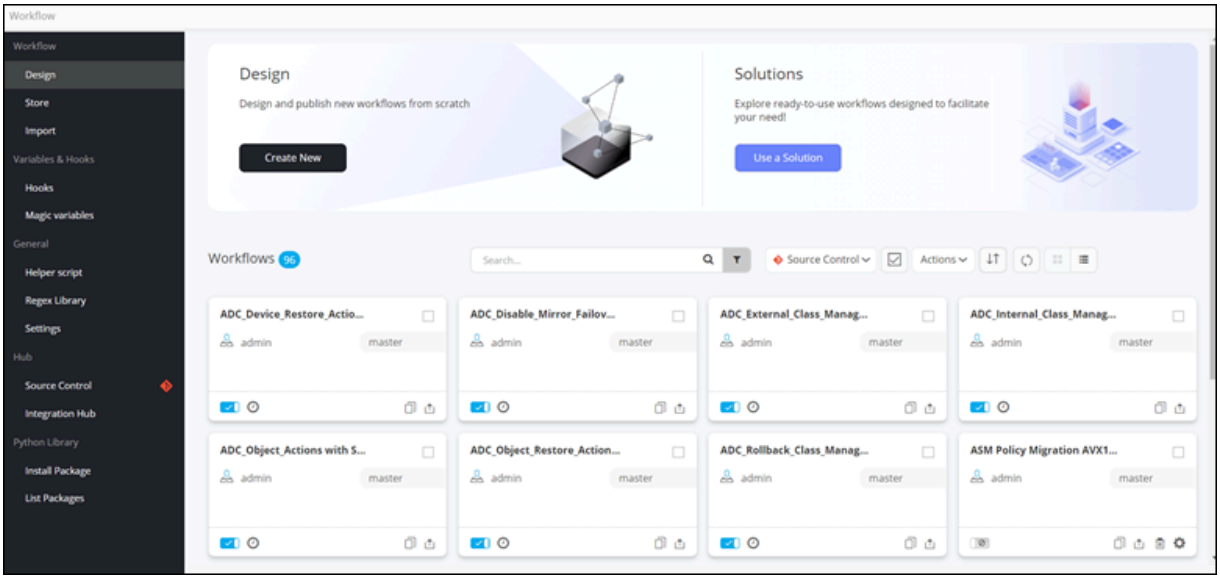
1. Log into AppViewX with valid credentials.



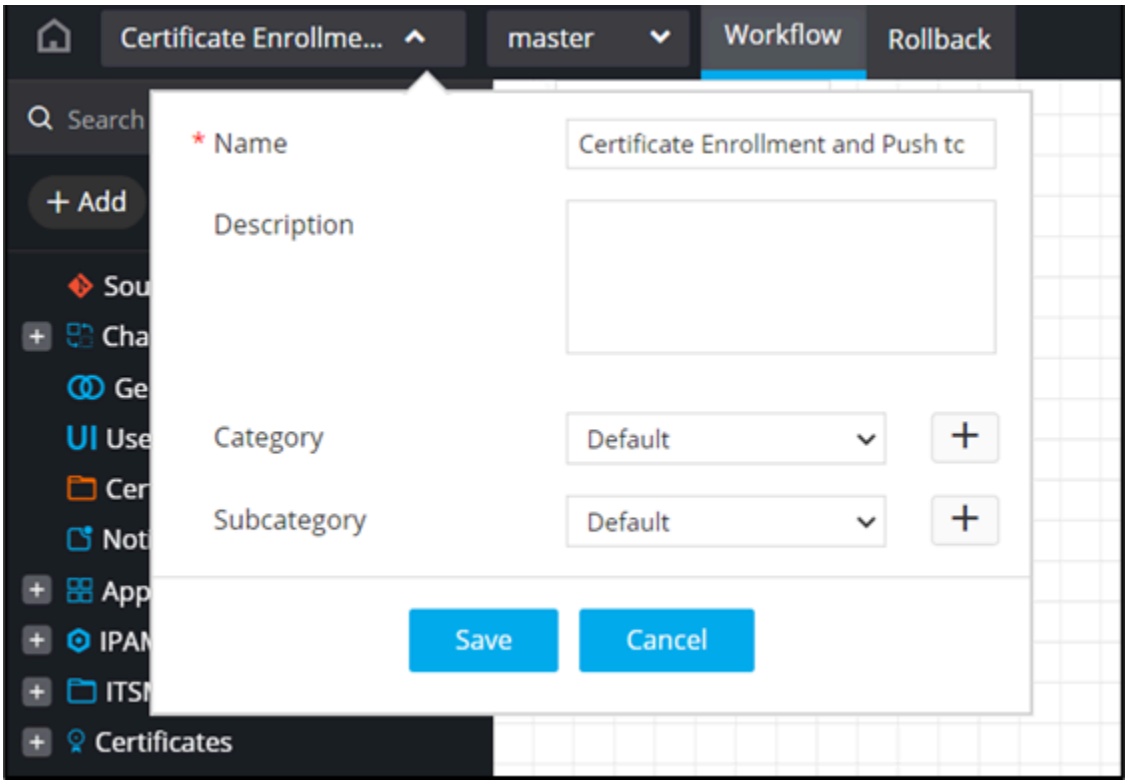
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Studio** > **Workflow**.



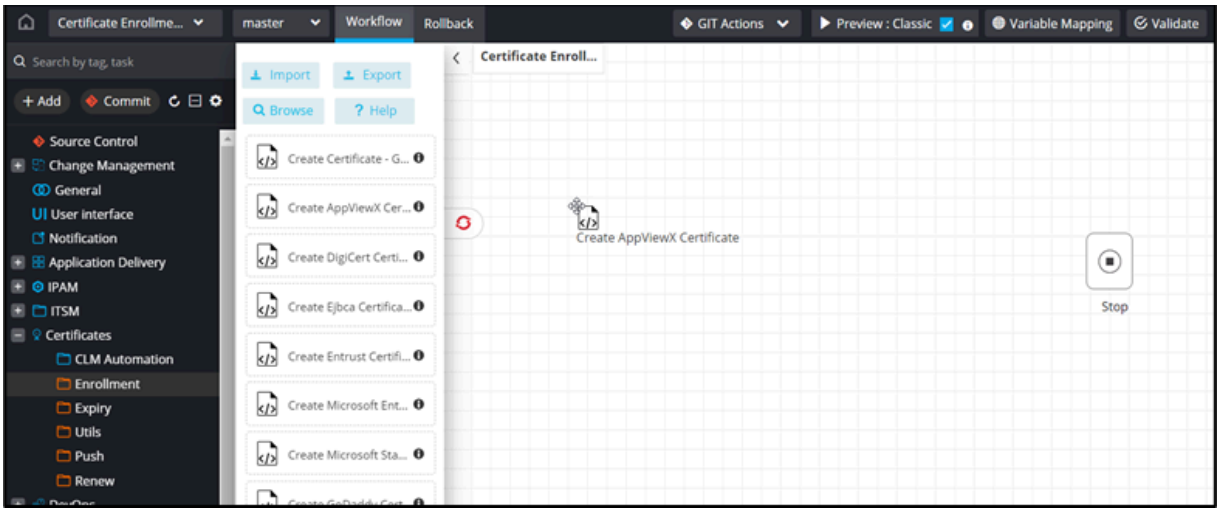
The **Workflow** inventory page is displayed.



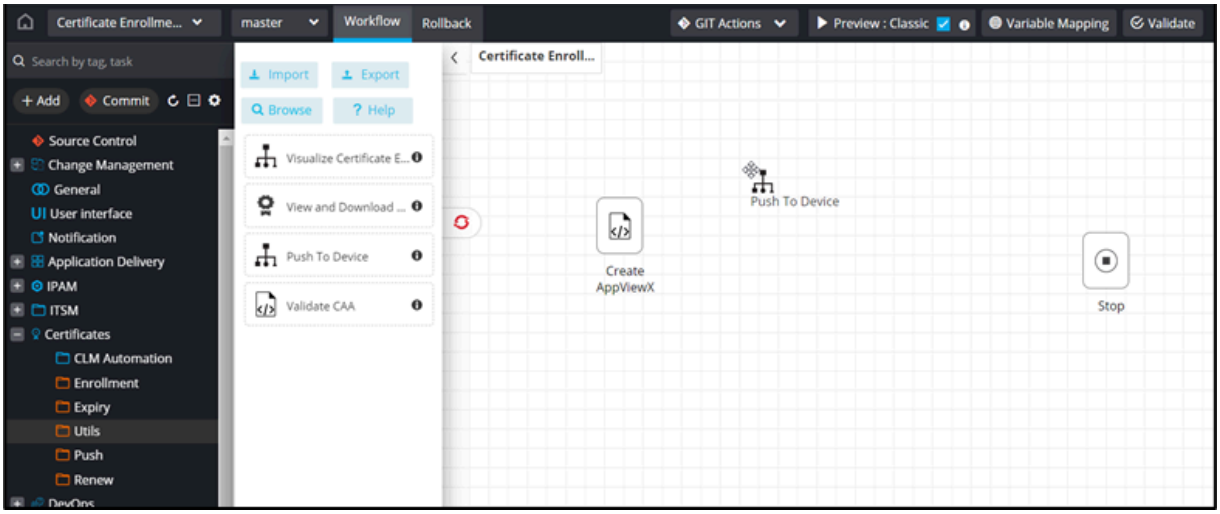
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



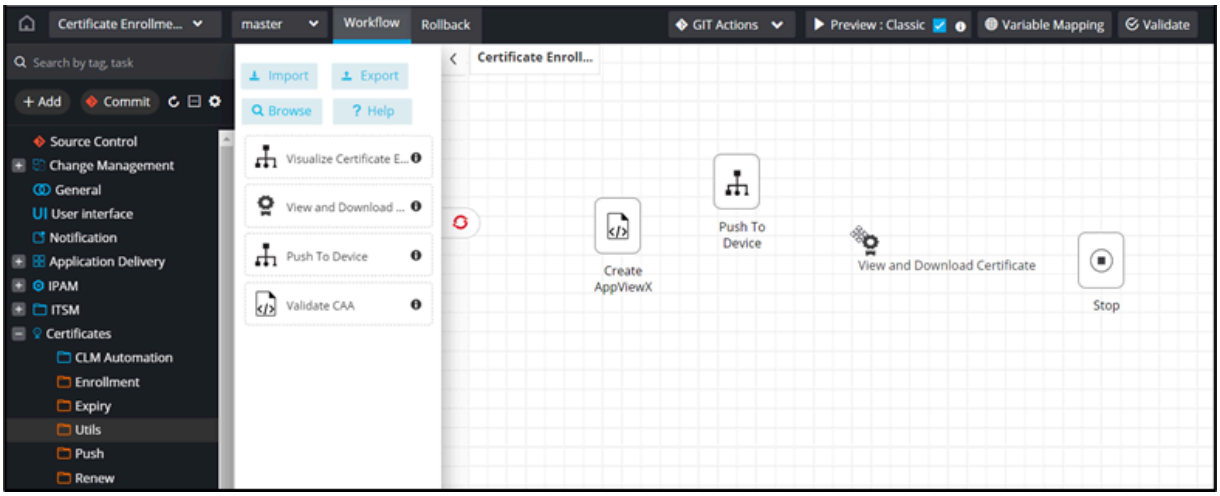
7. To access the OOB workflow tasks, from the left menu, click **Certificates**.
8. Under **Certificates**, from the **Enrollment** folder, drag and drop the required OOB task for enrolling a certificate, for example, the **Create AppViewX Certificate** task.



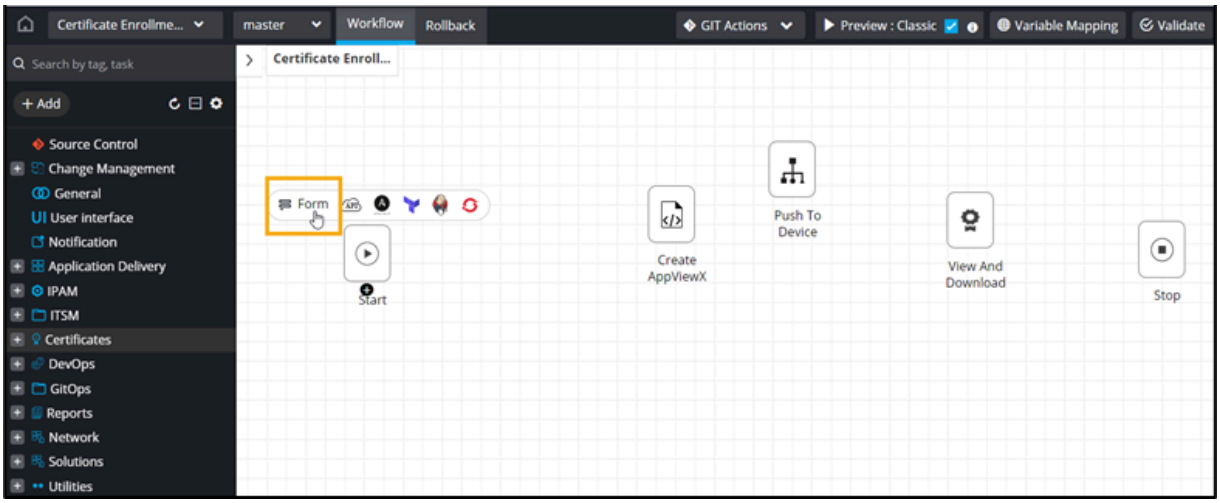
9. Click **Save**.
10. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **Push to Device** subflow.



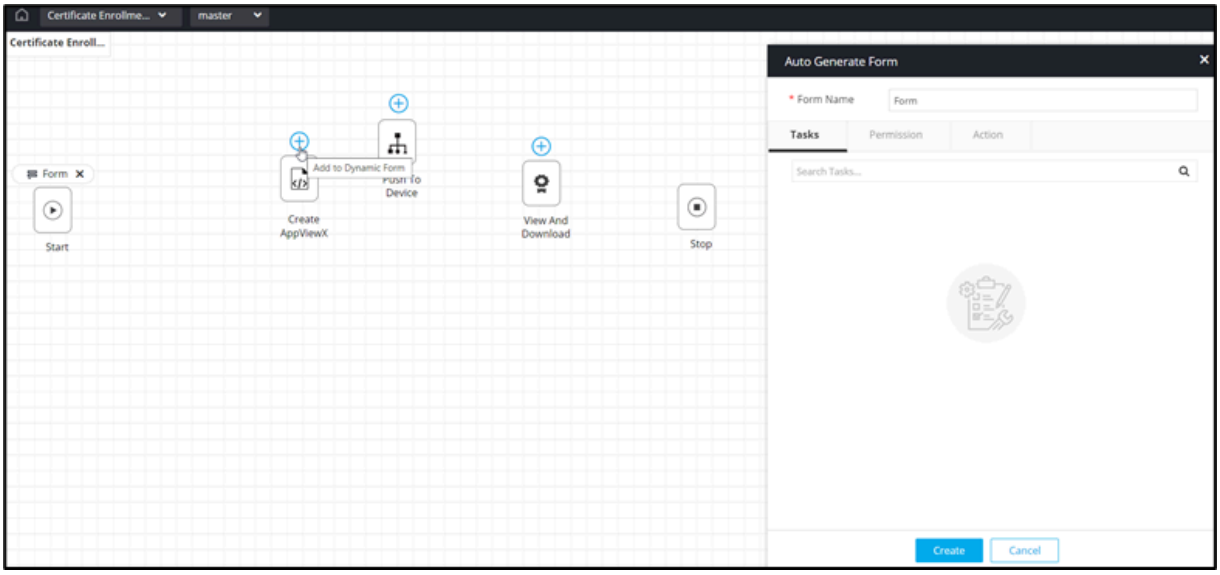
11. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **View and Download Certificate** task.



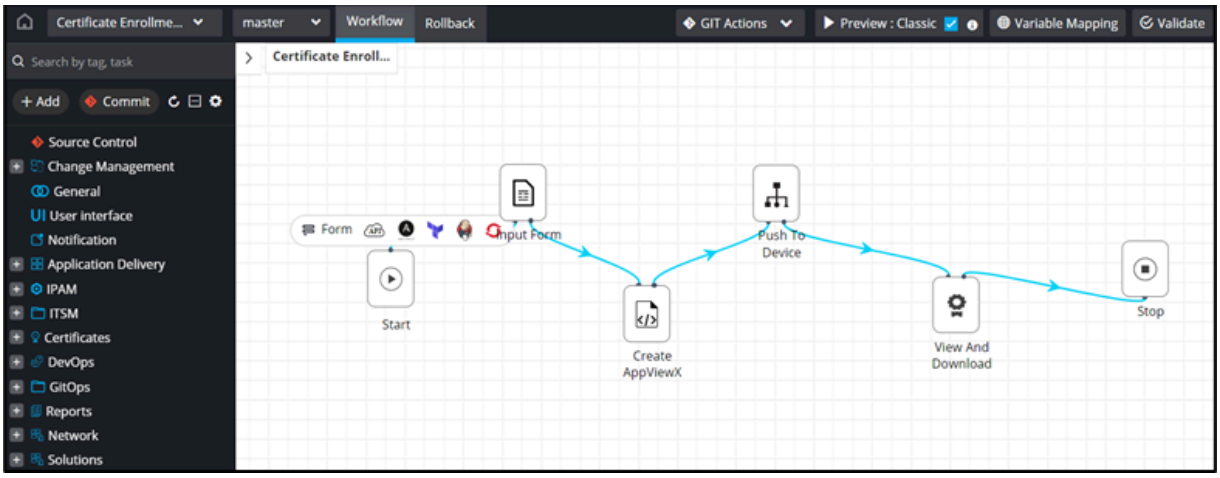
12. To generate a form for this workflow, click **Form** above the **Start** task.



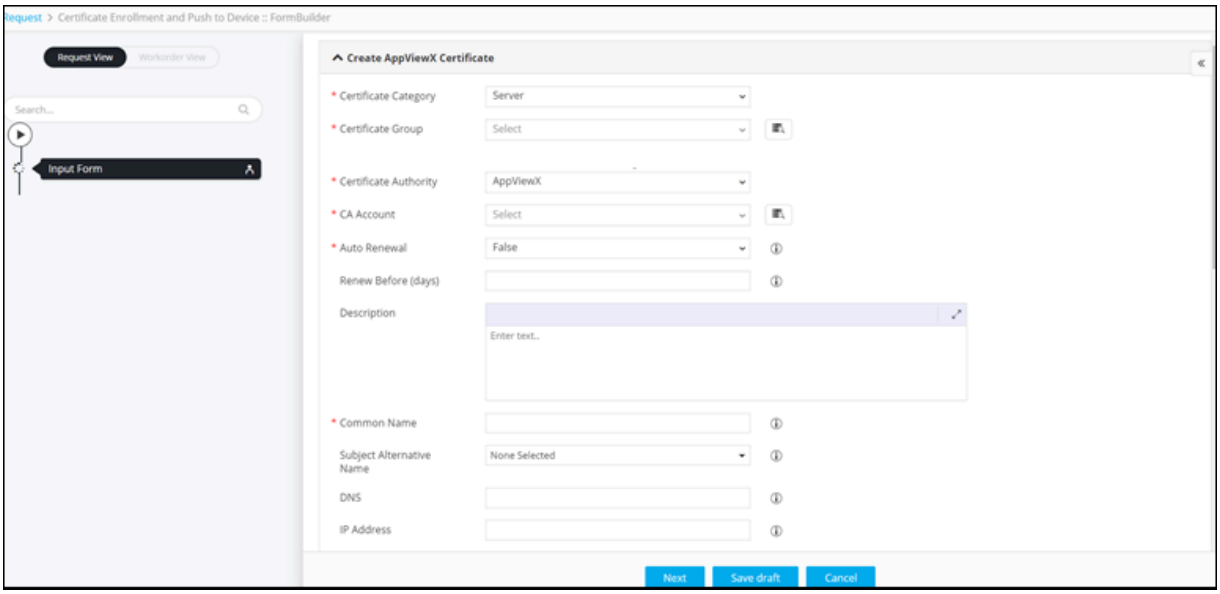
13. Click ⊕ above the **Create AppViewX Certificate** task to auto-populate the form fields.



14. Connect all workflow tasks and enable the workflow.



15. Trigger the workflow from the **Request :: View/Run** page.
16. The workflow execution page is displayed with the workflow inputs requested at the first stage.



The following table describes the fields in the input form:

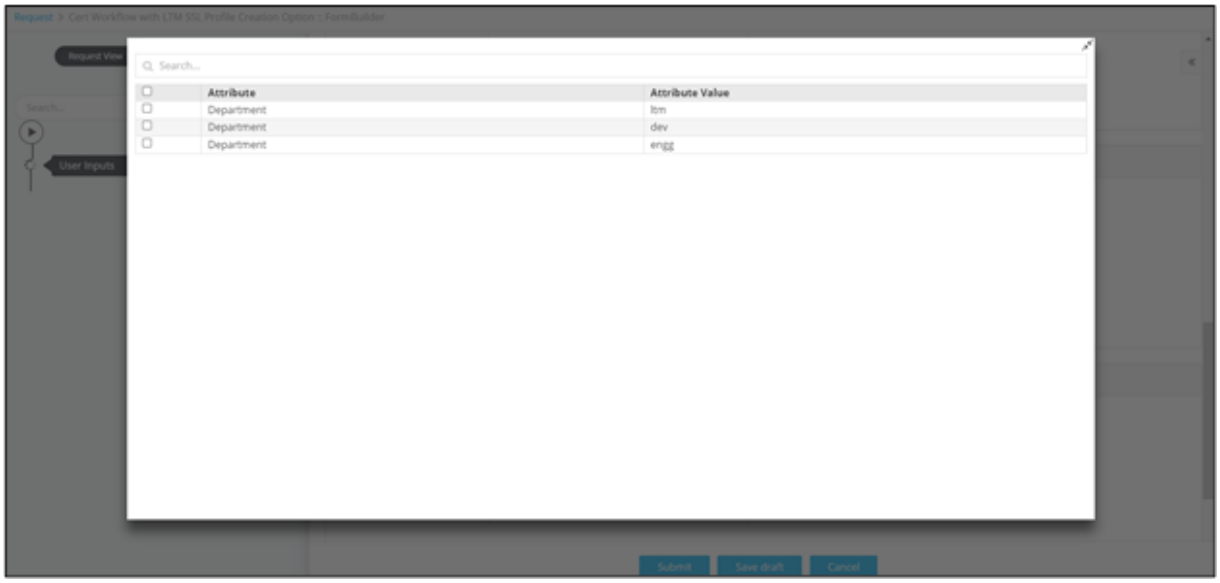
Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note:** Server is the default selection.

Field	Description
	:
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
Description	Enter a description for the certificate to be created.

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***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.  **Note:** This field will be populated based on the selected **Key Type**.

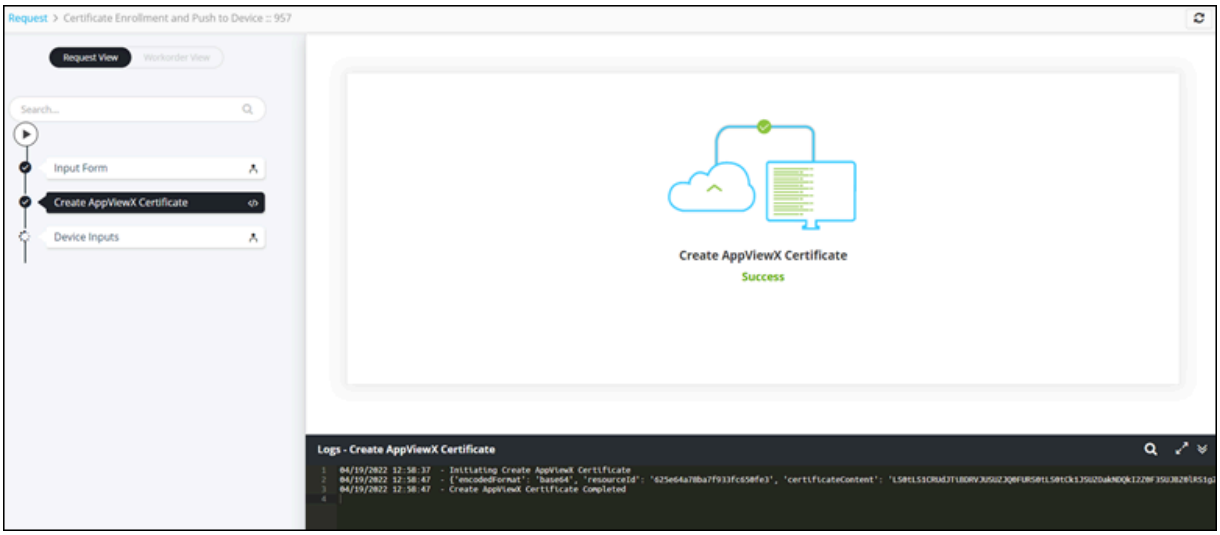
Field	Description
Attribute	Select the **Attribute** from the available options.
Attribute Value	Enter a value for the selected attribute.
All Asterisk (*) marked fields are mandatory.	

17. To add this attribute to the **Certificate Attributes** grid, click  .
18. To edit the value of a particular attribute, select the attribute in the grid and click  .
19. Enter the new value for the attribute in the **Value** field and click  again to update the value.
20. To delete a certificate attribute, select the attribute in the grid and click  .
21. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click  .

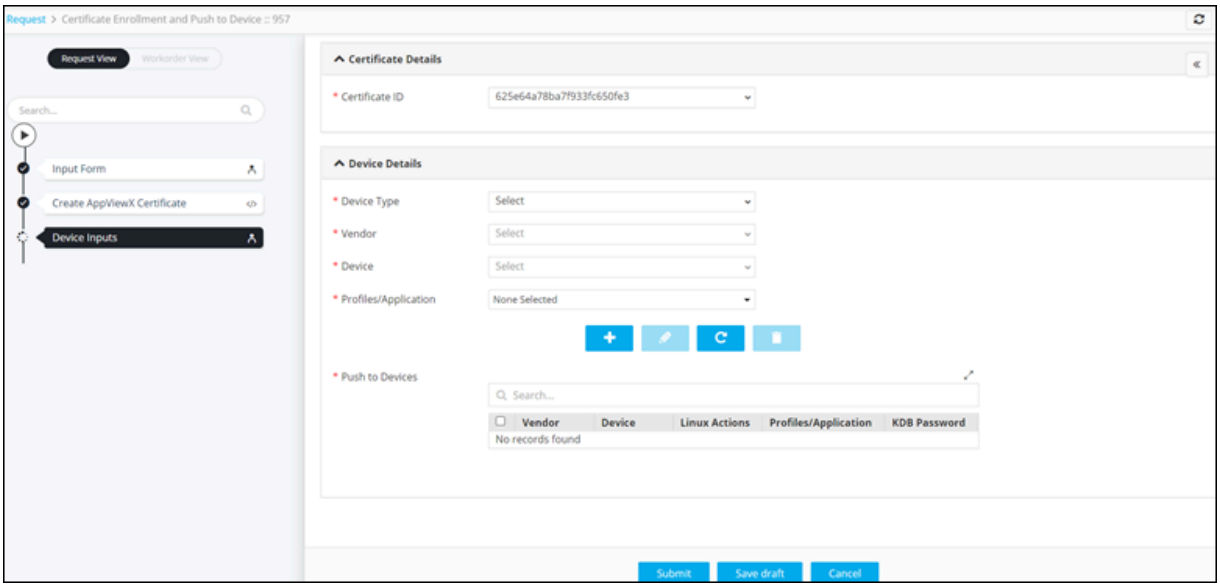


22. To search for a particular attribute in the grid, type the keyword(s) in the search field.
23. Click **Next**.

    AppViewX Certificate is created successfully.



24. At the **Device Inputs** stage of workflow execution, under **Device Details**, select the field information.



This table describes the field information in this section:

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown.

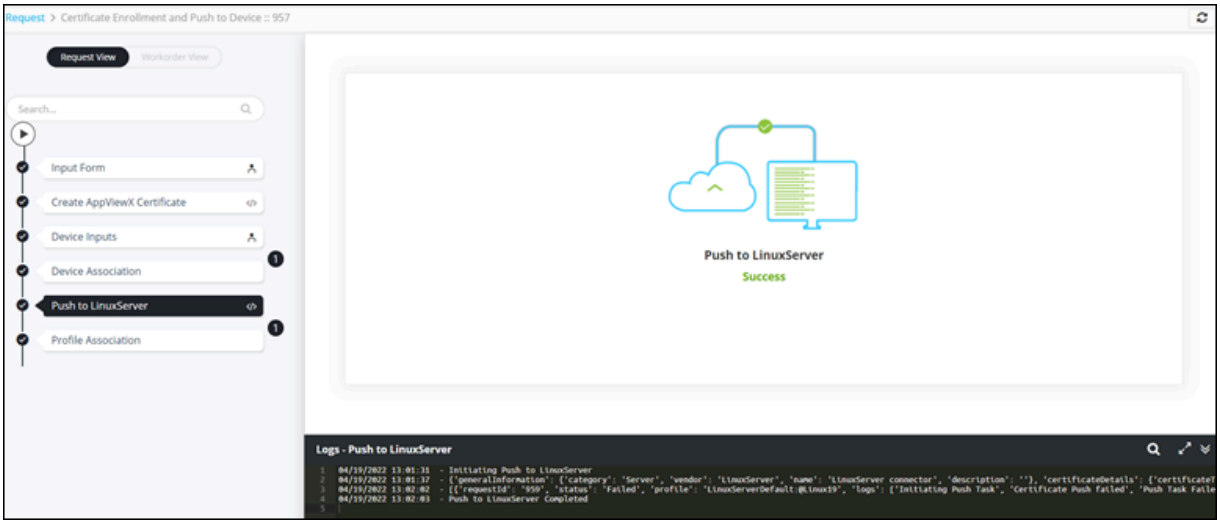
Field	Description
	Note: The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

25. To add the selected profile/application to the grid, click +.
    The **Profile/Application** is added to the **Push to Devices** grid.

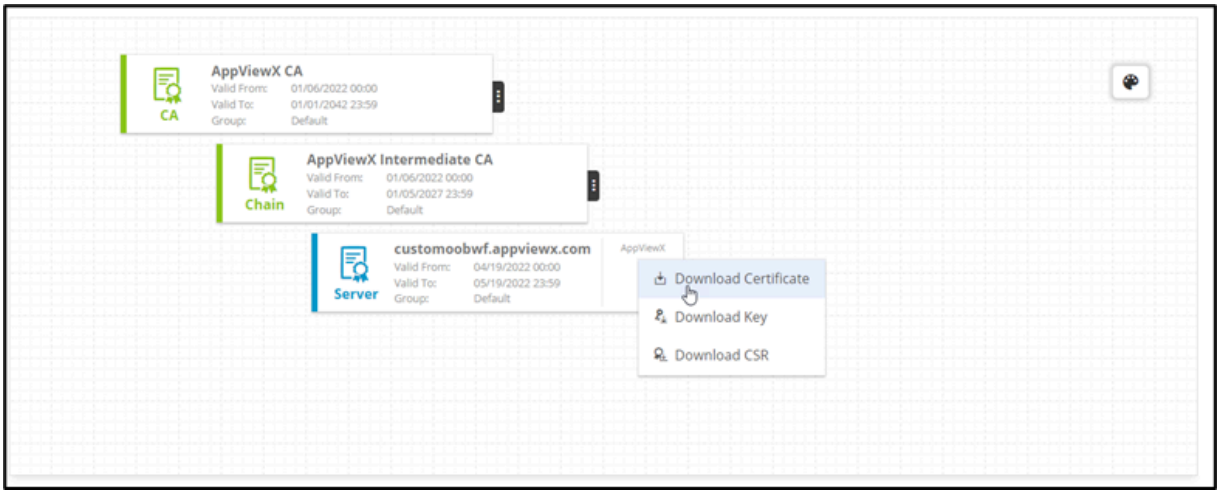
Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

26. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click  .
27. Select a new device and click  again to update the value.
28. To delete a profile/application, select the row to be deleted in the grid and click  .
29. To maximize the **Push to Devices** grid, from the top right corner of the grid, click  .
30. To search for a particular profile/application in the grid, type the keyword(s) in the search field.
31. Click **Submit**.

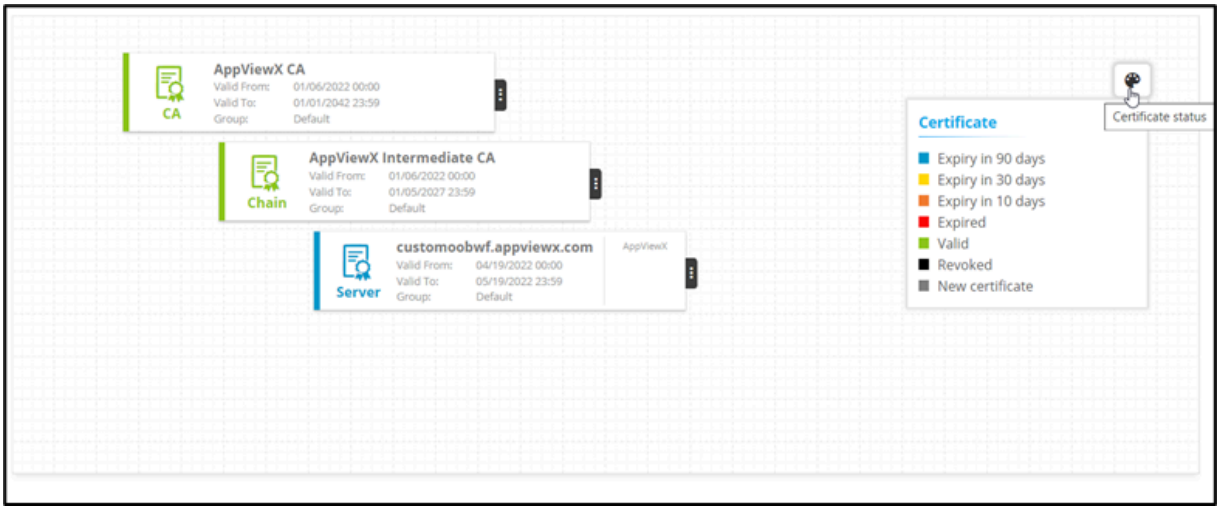
    Certificate pushed to the selected device.



32. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over  , and from the options displayed, click **Download Certificate**.



33. Hover your mouse over to view the Certificate status.



Chapter 10: Scheduling an OOB workflow

You can also schedule these OOB workflows to be triggered at specific time intervals (once or repeat daily, weekly, monthly, yearly) as per your requirement.

Note: For more information on scheduling workflows, refer to the Visual Workflow User Guide.

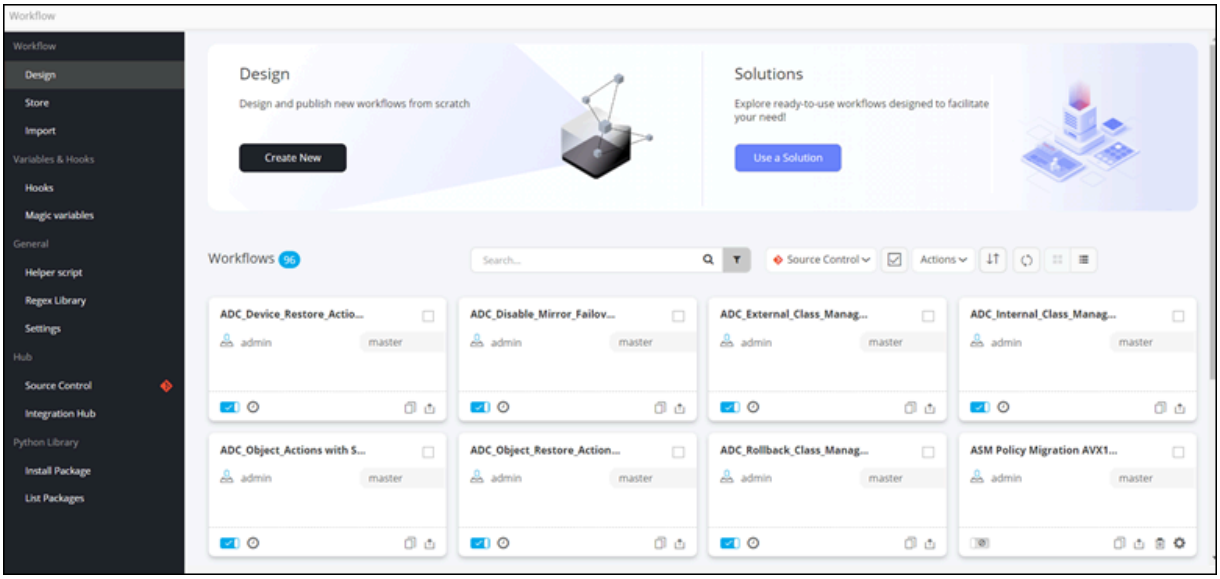
Chapter 11: Customizing an OOB Workflow

You can customize any of these OOB workflows by modifying individual tasks within the workflow.

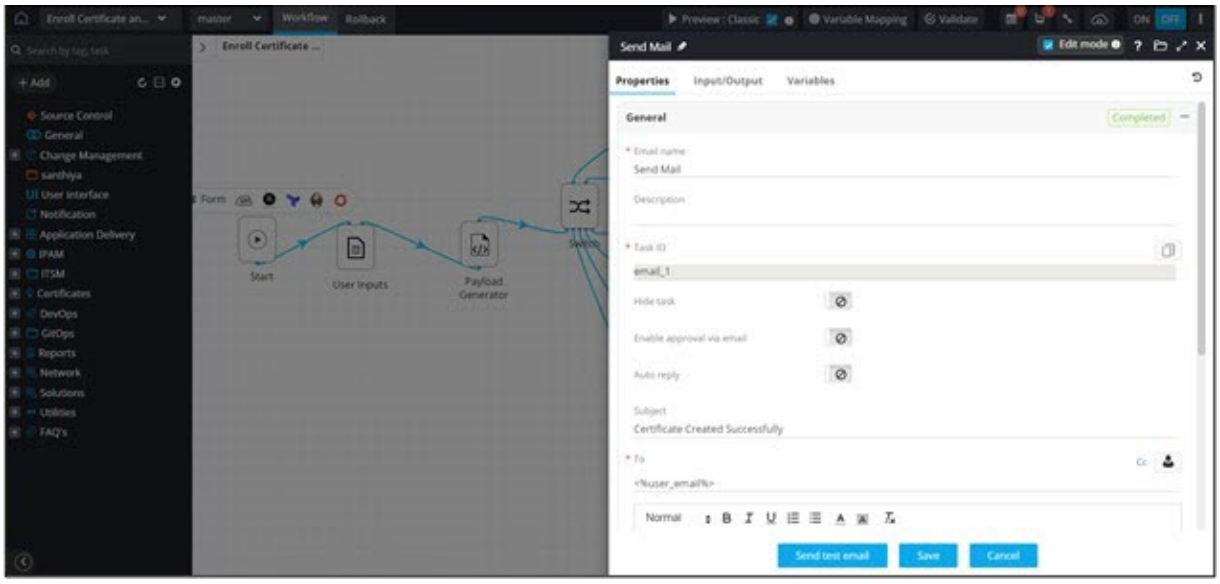
To customize a workflow:

1. Navigate to **Studio** > **Workflow**.

   The **Workflow Inventory** page is displayed.

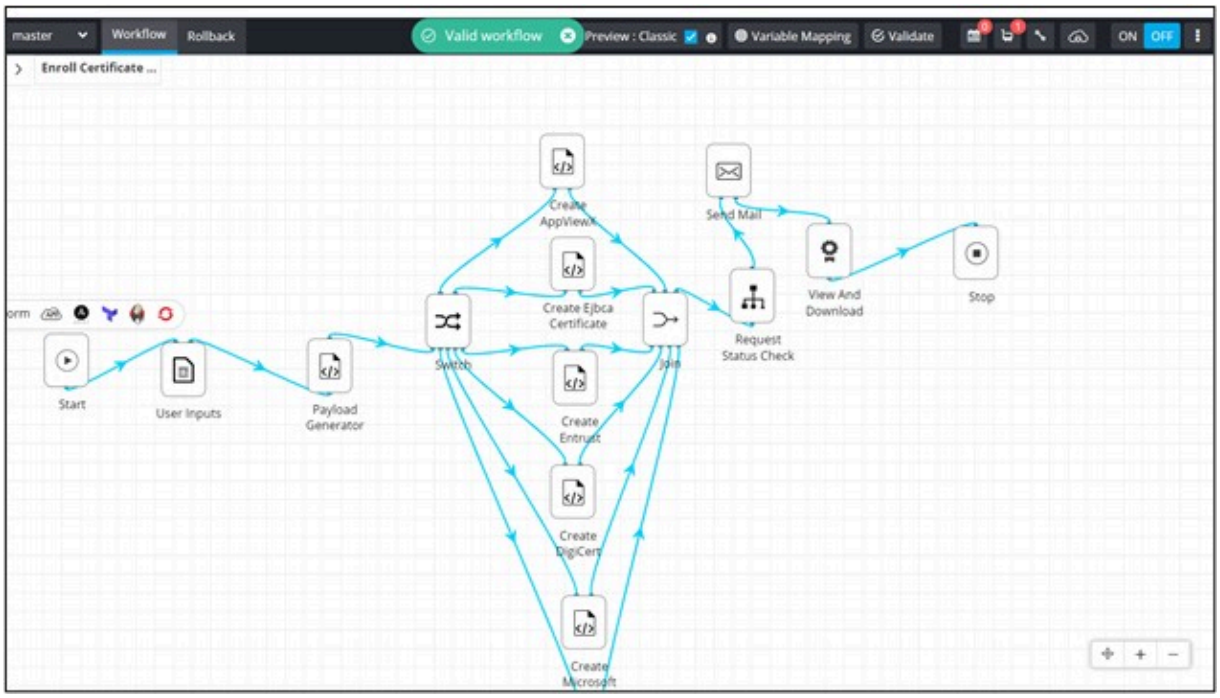


2. Search for the workflow by typing the keyword in the search bar.
3. Disable the workflow by turning off the toggle on the workflow card.
4. Click on the workflow to open it in the design space.
5. Modify the required tasks.



Note: For more information on workflow tasks, refer to the Visual Workflow User Guide.

6. Once the tasks have been modified as per your requirement, validate the workflow.



Note: For more information on validating a workflow, refer to the Visual Workflow User Guide.

7. Enable the workflow.

> **Note:** For more information on enabling a workflow, refer to the Visual Workflow User Guide.

8. Trigger the workflow from the **Request** page.

> **Note:** For more information on triggering workflows, refer to the Visual Workflow User Guide.